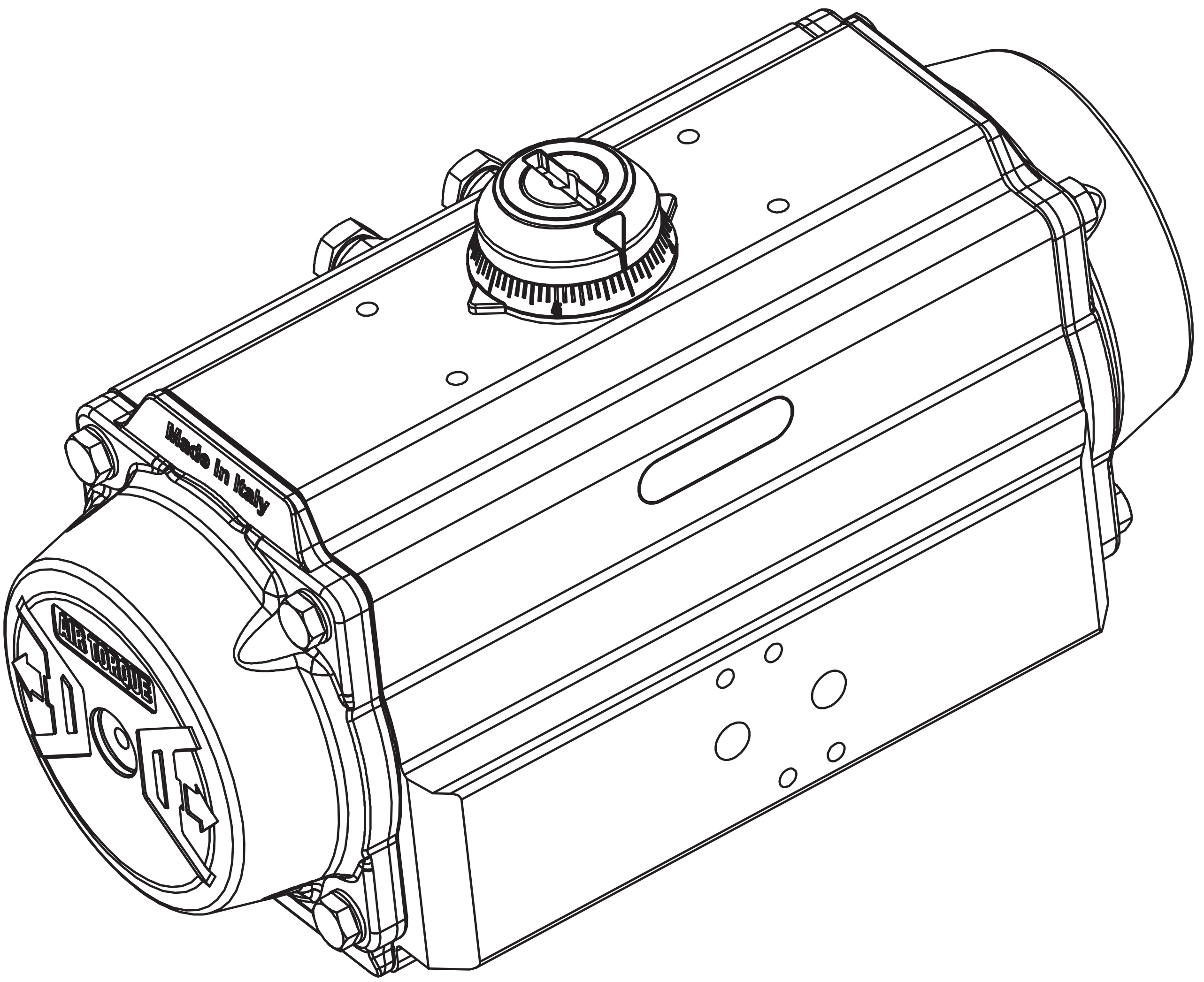
AIR TORQUE®

SIL-SAFETY MANUAL
FOR AIR TORQUE 4TH GENERATION
"*Upgrade*" Series Actuators



1) INTRODUCTION

1.1) Scope

This manual contains information, safety-related characteristics and warnings concerning the functional safety in accordance with IEC 61508 and concerning the application in the process industry in accordance with IEC 61511. It does not contain any particular details on other safety requirements, such as explosion protection or electrical safety.

