

Multi-turn actuators

SA 07.2 – SA 16.2/SAR 07.2 – SAR 16.2

SAEx 07.2 – SAEx 16.2/SAREx 07.2 – SAREx 16.2

with actuator controls

AC 01.2-SIL/ACExC 01.2-SIL

SIL version



NOTICE for use!

This document is only valid with the latest operation instructions attached to the device, the attached Manual as well as the respectively pertaining technical and electrical data sheets. They are understood as reference documents.

Purpose of the document:

This document informs about the necessary actions required for the deployment of the device in safety-related systems according to IEC 61508, or IEC 61511.

Reference documents:

- Operation instructions (Assembly and commissioning) for the actuator
- Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls
- Manual (Device integration) AC(V) 01.2/AC(V)ExC 01.2 actuator controls
- Technical data for multi-turn actuator.
- Technical data for actuator controls.

Reference documents are available on our website <https://www.auma.com>.

Table of contents

1 Terminology	5
1.1 Terms and abbreviations	5
2 Application and validity	7
2.1 Range of application	7
2.2 Standards	7
2.3 Valid device types	7
3 Architecture, configuration and applications	8
3.1 Architecture (actuator sizing)	8
3.2 Configuration (setting)/version	9
3.3 Protection against uncontrolled operation (self-locking/brake)	11
3.4 Operation mode (low/high demand mode)	12
3.5 Further notes and indications on architecture	12
3.6 Applications (environmental conditions)	12
4 Safety instrumented systems and safety functions	14
4.1 Safety instrumented system including an actuator	14
4.2 Safety functions	14
4.3 Safe inputs and outputs	15
4.4 Redundant system architecture	15
4.5 Examples of applications	17
4.6 System representation	18
5 Installation, commissioning and operation	19
5.1 Installation	19
5.2 Commissioning	21
5.3 Operation	22
5.4 Lifetime	22
5.5 Decommissioning	22
6 Indications on display	24
6.1 Status indications on SIL functions	24

6.2	SIL configuration warning.....	25
6.3	Backlight.....	25
7	Indications	26
7.1	Signals via SIL module.....	26
7.2	SIL fault signal via the display of the actuator controls in standard version (for troubleshooting support)	26
7.3	Status signals via output contacts (digital outputs) of actuator controls in standard version	27
7.4	Signals via fieldbus of actuator controls in standard version	28
8	Tests and maintenance.....	29
8.1	Check safety equipment.....	29
8.2	Internal actuator monitoring of the device with control via actuator controls in standard version	29
8.3	Execute Partial Valve Stroke Test (PVST).....	29
8.4	Proof test (verification of safe actuator function).....	31
8.4.1	Preliminary test	32
8.4.2	Check "Safe OPENING/CLOSING" Safe ESD safety operation	32
8.4.3	Check SIL fault signal "Actuator monitoring"	32
8.4.4	Check Safe ESD reaction for "Motor protection (thermal fault)" signals	33
8.4.5	Check Safe ESD reaction to "Limit seating with overload protection" (limit and/or torque evaluation)	34
8.4.6	Check Safe ESD reaction to "Forced limit seating in end position" (limit evaluation) – for actuators with electromechanical control unit	35
8.4.7	Check Safe ESD reaction to "Forced limit seating in end position" (limit evaluation) – for actuators with electronic control unit and limit switches	35
8.4.8	Check Safe ESD reaction to "Forced torque seating in end position" (torque after limit evaluation)	36
8.4.9	Check Safe ESD reaction for "no seating" (no evaluation of limit and torque).....	36
8.4.10	Check Safe STOP function	37
8.4.11	Check combination of Safe ESD and Safe STOP function.....	37
8.5	Maintenance.....	38
9	Safety-related figures.....	39
9.1	Determination of the figures	39
9.2	Specific figures for AC 01.2 actuator controls in SIL version with actuators of SA .2 series.....	40
9.2.1	Figures for actuators with conventional output drive types (without extension flange)	40
9.2.2	Figures for actuators equipped with alternative output drive types.....	42
10	Checklists	44
10.1	Commissioning checklist.....	44
10.2	Proof test checklists	44
10.2.1	Preliminary inspection checklist.....	44
10.2.2	Safe ESD safety operation (Safe OPENING/CLOSING) – irrespective of the selected control unit	44
10.2.3	SIL fault signal "Actuator monitoring" – irrespective of the selected control unit	45
10.2.4	Safe ESD reaction for "Motor protection (thermal fault)" signals – irrespective of the selected control unit	45
10.2.5	Safe ESD reaction to "Limit seating with overload protection" (limit and/or torque evaluation) – for actuators with electromechanical control unit.....	46
10.2.6	Safe ESD reaction to "Forced limit seating in end position" (limit evaluation) – for actuators with electromechanical control unit	47
10.2.7	Safe ESD reaction to "Forced limit seating in end position" (limit evaluation) – for actuators with electronic control unit and limit switches	48
10.2.8	Safe ESD reaction to Forced torque seating in end position (limit evaluation) – for actuators with electromechanical control unit	48
10.2.9	Safe ESD reaction to "No seating" – for actuators with electromechanical control unit or with electronic control unit with limit switches	49
10.2.10	Safe STOP function – irrespective of the selected control unit.....	50

10.2.11 Combination of Safe ESD and Safe STOP – irrespective of the selected control unit 51

Index..... 52

1 Terminology

- Information sources
- IEC 61508-4, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Terms and abbreviations
 - IEC 61511-1, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

1.1 Terms and abbreviations

For assessment of the safety function, the lambda values or the PFD value (probability of dangerous failure on demand) and the SFF value (safe failure fraction) are predominantly required. Further figures are required for assessment of the individual components. For a short explanation, refer to the table below.

Table 1: Abbreviations of safety-related figures

Figure	Full expression	Description
λ_S	Lambda S afe	Number of safe failures.
λ_D	Lambda D angerous	Number of dangerous failures.
λ_{DU}	Lambda D angerous U ndetected	Number of undetected dangerous failures.
λ_{DD}	Lambda D angerous D etected	Number of detected dangerous failures.
DC	D iagnostic C overage	Diagnostic Coverage – Ratio between the failure rate of dangerous failures detected by diagnostic tests and total rate of dangerous failures of the component or subsystem. The diagnostic coverage does not include any failures detected during proof tests.
MTBF	M ean T ime B etween F ailures	Mean time between the occurrence of two subsequent failures
SFF	S afe F ailure F raction	Fraction of safe failures as well as of detectable dangerous failures
PFD _{avg}	Average P robability of dangerous F ailure on D emand	Average probability of dangerous failures of a safety function on demand
HFT	H ardware F ault T olerance	Ability of a functional unit to execute a required function while faults or deviations are present. HFT = n means that the function can still be safely executed for up to n faults occurring at the same time.
T _{proof}	Proof test interval	Interval for proof test

SIL Safety integrity level

The international standard IEC 61508 defines four levels (SIL 1 to SIL 4).

Safety function Function to be implemented by a SIS or safety-related system for risk reduction with the objective to achieve or maintain a safe state for the plant/equipment with respect to a specific dangerous event.

Safety instrumented function (SIF) Function to be implemented by a SIS for risk reduction with the objective to achieve or maintain a safe state for the plant/equipment with respect to a specific dangerous event.

Safety instrumented system (SIS) Safety instrumented system for executing a single or several safety instrumented functions. An SIS consists of sensor(s), logic system and actuator(s).

Safety-related system A safety-related system includes all factors (hardware, software, human factors) necessary to implement one or several safety functions. Consequently, failures of safety function would result in a significant increase in safety risks for people and/or the environment.

A safety-related system can comprise stand-alone systems dedicated to performing a particular safety function or can be integrated into a plant.

Proof test Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition.

