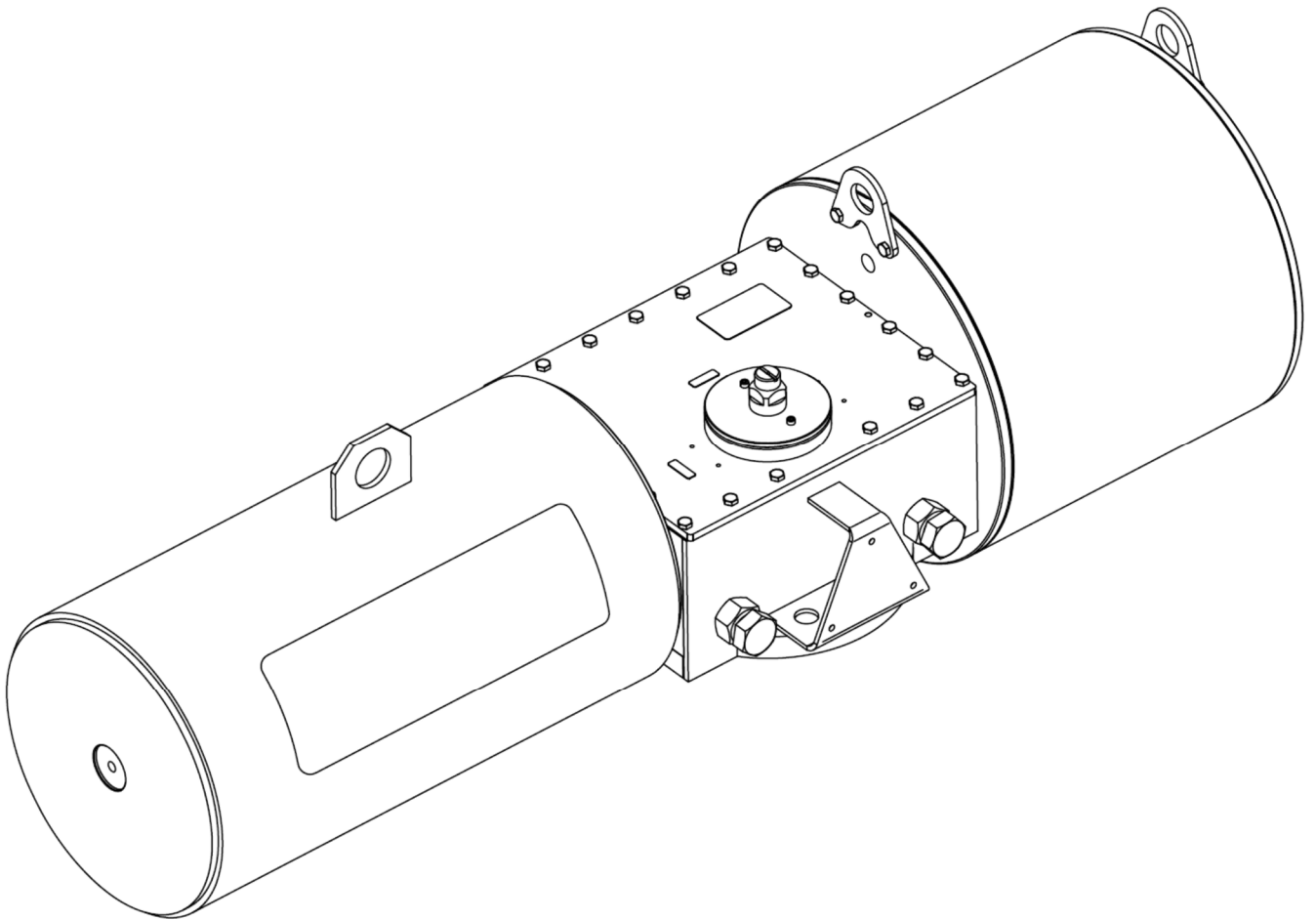


---

# **SIL-SAFETY MANUAL**



## 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 SCOTCH YOKE actuators AT-HD Series (in the following mentioned only as "AT-HD"). The "AT-HD" series actuators are to be intended as a device for remote operation of industrial valves when is energized (supplying pressurized gases or oil to the power module depending by actuator type) and or de-energized, and in any case the "AT-HD" series 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 "AT-HD" series 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 "AT-HD" series actuators are only one component.