1.2) Premises

This safety manual provides the necessary information to design, install, verify and maintain a Safety Instrumented Function (SIF) when using the Air Torque 4th Generation “Upgrade” series (in the following mentioned only as “Upgrade”). The “Upgrade” series pneumatic actuators are to be intended as a pneumatic device for remote operation of industrial valves when is pneumatically energized and or de-energized, and in any case the “Upgrade” series pneumatic actuators are to be intended to be part of a final element subsystem where the final element subsystem (consisting of a valve, positioner, actuator etc.) is connected to the safety rated logic solver which is actively performing the Safety Function as well as any automatic diagnostics designed to diagnose potentially dangerous failures of the actuator and any other final element components, (i.e. Partial Valve Stroke Test).
Anyway, the subject of this safety manual are just “Upgrade” series pneumatic actuators. Not subject of the safety manual are the driven valves, power and compressed air supply or the control of the actuators from the system as well as the control valves. Unambiguous assignments in a SIL can be only given to complete safety-related systems. Herein the “Upgrade” series pneumatic actuators are only one component.

1.3) Terms, abbreviation and definition

Term	Definition
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	Where solenoid valve is de-energized, supply pressure to the actuator is discontinued and spring are 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.
Safe failure Fraction	Safe failure fraction. $SFF \stackrel{\text{def}}{=} \left(1 - \frac{\lambda_{DU}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}\right)$
Failures in Time (FIT)	Number of failures in time. 1 FIT = (1 Failures/10^9 hr)
Partial Stroke Test (PST) Period	Minimum one PST per year Failures can be uncovered during PST.
Mission Time (T mission)	Expected operating lifetime expressed in hours for device to provide safety function.
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.
Dangerous failure	Failure with the potential to set the safety-related system to a dangerous or inoperative state.

Safety-related system	A safety-related system carries out the safety functions needed to establish or maintain a safe state, e.g. in a plant. Example: Pressure measuring instrument, logic unit (e.g. limit switch) and valve form a safety-related system.
Safety function	A defined function carried out by a safety-related system in order to establish or maintain a safe state of the plant, under consideration of a specified dangerous incident. Example: Pressure limit monitoring

1.4) Acronyms

Acronyms	Designation	Description
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).
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	One of four discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest.
MTBF	Mean Time Between Failures	Mean time between two failures
MTTR	Mean Time To Restoration	Mean time between the occurrence of a failure in a device or system and its repair
HFT	Hardware Fault Tolerance	Capability of a functional unit to continue executing the demanded function in case of faults or deviations.
λsd	Failure rate for all safe detected failures	
λsu	Failure rate for all safe undetected failures	
λdd	Failure rate for all dangerous detected failures	
λdu	Failure rate for all dangerous undetected failures	
SFF	Safe Failure Fraction	Fraction of non-hazardous failures, i.e. the fraction of failures without the potential to set the safety-related system to a dangerous or impermissible state.
PFDavg	Average Probability of Failure on Demand	Average likelihood that a dangerous safety function failures occurs on demand.
TI	Test interval between life testing of the safety function	Time interval between functional tests of the safety function
Low demand mode	Low demand mode of operation	Low demand mode is 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.
FMEA	Failure Modes, Effects and Diagnostic Analysis.	
MOC	Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.	