MTTR (Mean Time To Restoration)	Mean time to restoration once a failure has occurred. Indicates the expected mean time to achieve restoration of the system. It is therefore an important parameter for system availability. The time for detecting the failure, planning tasks as well as operating resources is also included. It should be reduced to a minimum.
MRT (Mean Repair Time)	Mean repair time indicates the mean time required to repair a system. The MRT is crucial when defining the reliability and availability of a system. The MRT should preferably be small.
Device type (type A and type B)	A component can be regarded as a type A device if all of the following conditions are met for all components required to achieve the safety instrumented function: • The failure modes for all constituent components involved are well defined. • The behaviour under fault conditions can be completely determined. • There is sufficient dependable failure data from the field to show that the claimed rates of failure are met (confidence level min. 70 %). A component must be regarded as a type B device, if one or several of the following conditions apply: • The failure of at least one constituent component is not well defined. • The behaviour under fault conditions is not completely known. • There is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.
PTC (Proof Test Coverage)	Proof test coverage describes the fraction of failures which can be detected by means of a proof test.

2 Application and validity

2.1 Range of application

AUMA actuators and actuator controls in SIL version, with the safety functions mentioned in this manual, are intended for operation of industrial valves and are suitable for use in safety instrumented systems in accordance with IEC 61508 or IEC 61511.

2.2 Standards

Both actuators and actuator controls meet the following requirements:

- IEC 61508 ED.2: Functional safety of electrical/electronic/programmable electronic safety-related systems

2.3 Valid device types

Table 2: Overview on suitable device types

Type		Power supply
Actuator	Actuator controls	Motor
SA 07.2 – SA 16.2	AC 01.2 in SIL version	3-phase AC
SAR 07.2 – SAR 16.2	AC 01.2 in SIL version	3-phase AC
SAEx 07.2 – SAEx 16.2	ACExC 01.2 in SIL version	3-phase AC
SAREx 07.2 – SAREx 16.2	ACExC 01.2 in SIL version	3-phase AC

Hardware, software and configuration of actuator and actuator controls must not be modified without prior written consent by AUMA. Unauthorised modifications may have a negative impact on both safety figures and SIL capability of the products.



In applications with requirements on functional safety, only AUMA actuator controls and actuators in SFC or SIL version may be used.

AUMA actuator controls and actuators in SIL version can among others be identified by the letters “SIL” on the name plate.

Figure 1: Example of AC name plate with “SIL” marking

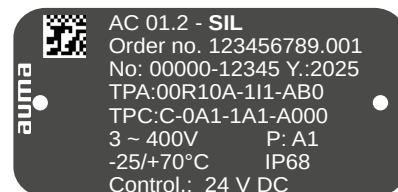


Figure 2: Example of SA name plate with “SIL” marking



3 Architecture, configuration and applications

3.1 Architecture (actuator sizing)

For actuator architecture (actuator sizing) the maximum torques, run torques and operating times are taken into consideration.

NOTICE

Incorrect actuator architecture can lead to device damage within the safety-related system!

Possible consequences are for example: Valve damage, motor overheating, contactor seizure, damage to the electronics, heating up or damage to cables.

- It is imperative to observe the actuator technical data when selecting the actuator.
- Sufficient reserves have to be provided to ensure that actuators are capable of reliably opening or closing the valve even in the event of an accident or under-voltage.

Architecture when using the Safe STOP function

For the Safe STOP function, the motor is switched off, overrun may possibly occur!

NOTICE

Valve damage due to overrun!

- For the Safe STOP function, the overrun of the arrangement (actuator, gearbox, valve) and the reaction time have to be observed.
- If the application requires self-locking of the actuator, please consult AUMA.

Architecture when using the Safe ESD function

Actuators with electromechanical control unit:

The end position feedback (limit switching) and the torque signal of the electromechanical control unit are safe signals, which can be integrated into a safety-related system if they are directly wired to the XK customer output of the actuator controls. However, this signal is not part of the certification by TÜV Nord. Please refer to the specific safety manual for details regarding this signal.

For “SIL seating” = “No seating” (without end position protection), we recommend:

- To prevent valve damage during safety operation, we recommend, depending on the stiffness, sizing the valve to 3 – 5 times the maximum actuator torque.
- To avoid thermal damage due to excessive currents, we recommend monitoring (assessing) the motor protection.

Actuators with electronic control unit MWG:



The end position feedback (limit switching) and the torque signal of the electronic control unit MWG as well as all signals via the standard I/O interface and the field-bus interfaces are no safe signals.

- Should safe signals be required, they have to be implemented differently, e.g. via switches on the valve.
- To prevent valve damage during safety operation, we recommend, depending on the stiffness, sizing the valve to 3 – 5 times the maximum actuator torque.
- To avoid thermal damage due to excessive currents, we recommend monitoring (assessing) the motor protection.

Actuators with electronic control unit MWG including limit switches:



In this version, safe signalling can exclusively be ensured via limit switches if they are directly wired to the XK customer output of the actuator controls. However, this signal is not part of the certification by TÜV Nord. Please refer to the specific safety manual for details regarding this signal.

For “SIL seating” = “No seating” (without end position protection), we recommend:

- To prevent valve damage during safety operation, we recommend, depending on the stiffness, sizing the valve to 3 – 5 times the maximum actuator torque.
- To avoid thermal damage due to excessive currents, we recommend monitoring (assessing) the motor protection.



For the “SIL seating” = “Forced limit seating in end position” configuration, the seating is performed via limit switches in the end position. Since each switch has a hysteresis, the actuator leaves the end position prior to limit switch release. Consequently, there is a marginal range of actuator positions to the safety position, for which the limit switch is still operated when leaving the safety position and for which the Safe ESD function is therefore NOT available. In this case, safety function triggering leads to actuator standstill. If the range in question is approached from the opposite direction, this limitation does not apply. In general, this range is relatively small. However, for unfavourable configurations (low number of turns per stroke), this range can amount to more than 10 % of the total stroke.

Should, within the framework of unfavourable conditions, the effect described above represent an unacceptable limitation for the safety function, we recommend applying the configuration “Forced torque seating in end position” or “no seating” for safety operation.

Power supply

The plant operator is responsible for ensuring the power supply.

3.2 Configuration (setting)/version

Configuration (setting) of safety-related functions is defined in the factory during actuator controls assembly and validated during final inspection. Subsequent modification of the configuration by the plant operator is not permissible.

General functions are set as described in the operation instructions or the Manual (Operation and setting) Actuator controls AC 01.2/ACExC 01.2.

Configuration of safety-related functions is listed in the order-related technical data sheet.



If limit and/or torque switches for the end positions are available, precise setting is imperative to ensure correct function of the “Safe end position feedback” or the “ESD function”. For setting details related to the respective switches, please refer to operation instructions.



For high output speeds > 63 rpm allow for longer overrun of the actuator after seating in end position. If the following conditions - torque seating, - very rigid valve and- speed > 63 rpm occur at the same time, the actuator might run too “hard” into the end stop which might lead to damage.

The respective combinations should be avoided if possible. When using a GS

gearbox at speeds > 63 rpm and “torque seating”, it must be ensured that the end stop of the GS gearbox is not approached by the seating is due to the torque applied at the valve.

Configuration options for safety function

Table 3: Configuration options for safety function

Configuration SIL function	Short description
Safe ESD CLOSE/CLOSE	Safe CLOSING
Safe ESD OPEN/OPEN	Safe OPENING
Safe STOP CLOSE/OPEN	Safe STOP in direction CLOSE and direction OPEN
Safe ESD CLOSE/CLOSE + Safe STOP CLOSE/OPEN	Safe CLOSING and safe STOP in direction CLOSE and direction OPEN
Safe ESD OPEN/OPEN + Safe STOP CLOSE/OPEN	Safe OPENING and safe STOP in direction CLOSE and direction OPEN

When configuring a Safe ESD function and a Safe STOP function, the Safe ESD function is always prioritised compared to the Safe STOP function when requested simultaneously.