### 1.3. Terms, abbreviation and definition

Term	Definition
<b>Safety</b>	Freedom from unacceptable risk of harm.
<b>Functional Safety</b>	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.
<b>Basic Safety</b>	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
<b>Safety Assessment</b>	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.
<b>Fail-Safe State</b>	where solenoid valve is de-energized, supply pressure to the actuator is discontinued and spring are extended.
<b>Fail Safe</b>	Failure that causes the valve to go to the defined fail-safe state without a demand from the process
<b>Fail Dangerous</b>	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
<b>Fail Dangerous Undetected</b>	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
<b>Safe failure fraction</b>	Safe failure fraction. $SFF \stackrel{\text{def}}{=} \left( 1 - \frac{\lambda_{DU}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \right)$
<b>Failures in Time (FIT)</b>	Number of failures in time. 1 FIT = (1 Failures/10 <sup>9</sup> hr)
<b>Partial Stroke Test (PST) Period</b>	Minimum one PST per month ==> 720 hr Failures can be uncovered during PST.
<b>Mission Time (T mission)</b>	Expected operating lifetime expressed in hours for device to provide safety function (10, 15 or 20 years).
<b>Fail Annunciation Undetected</b>	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.
<b>Fail Annunciation Detected</b>	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.
<b>Fail No Effect</b>	Failure of a component that is part of the safety function but that has no effect on the safety function
<b>Low demand Mode</b>	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
<b>Dangerous failure</b>	Failure with the potential to set the safety-related system to a dangerous or inoperative state.

<b>Safety-related system</b>	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.
<b>Safety function</b>	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
<b>SIS</b>	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).
<b>SIF</b>	Safety Instrumented Function	A set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
<b>SIL</b>	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.
<b>MTBF</b>	Mean Time Between Failures	Mean time between two failures
<b>MTTR</b>	Mean Time To Restoration	Mean time between the occurrence of a failure in a device or system and its repair
<b>HFT</b>	Hardware Fault Tolerance	Capability of a functional unit to continue executing the demanded function in case of faults or deviations.
$\lambda_{sd}$	Failure rate for all safe detected failures	
$\lambda_{su}$	Failure rate for all safe undetected failures	
$\lambda_{dd}$	Failure rate for all dangerous detected failures	
$\lambda_{du}$	Failure rate for all dangerous undetected failures	These failures may be detected by PST.
<b>SFF</b>	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.
<b>PFD<sub>avg</sub></b>	Average Probability of Failure on Demand	Average likelihood that a dangerous safety function failures occurs on demand.
<b>TI</b>	Test interval between life testing of the safety function	Time interval between functional tests of the safety function
<b>Low demand mode</b>	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.
<b>FMEA</b>	Failure Modes, Effects and Diagnostic Analysis.	
<b>MOC</b>	Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.	

#### 1.5. Related Literature

- “AT-HD” actuator product catalogue and technical data sheets,
- Installation, maintenance and operating instruction manual for “AT-HD” 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 “AT-HD” series actuators are available in double acting (D) and spring return (S) configuration with or without manual emergency override. The Series can be powered with pneumatic or hydraulic fluids. When fast actin maneuver is required, quick and damper system (Q&D) can be mounted on the pneumatic cylinder.

For output torque values see technical data sheets. The “AT-HD” series actuators are designed in compliance to ISO 5211, EN 15714/3 and EN 15714/4.

In double acting version (air/oil 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/oil 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 “AT-HD” SERIES ACTUATORS

### 3.1. Safety Function

Emergency Shutdown Close (ESD-Close): A remote, external ESD signal may be applied to the actuator to move the valve to the CLOSE position through predetermined, user-configured shutdown position, overriding existing control signals.

**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. Enviromental 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 “AT-HD” series actuators .

### 3.3. Application Limits

The construction materials of the “AT-HD” series actuators are specified in the product brochure and technical data-sheets. It is important for 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 “AT-HD” 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 “AT-HD” series 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)

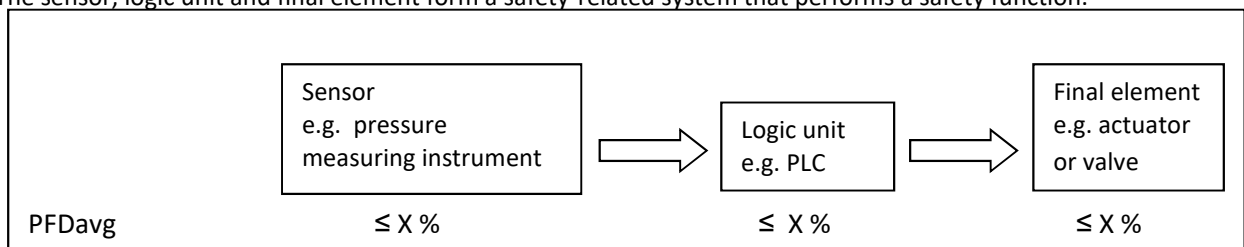
- Safe failure fraction (SFF)

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.