1.5) Related Literature

- Pneumatic Actuator product catalogue and technical data sheets,
- Installation, maintenance and operating instruction manual for 4th Generation “Upgrade” series actuators

1.6) Relevant Standards

- IEC 61508 Parts 1 to 7: Functional safety of electrical/electronic/ programmable electronic safety-related systems
- IEC 61511 Parts 1 to 3: Functional Safety - Safety Instrumented Systems for the Process Industry Sector.
- VDI 2180 Parts 1 to 5: Safeguarding of industrial process plants by means of process control engineering

2) DEVICE DESCRIPTION

The “Upgrade” series pneumatic actuators, are available in double acting (D) and spring return (S..) function. The output torque for double acting is from 13.2 Nm to 9,173 Nm at 5.5 bar supply pressure, while for spring return version the output torque is from 8.1 Nm to 4,068 Nm at the maximum spring set configuration. The “Upgrade” series pneumatic actuators are designed to meet ISO 5211 and EN 15714/3 requirements. In double acting version (air requested for both opening and closing operations), the safety function is determined by specific plant measures (e.g. by providing an auxiliary circuit equipped with compressed air reservoir), the actuator is controlled by 5/2 way valve.
In single acting (spring return) version, the safety function is provided by the springs force action when actuator is de-energized in case of loss of supply pressure (when power supply fails), the actuator is controlled by 3/2 way valve.

3) DESIGNING A SIF USING THE AIR TORQUE 4TH GENERATION LINE “UPGRADE” SERIES ACTUATORS

3.1) Safety Function

In case of dangerous situation a safety-related system will perform defined safety function. In this situation the actuator will be activated so that the actuator and the operated valve shall move to its failsafe position.
For example for spring return actuator when the actuator is de-energized, the actuator and valve shall move to its fail-safe position (depending on Fail direction specified fail-closed or fail-open).

⚠ **Warning:** It is user responsibility to verify if the actuator is equipped with device or accessories (e.g. lock-out system, gear-boxes, 100% travel stop adjustment etc.) that cannot permit to perform the requested safety function.
The actuator SIL capability may be invalidated.

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 installation, maintenance and operating instruction manual, brochure and technical data-sheets for service data and relevant information, of the “Upgrade” series actuators .

3.3) Application Limits

The construction materials of the “Upgrade” series actuators are specified in the product brochure and technical data-sheets. It is important the designer to check for the material suitability considering working conditions and on-site conditions. The use outside the application limits or with incompatible material of the “Upgrade” series actuators, may compromise the safety functions and the reliability of the provided data becomes invalid.

3.4) Design Verification

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. A complete report for the achieved Safety Integrity Level (SIL) of the “Upgrade” series pneumatic actuators is available at AIR TORQUE Spa.

3.5) Safety integrity level determination

The achievable safety integrity level (SIL) is determined by the following safety-related characteristics:

- Average probability of failure on demand (PFDavg)
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF)

The following table in accordance with IEC 61508 and IEC 61511 shows how the safety integrity level (SIL) depends on the average probability of failure on demand (PFDavg). It is based on low demand mode of operation, i.e. the frequency of demands on a safety-related system is no greater than once per year.

Safety integrity level (SIL)	PFDavg (low demand mode)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
PFDavg in low demand mode of operation according to IEC 61508-1, Table 2	

The sensor, logic unit and final element form a safety-related system that performs a safety function.

	Sensor e.g. pressure measuring instrument		Logic unit e.g. PLC		Final element e.g. actuator or valve
PFDavg	≤ X %	⇨	≤ X %	⇨	≤ X %

The average probability of failure on demand (PFDavg = sum of sensor, logic unit and final element failures) must be within the range of the demanded safety integrity level (SIL) in case of demand as listed in the above table.

The failure rate data listed in the certificates and FMEA (Failure Mode and Effect Analysis) reports are only valid for the useful life time of an “Upgrade” series actuator.

3.6) SIL Capability

3.6.1) Systematic Integrity

For standard and special version/type of “Upgrade” pneumatic actuators, the achievable failure rates when used in a redundant structure (multi-channel architecture) allow the usage up to and including a Safety Integrity Level SIL 3 (for SIL 3 application HFT = 1 is required).
Standard and special version/type of “Upgrade” pneumatic actuators, fulfills the safety relevant constrains for usage in single channel system up to and including Safety Integrity Level SIL 2.
See the product related certificates. 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.