Seating configuration options



The type of seating of the actuator controls in standard version should be configured as follows:

Table 4: Configuration options of the type of seating for actuators with electromechanical control unit

Configuration SIL seating type	Short description	Configuration Type of seating Actuator controls in standard version
1: No seating	No seating by limit or torque switches during safety operation	Freely selectable
2: Forced torque seating in end position	Safety operation is stopped by simultaneous tripping of limit and torque switches.	Torque seating
3: Forced limit seating in end position	Safety operation is stopped by limit switch tripping	Limit seating
4: Limit seating with overload protection	Safety operation is stopped by tripping the limit switches and/or the torque switches (overload protection).	Limit seating

Table 5: Configuration options of the type of seating for actuators with electronic control unit

Configuration SIL seating type	Short description	Configuration Type of seating Actuator controls in standard version
1: No seating	No seating by limit or torque switches during safety operation	Freely selectable

Table 6: Configuration options of the type of seating for actuators with electronic control unit MWG including limit switches

Configuration SIL seating type	Short description	Configuration Type of seating Actuator controls in standard version
3: Forced limit seating in end position	Safety operation is stopped by limit switch tripping	Limit seating

Configuration options for motor protection assessment

Table 7: Configuration options for motor protection assessment

Configuration SIL motor protection	Short description
Active	Tripping of the motor protection (thermal fault) stops or prevents safety operation.
inactive	Motor protection has no impact on the safety operation



“SIL motor protection” = “inactive” configuration is only set if explicitly required. The version does not meet the Ex approval requirements.

Configuration of “reaction monitoring” diagnostics and “Partial Valve Stroke Test (PVST)”

Depending on the type of diagnostics specified, the reaction monitoring via blinker transmitter or Partial Valve Stroke Test (PVST) configurations have to be checked and adapted, if required.

For detailed configuration options as well as detailed information on the Partial Valve Stroke Test (PVST), refer to Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls. Please note that reaction monitoring may only be executed via the blinker transmitter/SIL fault signal and not via the reaction monitoring function of the AC .2 firmware.

3.3 Protection against uncontrolled operation (self-locking/brake)

For self-locking AUMA actuators, it can be assumed that a load up to maximum torque will not result in uncontrolled valve operation from standstill due to valve torque load. Consequently, in these cases, further protection against uncontrolled operation is not imperatively required. This might become necessary if, for example, self-locking can either not be guaranteed, e.g. due to vibration or if it is insufficient. In addition, certain applications may require active position locking, for example by using a brake. There are user-specific standards demanding this type of protection. Therefore, each project must be subject to individual verification if any further protection is required. In any case, this protection is required for actuators without self-locking.

Table 8: Overview of self-locking for AUMA actuators (at the time of printing of this document)

Type	Output speed		Self-locking
	50 Hz	60 Hz	
SA 07.2 – SA 16.2	≤ 90 rpm	≤ 108 rpm	Self-locking
SAR 07.2 – SAR 16.2	≥ 125 rpm	≥ 150 rpm	NOT self-locking
SAEx 07.2 – SAEx 16.2			
SAREx 07.2 – SAREx 16.2			

If actuators with insufficient self-locking function paired with seating type “Forced torque seating in end position” are used for the safety function, the following effect might occur: During ESD, the actuator operates to the end position and switches off due to reaching the end position and the tripping torque. Thereafter, the gear train is relieved and the torque falls below the preset limit value. As a matter of fact, the actuator – correctly – detects this behaviour as termination of the ESD conditions and switches the actuator on again. The latter generates additional torque until the switching off condition is reached again, and so on. The “pumping effect” of the actuator is the consequence.

To avoid this effect, we recommend either selecting actuators or other elements with sufficient self-locking within the gear train or – if possible from a process and safety point of view – selecting “Forced limit seating in end position” as safety function.

3.4 Operation mode (low/high demand mode)

The safety functions of the actuators supplied by AUMA are suitable for the low demand mode and may only be used in this operation mode. If a non-safety instrumented function of the basic process control system is executed in addition to the safety function via the same actuator, note that while considering the sum of operational function, required tests and safety function, the defined number of maximum permissible starts¹⁾ as well as the maximum number of starts²⁾ for the respective actuator may not be exceeded during deployment of the actuator within a safety instrumented system.

3.5 Further notes and indications on architecture

HFT is 0.

The systematic capability is 3 (SC = 3).

Only flanges of F07 or FA 07 sizes or larger may be used for valve attachment.

If the actuator is equipped with one of the three position transmitter types, i.e. MWG, RWG or EWG, these elements may not be integrated within the safety instrumented system.

The actuator safety functions can be considered as type A device.

The operating time for a complete stroke must exceed 4 seconds. CAUTION: Any modification of the nominal stroke results in operating time change.

Safety function(s) and their feedback signals may only be issued via the digital inputs and outputs of the SIL module.

The signal issued via the `SIL-Fehler/Failure` output must be continuously evaluated. If the output signals a fault, assumption can be made that the safety function is not available. In this case, the safety function must be checked without delay. Possibly further safety measures are to be taken to restore the safety function without fault.

3.6 Applications (environmental conditions)

When specifying and using the actuators within safety instrumented systems, make sure that the permissible service conditions and the EMC requirements by the peripheral devices are met. Service conditions are indicated in the technical data sheet:

- Enclosure protection
- Corrosion protection
- Ambient temperature
- Vibration resistance

If the actual ambient temperatures exceed an average of +40 °C, the lambda values have to be incremented by a safety factor.

For an average temperature of +60 °C, this factor is specified to 2.5.

In case of direct, intensive exposure to sun, the resulting excessive temperature on the actuator surface has to be considered when determining the effective ambient temperature. As an alternative, appropriate countermeasures can be taken (e.g. a sunshade).

For environmental tests, actuator and actuator controls were subjected to the following standards:

- Dry heat: EN 60068-2-2
- Damp heat: EN 60068-2-30
- Cold: EN 60068-2-1
- Vibration (sinusoidal): IEC 60068-2-6

1) Definition of "cycles" according to EN 15714-2:2010

2) Definition of "starts" according to EN 15714-2:2010

- Induced seismic vibration (earthquake): IEC 60068-3-3³⁾
- Enclosure protection test: EN 60529
- Salt spray test: EN ISO 12944-6
- Immunity level: EN 61326-3-1
- Emission: EN 61000-6-4