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 “AT-HD” series actuator.

### 3.6. SIL Capability

#### 3.6.1. Systematic Integrity

Standard version of “AT-HD” actuator has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. 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 version of “AT-HD” actuator is a Type A Device (See the product related Certificate) and is typically one of several devices that can be used in a final element assembly. When the final element assembly consists of many components (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 “AT-HD” series actuator.

### 3.7. Connection of the “AT-HD” series actuator to the SIS Logic-solver






The “AT-HD” series 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 “AT-HD” series actuator (i.e. partial stroke test).

### 3.8. General Requirements

The system’s response time shall be less than process safety time. The “AT-HD” series 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 “AT-HD” actuator must be operational before process start-up.

User shall verify that the “AT-HD” actuator is suitable for use in safety applications by confirming the “AT-HD” actuator’s label is properly marked (see below example).

 <b>AIR TORQUE</b> ® Made in Italy www.airtorque.it	
Actuator Model:	
Type:	
Fluid:	Op. Temperature:
Operating Pressure:	
Max. Operating Torque:	
Produc. / S.N. :	
TAG No:	
 	ATEX 94/9/EC: T.F. : ATX 13AT-HD
	

Personnel performing maintenance and testing on the “AT-HD” 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 “AT-HD” series 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 “AT-HD” series actuator must be accessible for physical inspection.

##### 4.2. Physical Location and Placement

The “AT-HD” series actuator shall be accessible with sufficient room for power module connections and for manual proof testing.

The piping to the actuator control devices shall be kept as short and straight as possible to minimize the flow restrictions and potential clogging. Long or kinked tubes may also increase the valve closure time.

The “AT-HD” 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 the supply connectors or the vibration should be reduced using appropriate damping mounts.

##### 4.3. Mechanical installation and Power Connections

- During mechanical installation and pneumatic/hydraulic connection, the mounting 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 (power 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 supply connections to the “AT-HD” actuator is minimum 1/4” (depending on actuator power module size), typically are in stainless steel material. The length of tubing between the actuator and the control device, such as a solenoid valve, shall be kept as short as possible and free of kinks. The power supply capacity of the system shall be sufficient to move the “AT-HD” actuator within the required time.
- Operating medium (power supply): The quality of the operating medium shall be at least as specified in the EN 15714/3 and EN 15714/4
- 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 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 person(s) performing the proof test should be trained in SIS operations, including bypass procedures, "AT-HD" actuator maintenance and company Management of Change procedures. No special tools are required.

Written internal administrative procedures must be created by end user to guarantee the correct use/managing of bypass, manual override and proof test.

**Table1: 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 "AT-HD" 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 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 "AT-HD" 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 "AT-HD" actuators are described in the Installation, Operation and Maintenance manual that must be followed.

The SIL rating of the "AT-HD" 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

According to IEC 61508-2 section 7.4.7.4, a useful life of the "AT-HD" actuator is 10 to 15 years. This statement applies only to "AT-HD" actuator and for deployment thereof for a period of time of maximum 8 years plus maximum of 2 years storage time before being used for the first time and provided that all safety-relevant operating conditions as stated by the manufacturer are complied with. Other life value can be assumed based the user's experience. Cycle life varies by actuator size up to over 500.000 cycles for smaller size depending on 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](mailto: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 “AT-HD” series actuators in a safety critical SIF compliant to IEC61508.

Activity	Result	Verified	
		By	Date
<b>Design</b>			
Target Safety Integrity Level and PFD <sub>avg</sub> determined			
Correct valve mode chosen (Fail closed, Fail open)			
Design decision documented			
Power operating fluid compatibility and suitability verified			
SIS logic solver requirements for valve tests defined and documented			
Routing of power fluid connections determined			
SIS logic solver requirements for partial stroke tests defined and documented			
<b>Implementation</b>			
Physical location appropriate			
Power fluid 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			
<b>Verification and Testing</b>			
Electrical connections verified and tested			
Power fluid 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			
<b>Maintenance</b>			
Tubing blockage / partial blockage tested			
Safety loop function tested			