3.6.2) Random Integrity

Standard and special version/type of “Upgrade” pneumatic actuator are Type A Device (See the product related Certificate). The “Upgrade” pneumatic actuators are typically one of several devices that can be used in a final element assembly. When the final element assembly consists of many components (pneumatic actuator, valve, solenoid, 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.

3.6.3) Safety Parameters

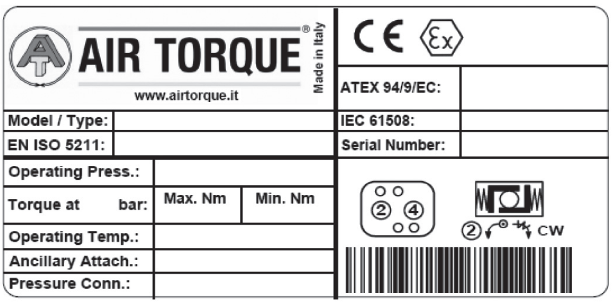
Refer to the certificates and test reports for detailed failure rate information of the “Upgrade” series pneumatic actuator.

3.7) Connection of the 4th Generation “Upgrade” series actuator to the SIS Logic-solver

The “Upgrade” series pneumatic actuator may be connected to the safety rated logic-solver which may actively perform the safety function as well as automatic diagnostics designed to diagnose potentially dangerous failures within “Upgrade” series actuator (i.e. partial stroke test).

3.8) General Requirements

The system’s response time shall be less than process safety time. The “Upgrade” series pneumatic actuator is only one part of the final element of a SIS. All elements of the SIF must be selected to meet safety response time. All SIS components including the “Upgrade” actuator must be operational before process start-up. User shall verify that the “Upgrade” pneumatic actuator is suitable for use in safety applications by confirming the “Upgrade” actuator’s label is properly marked (see below example).



Personnel performing maintenance and testing on the “Upgrade” series actuator 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 “Upgrade” series pneumatic actuator must be installed as per standard practices outlined in the Installation Manual.
The environment must be checked to verify that environmental conditions do not exceed the ratings.
The “Upgrade” series pneumatic actuator must be accessible for physical inspection.

4.2) Physical Location and Placement

The “Upgrade” series pneumatic actuator shall be accessible with sufficient room for pneumatic connections and for manual proof testing. Pneumatic piping to the valve shall be kept as short and straight as possible to minimize the air-flow restrictions and potential clogging. Long or kinked pneumatic tubes may also increase the valve closure time. The “Upgrade” pneumatic actuator 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 connectors or the vibration should be reduced using appropriate damping mounts.

4.3) Mechanical and pneumatic installation and Connections

- During mechanical and pneumatic installation, themounting and operating instructions of the corresponding device must be followed.
- On sizing actuators, note that the actuator must provide sufficient torque to overcome the closing torque in closed position as well as the dynamic torque in open position. The actuator sizing, include also verification of the permissible torques for the valve shaft, shaft adapter etc. as a result, the max. torque of the actuator (air or spring torque) must not exceed these torques under any circumstances. The ISO 5211 and EN 15081 requirements must be respected.
- Recommended piping for the inlet and outlet pneumatic connections to the “Upgrade” pneumatic actuator is minimum 1/4” (depending on actuator size and air volume) stainless steel or PVC tubing. The length of tubing between the pneumatic actuator and the control device, such as a solenoid valve, shall be kept as short as possible and free of kinks. Direct mount on actuator air connections interface of the control device is recommended.
- The process air capacity shall be sufficient to move the “Upgrade” pneumatic actuator within the required time.
- The minimum requirements for the operating medium (power supply) according to ISO 8573-1 are:
  pressure dewpoint ≤ -20°C (or at least 10 °K below ambient temperature), maximum particle size < 30 microns.
- To prevent corrosion of the actuator springs, measures must be taken to prevent water or moisture entering the actuator.
- The process air pressure shall meet the requirements set forth in the installation manual. Important Verification: Function and operating time (open and closing time) shall be verified after installation. Effect of different operating pressure shall be considered for the verification.