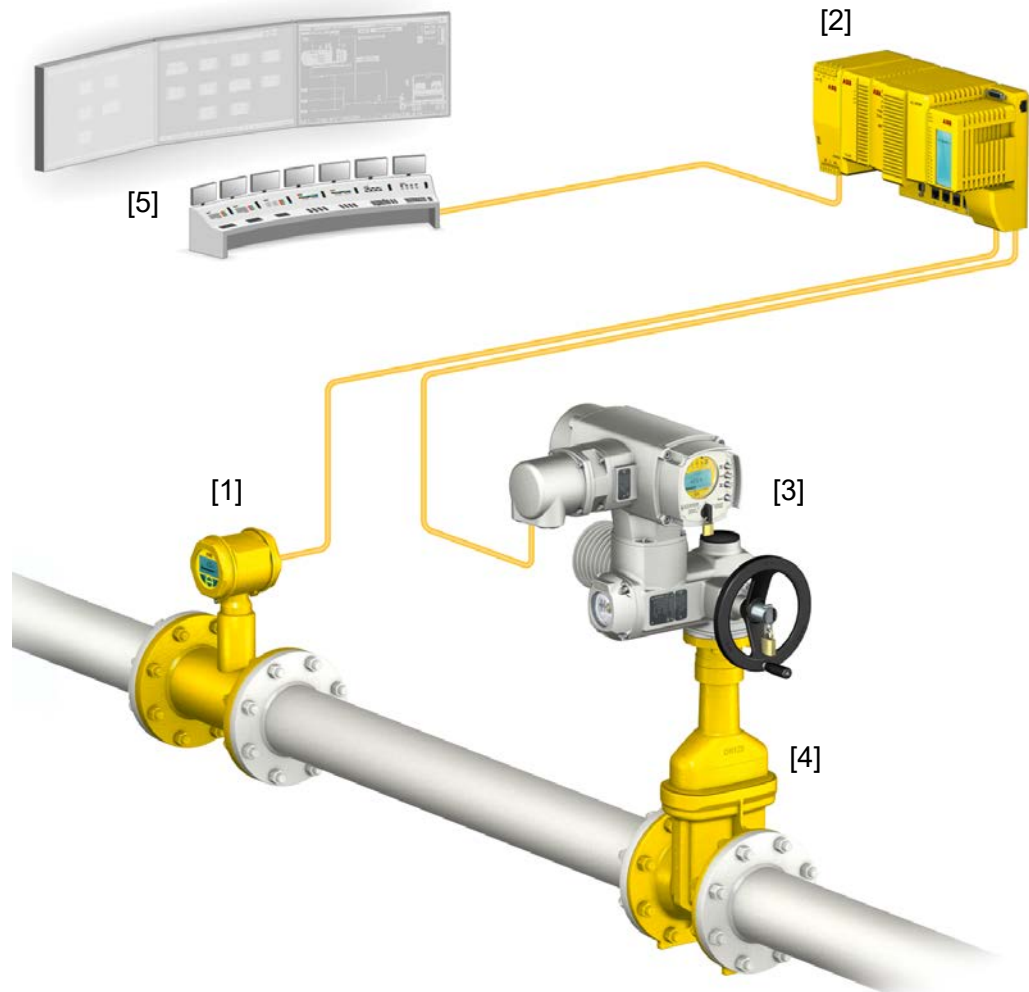
3) Thyristor version only

4 Safety instrumented systems and safety functions

4.1 Safety instrumented system including an actuator

Typically, a safety instrumented system including an actuator is composed of the components as shown in the figure.

Figure 3: Typical safety instrumented system



- | | | | |
|-----|---------------------------------|-----|-----------------------|
| [1] | Sensor | [2] | Controls (safety PLC) |
| [3] | Actuator with actuator controls | [4] | Valve |
| [5] | DCS | | |

The safety integrity level is always assigned to an overall safety instrumented system and not to an individual component.

For individual components (e.g. an actuator), only one “SIL capability” (e.g. SIL 2 capable) can be indicated. The final classification of the safety instrumented system can only be made after assessing and calculating the overall system.

4.2 Safety functions

In calculating the safety figures of the actuator system, the following safety functions are taken into account:

- Safe ESD function (**E**mergency **S**hut **D**own): Safe OPENING/CLOSING
 - Redundant Safe ESDa and Safe ESDb signals (default: low active) make the actuator run into the configured direction (OPEN/CLOSE), irrespective of the selector switch position.

- Safe STOP function: safe STOP
 - An operation command of actuator controls in standard version (in directions OPEN or CLOSE) will only be executed if an additional enable signal for the operation command is present.
 - If this is not the case, operation in directions OPEN or CLOSE is stopped or even suspended (motor is switched off).
 - If the enable signal is missing in both directions (Safe STOP AUF/OPEN and Safe STOP ZU/CLOSE to 0 V DC), the operation commands of the actuator controls in standard version will be stopped or prevented in both directions.
 - If the enable signal is missing in only one of the two directions (e.g. Safe STOP AUF/OPEN to 0 V DC and Safe STOP ZU/CLOSE to 24 V DC), the operation commands of the actuator controls in standard version will be stopped or prevented in this direction (in our example in direction OPEN). In the other direction (in our example direction CLOSE), operation via standard operation commands is possible in push-to-run operation. Operation with self-retaining is not possible in this direction.
 - The Safe STOP function is effective for all operation commands of the actuator controls in standard version, irrespective of the command source (e.g. Remote or Local).
- Safe ESD function combined with Safe STOP function
 - Safe ESD function has a higher priority i.e. if both functions are activated, the actuator is operated into the configured direction (OPEN/CLOSE).



The safety functions of the AC .2-SIL / ACExC .2-SIL are always controlled via 24 V DC.

“Safe end position feedback” is not part of the certification by TÜV Nord and neither part of this safety manual. Please refer to the specific safety manual for details regarding this function.

The different configuration options of the safety functions are described in the [Configuration \(setting\)/version \[► 9\]](#) chapter.

4.3 Safe inputs and outputs

Safe inputs for safe OPENING/CLOSING (Safe ESD function):

- Safe ESDa
- Safe ESDb

Safe inputs for safe stop (Safe STOP function):

- Safe STOP AUF/OPEN
- Safe STOP ZU/CLOSE

Safe outputs (indication that it might not be possible to perform the safety function):

- SIL-Fehler/Failure
- SIL-Bereit/Ready

For further information on the safe inputs and output refer to [Configuration \(setting\)/version \[► 9\]](#) and [Installation \[► 19\]](#) chapters.

4.4 Redundant system architecture

Besides the already described typical safety instrumented system including an actuator, safety can be increased by implementing a second, redundant valve and actuator with actuator controls in SIL version into the safety instrumented system. The decision on the appropriate version depends on the entire system.



Depending on the safety function and the safety instrumented task of this safety function, it must be verified for each and every application whether and - if so - in which configuration a $HFT > 0$ can be actually achieved when using several actuators. This applies in particular – but is not limited to – the Safe STOP safety function.

A possible example of Safe CLOSING shows [Figure 4: \[▶ 16\]](#). A possible example of Safe OPENING shows [Figure 5: \[▶ 16\]](#).

Another example, in which several actuators do NOT achieve redundancy, is a Safe STOP function used to safely exclude the movement of mechanical system parts, if, for example, the plant section in question has to be accessed in case of an emergency. For this application, use of two actuators does generally not result in a 1oo2 but in a 2oo2 system in terms of safety effect to be achieved. Therefore, the HFT is not increased in this case.

Figure 4: Redundant system with Safe ESD for Safe CLOSING



Figure 5: Redundant system with Safe ESD for Safe OPENING

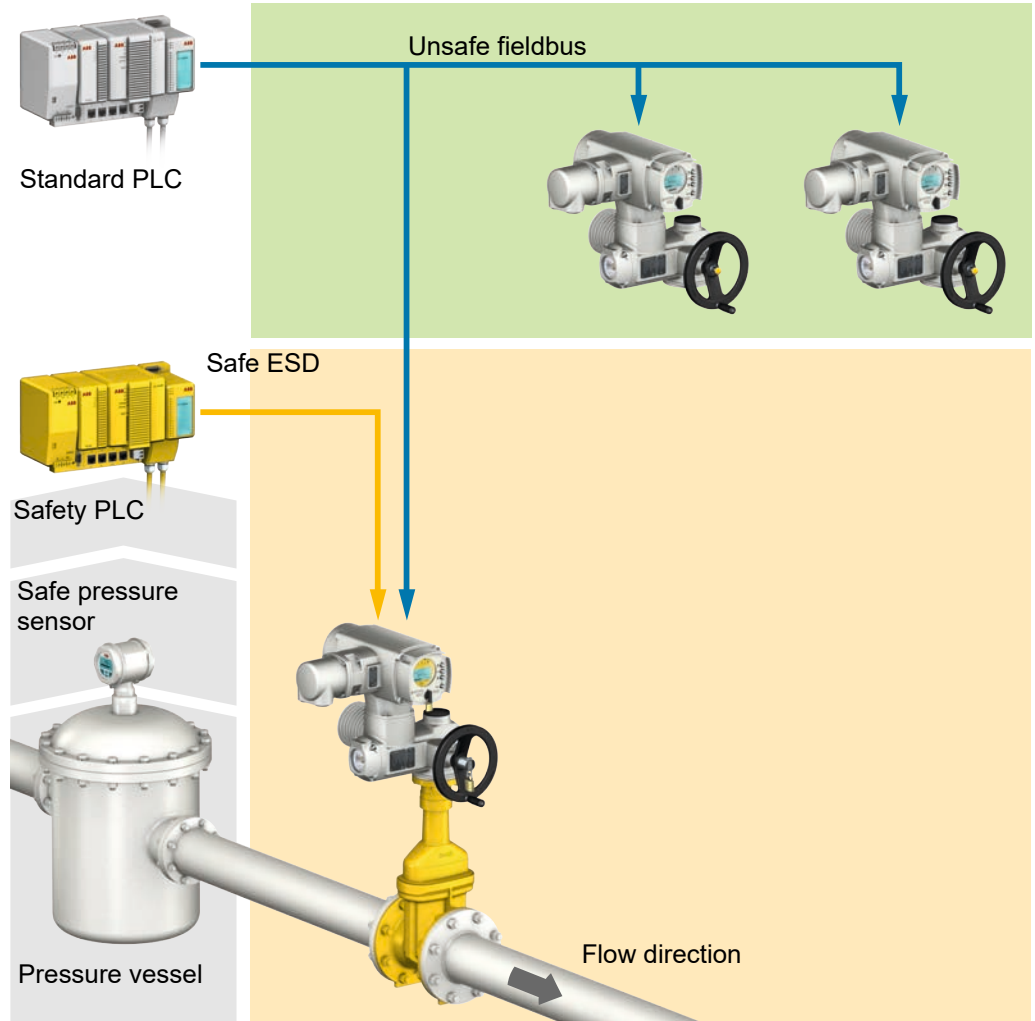


4.5 Examples of applications

Safe opening of a pressure vessel using the Safe ESD function

The standard PLC controls the entire system. A system fault occurs if excessive pressure is generated within the system. In this case, the safety PLC immediately opens the valve for safe pressure reduction.

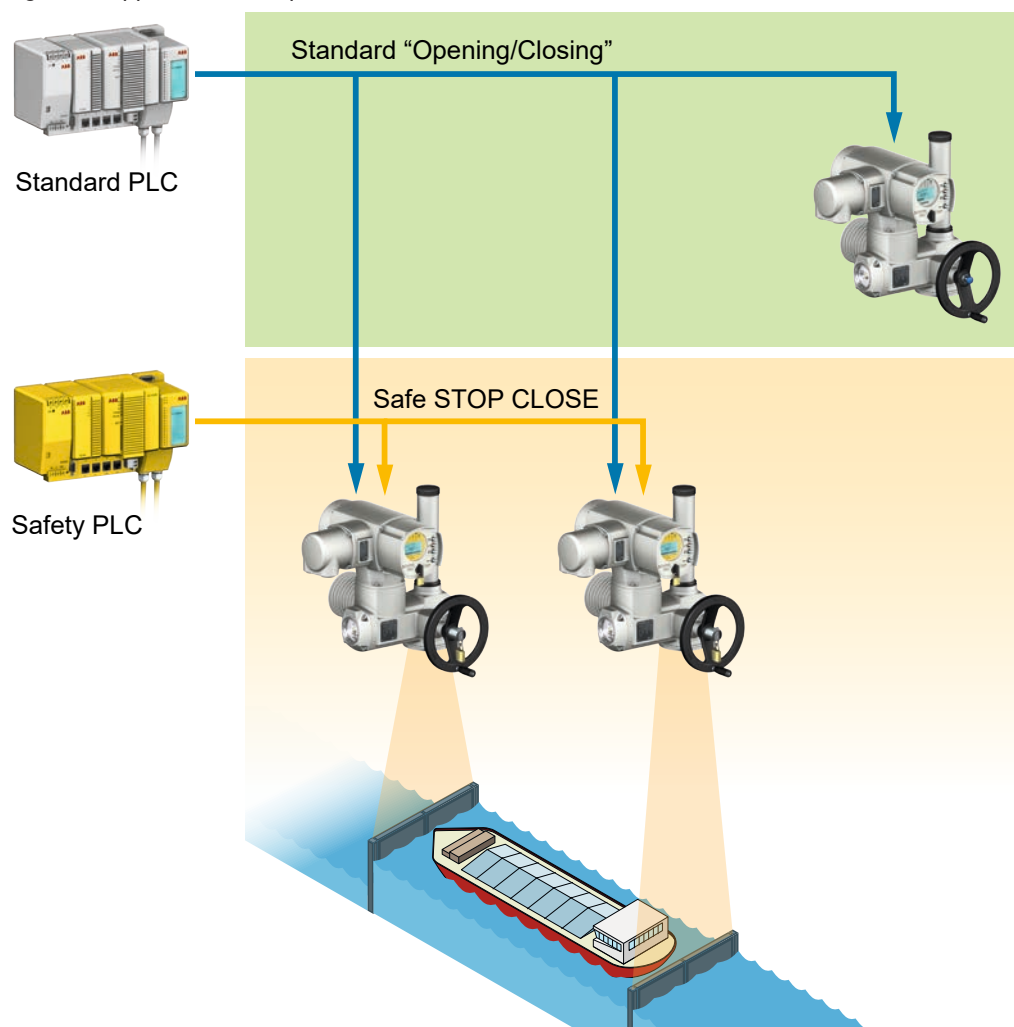
Figure 6: Application example: Pressure vessel



Safe stop of locks to prevent destruction using the Safe STOP function.

In case of navigation locks, operational safety ranks first (prevention of risks to humans and systems). Once the lock closes, no boats must be between the gates. Otherwise the Safe STOP function (e.g. via EMERGENCY STOP button) will be executed.

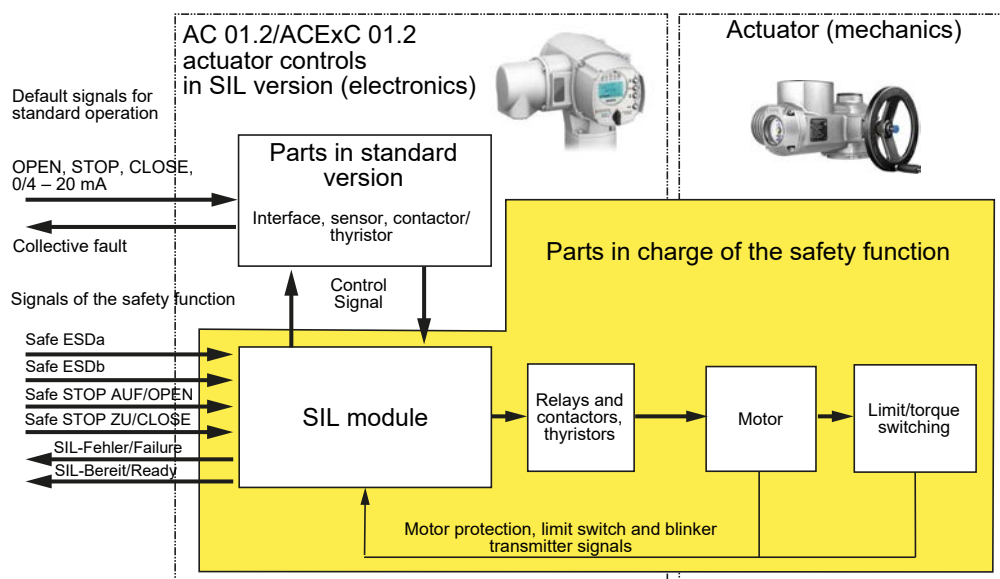
Figure 7: Application example: Lock



4.6 System representation

The following illustration shows a simplified layout of an AC 01.2/ACExC 01.2 in SIL version.

Figure 8: Simplified system representation



5 Installation, commissioning and operation



Installation and commissioning have to be documented by means of an assembly report and an inspection certificate. Installation and commissioning may only be performed by authorised personnel who have been trained on functional safety.

The plant operator is responsible for ensuring power supply including overvoltage and undervoltage protection during execution of a safety function.

5.1 Installation



The PIN assignments (XK ...) mentioned in this chapter (and also in other chapters) are considered as standard assignments of AC 01.2-SIL/ACExC 01.2-SIL. In certain configurations, this typical assignment is not respected with the objective to meet specific equipment demands. In case of doubt, the assignment as indicated on the pertaining wiring diagram is applicable.