5) OPERATION AND MAINTENANCE

5.1) Proof test without automatic testing

The scope of proof testing is to detect failures within the “Upgrade” pneumatic actuator 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 the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which the “Upgrade” pneumatic actuator 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 Air Torque Spa. The suggested proof test consists of a full stroke of the 4th Generation “Upgrade” pneumatic actuator The person(s) performing the proof test of an “Upgrade” pneumatic actuator should be trained in SIS operations, including bypass procedures, pneumatic actuator maintenance and company Management of Change procedures. No special tools are required.

Table 1: Recommended Proof Test

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 4th Generation “Upgrade” pneumatic actuator 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.

The proof test coverage for the “Upgrade” pneumatic actuator are listed in the certificates and FMEA (Failure Mode and Effect Analysis) reports which are available from Air Torque Spa.

5.2) Proof test with automatic partial stroke testing

An automatic partial valve stroke testing scheme that also performs a periodic full stroke of the “Upgrade” pneumatic actuator and valve movement timing will detect most potentially dangerous failure modes.
It is recommended that a physical inspection (Step 2 from Table 1) is 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

Repairing procedures for the “Upgrade” pneumatic actuators are described in the Installation, Operation and Maintenance manual that must be followed. The SIL rating of the “Upgrade” pneumatic actuator will be voided if the repair is not performed with Air Torque spa OEM repair parts and serviced by a competent person.

5.4) **Useful Life**

Useful lifetime is an engineering reliability term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues. For normal service condition and planned minimum maintenance for the 4th Generation “Upgrade” pneumatic actuator the useful lifetime can be up to 10 years and over depending by real operating conditions. When field experience indicates a shorter useful lifetime than indicated, the number based on field experience should be used.

The useful lifetime is highly dependent on the subsystem itself and its operating conditions. It is the responsibility of the end user to maintain and operate the 4th Generation “Upgrade” pneumatic actuator per manufacturer’s instructions. Furthermore regular inspections should show that all components are clean and free from damage.
Cycle life varies by actuator size up to over 1.000.000 cycles for smaller size depending on real working conditions and maintenance intervals.

5.5) **Manufacturer Notification**

Any failures that are detected and that compromise functional safety should be reported to Air Torque Spa. Please contact Air Torque Spa customer service or your local Air Torque service representative.

AIR TORQUE S.p.a. - Via Livelli di Sopra 8/11, 24060 - Costa di Mezzate (Bg) Italy
Tel.: + 39 035 682299 - Fax.: + 39 035 687791 - e-mail: info@airtorque.it - www.airtorque.it

5.6) **Start-Up Checklist**

The following checklist may be used as a guide to employ the Air Torque “Upgrade” series pneumatic actuators in a safety critical SIF compliant to IEC61508.

Activity	Result	Verified	
		By	Date
Design			
Target Safety Integrity Level and PFDAVG determined			
Correct valvemode chosen (Fail closed, Fail open)			
Design decision documented			
Pneumatic compatibility and suitability verified			
SIS logic solver requirements for valve tests defined and documented			
Routing of pneumatic connections determined			
SIS logic solver requirements for partial stroke tests defined and documented			
Implementation			
Physical location appropriate			
Pneumatic 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			
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			

Head office Works:

AIR TORQUE S.p.A.

società uninominale

Head Offices: Via dei Livelli Sopra, 11
Factory: Via dei Livelli Sopra, 8
24060 COSTA DI MEZZATE (BG) - Italy
Tel.:+39 035 682299 - Fax: +39 035 687791
info@airtorque.it - www.airtorque.it