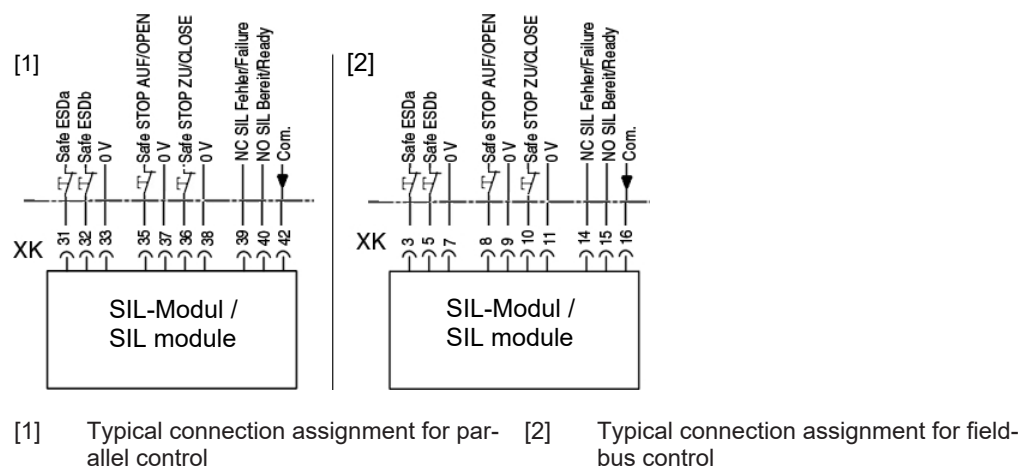
General installation tasks (assembly, electrical connection) have to be performed according to the operation instructions pertaining to the device and the enclosed order-specific wiring diagram.

When operating and storing the devices in ambient temperatures below $-25\text{ }^{\circ}\text{C}$, ensure power supply of integral heating system.

Safety functions are connected via the SIL module integrated in the AC 01.2/ACExC 01.2 actuator controls.

The SIL fault must be connected to an input compatible with the required SIL level of a safety PLC and subsequently analysed.

Figure 9: Connections for safety functions via SIL module



Switching behaviour of inputs:

Safe ESDa, Safe ESDb, Safe STOP AUF/OPEN, Safe STOP ZU/CLOSE

- Input signal = **high level** (default: +24 V DC)
 - = **No** safety operation for Safe ESD function or
 - = **No** safe stop for Safe STOP function
- Input signal = **low level** (0 V DC or input open)
 - = Safety operation for Safe ESD function or
 - = Safe stop for Safe STOP function



The **Safe ESDa** and **Safe ESDb** inputs are redundant inputs for the same safety function (depending on the configuration **ESD OPEN** or **ESD CLOSE**). Therefore, the same level (high level or low level) should be applied to them. If a high level is applied at one of the two **Safe ESDa** or **Safe ESDb** inputs and a low level at the other input, this presents a fault state of the safety instrumented system. In this instance, the actuator signals a “SIL fault”. Since it is not clear whether the high level input or the low level input is faulty, the safety function is performed for safety reasons.



The **Safe STOP AUF/OPEN** and **Safe STOP ZU/CLOSE** inputs are two independent inputs with independent functions:

- If **Safe STOP AUF/OPEN** = “low” level, the safety function inhibits operation in direction **OPEN** (exception **ESD OPEN**) as well as operations with self-retaining in direction **CLOSE**.
- If **Safe STOP ZU/CLOSE** = “low” level, the safety function inhibits operation in direction **CLOSE** (exception **ESD CLOSE**) as well as operations with self-retaining in direction **OPEN**.

For further information on the **Safe STOP** function, refer to the [Safety functions](#) [► 14] chapter.

Permissible input voltage range:

- High level: 15 ... 30 V DC
- Low level: maximum 5 V DC

Signalling behaviour of the outputs:

- SIL-Bereit/Ready**: Absence of fault to be detected by diagnostics:
NO (NO contact) output = **closed**
NC (NC contact) output = **open**
- SIL-Fehler/Failure**: Presence of fault to be detected by diagnostics:
NO (NO contact) output = **open**
NC (NC contact) output = **closed**

Table 9: Wiring diagram designations

Designation Wiring diagram	Signal	Customer connections for control (typical assignment)	
		[1] Parallel	[2] Fieldbus
Safe ESDa	Digital input for Safe ESD function	XK 31	XK 3
Safe ESDb	Redundant input for Safe ESD function	XK 32	XK 5
0 V	Common for Safe ESDa and Safe ESDb	XK 33	XK 7
Safe STOP ZU/ CLOSE	Digital input for Safe STOP function in direction CLOSE	XK 35	XK 8
0 V	Common for Safe STOP CLOSE	XK 37	XK 9
Safe STOP AUF/ OPEN	Digital input for Safe STOP function in direction OPEN	XK 36	XK 10
0 V	Common for Safe STOP OPEN	XK 38	XK 11
SIL-Bereit/Ready	NO contact of SIL fault signal	XK 40	XK 15
SIL-Fehler/Fail- ure	NC contact of SIL fault signal	XK 39	XK 14
Com.	Common for SIL fault signal	XK 42	XK 16

Table 10: SIL faults displayed via the **SIL-Fehler/Failure** output

Fault causes SIL	Description
Thermal fault	Motor protection tripped
Torque fault	Torque fault in directions OPEN and/or CLOSE
Fault position feedback	Current position feedback is outside permissible range.

Fault causes SIL	Description
Phase failure	One phase of power supply is missing. Controls are not supplied with mains voltage
Phase sequence fault	The phase conductors L1, L2 and L3 are connected in the wrong sequence.
Power supply failure	The safety-related part of controls is without power supply.
Temperature fault	Temperature within actuator controls housing too high. Failure of heating system for ambient temperatures below –25 °C
Failure of actuator monitoring	Actuator or valve locked
Fault in redundant wiring Safe ESD	Both signals Safe ESDa and Safe ESDb are not simultaneously on the same level.
Internal error	Internal error of the SIL module

For further information on SIL faults and in particular to assist in troubleshooting, refer to [Indications](#) ► [26](#) chapter.

Installation and commissioning must be recorded and a final installation and commissioning report must be issued.



The basic function "automatic correction of direction of rotation" is not available for this version. When connecting the power supply ensure that phases L1, L2 and L3 are correctly connected. For checking the direction of rotation, refer to operation instructions pertaining to the actuator.

The "external supply of electronics" option of the actuator controls refers to the part of actuator controls in standard version. In case of mains failure, the SIL module would no longer be operable despite external supply of the electronics.



Limit switch setting for version with electronic control unit and limit switches is slightly different from the standard setting for the electromechanical control unit. Refer to the supplement to operation instructions for correct setting (Y006.238 or PR00526).

5.2 Commissioning

The operation instructions pertaining to the device must be observed for general commissioning.



For the Safe ESD function, operation into the safe position can be performed irrespective of the selector switch position (LOCAL - OFF - REMOTE) or the operating status. This means, upon request of the safety function, the actuator will start operation even in positions LOCAL and OFF or on system start.

CAUTION

On delivery of the actuator, the motor is engaged and the handwheel activation (change-over between motor operation/manual operation) is locked via the handwheel locking device. Risk of immediate actuator operation when switching on if the Safe ESDa and Safe ESDb inputs are not supplied with +24 V DC!

Risk of personal injuries or damage to the valve.

→ Ensure that **high level** is present at the Safe ESDa/ESDb inputs when switching on (default: +24 V DC).

→ Observe warning sign within the electrical connection.

CAUTION

If the actuator is operated over a longer period (for several hours) while the motor is disengaged (e.g. white sleeve fitted in the locking device at the handwheel), this entails considerable wear of the actuator. Worst case would be accidental startup or even destruction of the actuator.

On delivery of the actuator, the motor is engaged (black sleeve fitted in the locking device at the handwheel). For certain actions, e.g. during the proof test, it might be necessary to lock the actuator while the handwheel is engaged (white sleeve fitted in the locking device at the handwheel).

If the actuator is connected to 3-phase AC current without high level present at the Safe ESDa/ESDb inputs (default: +24 V DC), the motor will start without any movement at the output drive.

- Operational actions have to be provided ensuring that the described state only persists for a short time, i.e. a few minutes at the maximum.
- The white sleeve in the handwheel locking device may only be used for a short time, e.g. during the proof test. It is imperative to remove the white sleeve prior to recommissioning the safety system.

After commissioning, the safe actuator function must be verified. Refer to [Proof test \(verification of safe actuator function\)](#) [► 31] chapter.

5.3 Operation

Regular maintenance and device checks in determined T_{proof} intervals are the basis for safe operation. The parameters indicated in the [Safety-related figures](#) [► 39] chapter are valid for $T_{\text{proof}} = 1$ year.

For operation, both the pertaining operation instructions and the Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls have to be observed.

In case of possible failures or defects of the safety system, the safe function must be guaranteed by introducing alternative actions. Furthermore, a detected fault including fault description has to be sent to AUMA Riester GmbH & Co. KG. Autonomous repair work by the plant operator is not permitted.

5.4 Lifetime

Actuator lifetime is described in the technical data sheets or the operation instructions.

The safety-related figures are valid for the cycles or modulating steps defined in the technical data specifications for typical periods of up to 10 years starting at the date of delivery (the criterion achieved first is valid). After this period, the probability of failure increases.

Extending this period is basically feasible in many cases provided both manufacturer and plant operator introduce respective actions in compliance with footnote N3 of NOTE 3 of the German version of IEC 61508-2:2010 7.4.9.5 b). This is the responsibility of the plant operator who will have to take appropriate and suitable measures. The minimum measures required for this are described in the [Maintenance](#) [► 38] chapter. The requirement of further measures must be assessed in individual cases and based on the conditions of application.

5.5 Decommissioning

When decommissioning an actuator with safety functions, the following must be observed:

- Impact of decommissioning on relevant devices, equipment or other work must be evaluated.
- Safety and warning instructions contained in the actuator operation instructions must be met.
- Decommissioning must be carried out exclusively by suitably qualified personnel.

- Decommissioning must be recorded in compliance with technical requirements. Notes regarding disposal are available in the operation instructions.

6 Indications on display

This section includes the indications of the actuator in standard version which are exclusively available in SIL version.

General indications as well as settings and operation are described in the pertaining operation instructions and in the Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls.



Indications on the display are not part of a safety function! They must not be integrated in a safety-related system!

The indications support the user on site at the device, making the safety function status easily discernible.

6.1 Status indications on SIL functions

Actuator controls may indicate status information on safety-related functions on the display.

SIL status (S0013)

Indication S0013 signals the safety function and the SIL fault indication status.

If the SIL symbol is shown in the header of the display, one of the following three indications is active: Safe ESD, Safe STOP or SIL fault.

Figure 10: Safety function and SIL fault indication status

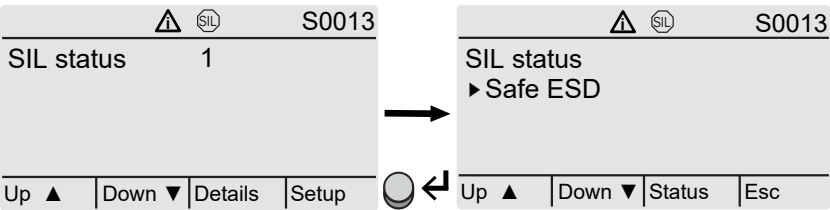


Table 11: Status of status indications on display

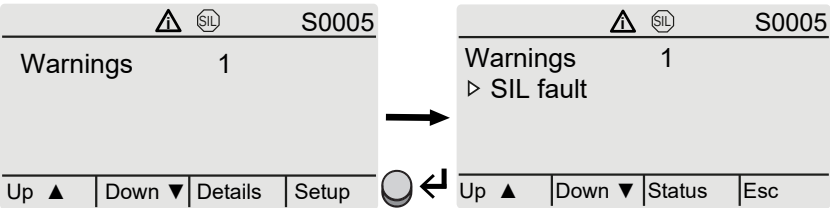
Status indications on display	Status
Safe ESD	Safe ESD function (safe OPENING/CLOSING) is active: Actuator is operated in the configured direction (CLOSE/OPEN) (Safe ESDa/Safe ESDb inputs = 0 V or open)
Safe STOP	Safe STOP function is active, actuator stops (Safe STOP AUF/OPEN or Safe STOP ZU/CLOSE input = 0 V or open)
SIL fault	SIL fault signal active, i.e. possible problems when executing a safety function (Safe ESD or Safe STOP).

Warnings (S0005)

Indication S0005 shows the numbers of warnings having occurred.

In case a SIL fault occurs, the SIL fault message is listed in S0005 indication. Further details are available under Details > Status.

Figure 11: Warning: SIL fault

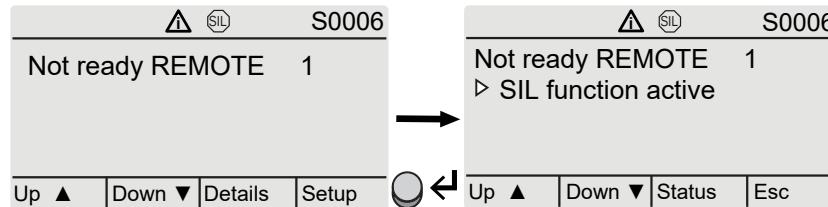


Not ready REMOTE (S0006)

Indication S0006 shows the number of occurring messages which are part of the Not ready REMOTE group.

If a safety function is active (Safe ESD or Safe STOP), the SIL function active signal is listed in the group Not ready REMOTE. Further details are available under **Details > Status**.

Figure 12: Signal: Safety function active



As soon as a safety function is active (SIL function active signal), the actuator is controlled via the safety PLC and the SIL module. For “standard control” (standard PLC), controls are therefore “Not ready REMOTE”.

6.2 SIL configuration warning

In combination with the safety functions, the following configurations or settings of the actuator controls in standard version may have an impact on the standard functions:

- Self-retaining Local M0076 = OPEN/CLOSE
- Self-retaining Remote M0100 = OPEN/CLOSE

If one of these configurations is selected in the actuator controls in standard version, the SIL config. warning is generated by the actuator controls up to firmware version 6.07.xx.

The different impact of the Safe STOP safety function on standard operation commands in push-to-run operation and with self-retaining is described in the [Safety functions \[► 14\]](#) chapter.

6.3 Backlight

In standard operation, display backlight of actuator controls is white. In the event of a fault, the display backlight is red. The red backlight does NOT refer to the safety function status but to the faults referred to as “faults” in the Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls.

7 Indications

7.1 Signals via SIL module

The integrated SIL module signals a SIL fault via an output contact (SIL-Bereit/Ready or SIL-Fehler/Failure). Only these signals may be used in a safety-related system.

For the signalling behaviour of the SIL-Bereit/Ready or SIL-Fehler/Failure outputs, refer to [Installation](#) [► 19] chapter.

Once a SIL fault occurs, the system has to be checked immediately and the installation has to be put in a safe state, if required.

7.2 SIL fault signal via the display of the actuator controls in standard version (for troubleshooting support)

If the SIL module output contact (SIL-Bereit/Ready or SIL-Fehler/Failure outputs) signals a SIL fault, the exact fault can be determined via the indication in the display of the actuator controls in standard version. For details on all fault indications and warning indications on the display of the actuator controls in standard version, refer to Manual (Operation and setting) AC 01.2/ACExC 01.2.

The SIL module output contact serves as collective signal for the faults listed in the table below.

Table 12: Individual signals of SIL fault collective signal

Indication on display Actuator controls in standard version	Description/ Cause of the fault	Impact on safety function → Remedy
Thermal fault	Motor protection tripped.	For “ SIL motor protection ” = active version: - The Safe ESD safety function cannot be executed. - If the fault is triggered during a safety operation, the operation is stopped. Remedy → Cool down, wait.
Torque fault CLOSE Torque fault OPEN	Torque fault in directions CLOSE or OPEN Torque fault in directions CLOSE and OPEN (simultaneously).	For “ SIL seating ” = “ Limit seating with overload protection ” configuration: - The Safe ESD safety function cannot be executed. - If the fault is triggered during a safety operation, the operation is stopped. - Once the cause for the torque fault has been remedied and the safety operation is still requested, the safety operation is immediately continued without manual reset. Remedy → Execute operation command in opposite direction. → Verify torque switching setting. → Check whether a foreign object prevents the valve from closing. → Possibly problems with the valve.
Wrn range act.pos.	The current signal range of the position feedback is outside the permissible range. Both limit switches (OPEN and CLOSED) are operated simultaneously. Possible defect at actuator mechanics.	For configurations “ SIL seating ” = “ Limit seating with overload protection ”, “ SIL seating ” = “ Forced limit seating in end position ”, or “ SIL seating ” = “ Forced torque seating in end position ”: - The Safe ESD safety function cannot be executed. - If the fault is triggered during a safety operation, the operation is stopped. Remedy → Verify reduction gearing settings within actuator. → In case of possible defect at the actuator: Contact AUMA service
Phase fault	One phase of power supply is missing. The actuator controls are not live.	- The Safe ESD safety function cannot be executed. - The Safe STOP safe function is indirectly executed as the motor is no longer supplied with power. Remedy → Test/connect phases.

Indication on display Actuator controls in standard version	Description/ Cause of the fault	Impact on safety function → Remedy
Incorrect phase seq	The phase conductors L1, L2 and L3 are connected in the wrong sequence.	In case of wrong phase sequence, the actuator is operated into the wrong direction during safety operation. Remedy → Correct the sequence of the phase conductors L1, L2 and L3 by exchanging two phases.
IE 24 V AC	Fault of internal 24 V AC power supply. The safety-related part of the actuator controls is without power supply.	- The Safe ESD safety function cannot be executed. - If the fault is triggered during a safety operation, the operation is stopped. - The Safe STOP safety function is indirectly executed as the SIL module is no longer supplied with power. Remedy → Check power supply.
Wrn controls temp.	Temperature within the actuator controls housing too high (outside the specified temperature range).	It might not be possible to execute the Safe ESD and Safe STOP safety functions. Remedy → Actuator controls must cool down (for display of the current temperature, check actuator controls under: Diagnostics M0022>Device temperatures M0524>Temp. controls). → Check service conditions.
No signal in display	Internal error SIL module electronics sub-assembly.	It might not be possible to execute the Safe ESD and Safe STOP safety functions. Remedy → Possible defect at SIL module: Contact AUMA service
	Actuator monitoring Actuator locked in handwheel operation. Possible defect at actuator.	The Safe ESD safety function can possibly not be executed. Remedy → In case of possible defect at the actuator: Contact AUMA service
	Fault of redundant wiring of Safe ESD input. Both signals, Safe ESDa and Safe ESDb, are not simultaneously on the same level.	The Safe ESD safety function can be executed. A SIL fault is displayed via the SIL-Fehler/Failure output. Remedy → Check redundant control of Safe ESD signals.

7.3 Status signals via output contacts (digital outputs) of actuator controls in standard version

Actuator controls offer the possibility of signalling status information on safety-related functions via output contacts (DOUT outputs).



Status signals via DOUT outputs are not part of a safety function! They may not be used instead of safety-relevant signals within a safety instrumented system! However, they can be used as additional information on the standard PLC, for example.



If digital inputs or outputs of actuator controls in standard version are connected to the safety PLC, imperatively ensure sufficient absence of interference of all non-safety-related system components with regard to the safety function. The absence of interference must be guaranteed even in case of standard component faults. For this, galvanic isolation between safety-related and non safety-related system components is important (but not necessarily sufficient).

Available signals:

Safe ESD
Safe STOP
SIL fault
SIL function active

Assignment via menu in the display:

Required user level: Specialist (4) or higher.

M▷ Device configuration M0053
I/O interface M0139
Digital outputs M0110

Default values:

Signal DOUT 5 = SIL function active

Signal DOUT 6 = SIL fault

7.4 Signals via fieldbus of actuator controls in standard version

For actuator controls in fieldbus interface version, status information on the safety-related functions is provided in the process representation.



Status signals via fieldbus are not part of a safety function! They must not be integrated in a safety-related system. They can be used as additional information on the standard PLC, for example.

The following signals are available in the process representation:

Safe ESD

Bit: Safe STOP

Bit: SIL fault

Bit: SIL function active

For further information on parameter configuration via fieldbus interface refer to Manual (Device integration Fieldbus).

8 Tests and maintenance

Inspection and maintenance tasks may only be performed by authorised personnel who have been trained on functional safety.

Test and maintenance equipment has to be calibrated.



Any execution of a test/maintenance must be recorded in a test/maintenance report.

Impact of testing/maintenance on relevant devices, equipment or other work must be evaluated.

8.1 Check safety equipment

All safety functions within a safety equipment must be checked for perfect functionality and safety at appropriate intervals. The intervals for safety equipment checks are to be defined by the plant operator.

The plant operator has to establish a safety schedule for the entire safety lifecycle of the SIS. It should include the strategy for achieving safety as well as different activities during the safety lifecycle.

8.2 Internal actuator monitoring of the device with control via actuator controls in standard version

The device, consisting of actuator with actuator controls and integral SIL module has an internal actuator monitoring. By controlling actuator controls/actuator in standard version via standard operation commands, internal actuator monitoring is automatically performed. Internal actuator monitoring identifies most of the safety-related actuator components. If a fault occurs, the fault would be signalled via the output contact of the SIL module (SIL Fehler/Failure).

To ensure the safety figures of the Safe ESD safety function, the device has to be controlled at least once per month via the standard controls, including output contact assessment of the SIL module (SIL-Fehler/Failure), as well as one of the AUMA **Faults** or NAMUR **Failure** signals via the standard part of the actuator controls. If it cannot be ensured that the equipment is controlled by the controls in standard version at least once per month, a [Partial Valve Stroke Test \(PVST\)](#) [► 29] has to be performed instead.

The control signal and the pertaining operation of the actuator have to be present for at least 4 seconds. If the control signal and pertaining operation of the actuator are present for at least 4 seconds without signalling a fault neither via the SIL output contact (SIL module: SIL-Fehler/Failure) nor via the AUMA **Faults** or the NAMUR **Failure** signals of the standard part of the actuator controls, the test is considered as successful. If this is not the case, the device has to be checked in accordance with the steps indicated in the [Proof test \(verification of safe actuator function\)](#) [► 31] chapter.

Other intervals can be selected for automated actuator monitoring.

The following should be observed In this case:

- The PFD values and all other safety figures affected by the diagnostic interval have to be recalculated. The respective values (refer to [Specific figures for AC 01.2 actuator controls in SIL version with actuators of SA .2 series](#) [► 40]) are not valid.
- Automated diagnostics should be performed at least 10 times more often than the proof test.
- Automated diagnostics should be performed at least 10 times more often than the demand rate of safety function.

8.3 Execute Partial Valve Stroke Test (PVST)

— Option —

There are two options for executing the PVST.

1. Executing the PVST using safe `Safe ESDa` and `Safe ESDb` inputs:
 The PVST must be controlled by the external safety PLC. Control is made via the safety PLC via the safe inputs, `Safe ESDa` and `Safe ESDb`. Desired diagnostics is performed by evaluating the SIL output contact (SIL module: `SIL-Fehler/Failure`). Both control signals and related actuator operation have to be present for at least 4 seconds.
 If the control signal and pertaining operation of the actuator are present for at least 4 seconds without signalling a fault neither via the SIL output contact (SIL module: `SIL-Fehler/Failure`) nor via the AUMA `Faults` or NAMUR `Failure` signals of the standard part of the actuator controls, the test is considered as successful. If this is not the case, the device has to be checked in accordance with the steps indicated in the [Proof test \(verification of safe actuator function\) \[► 31\]](#) chapter.
2. Executing the PVST using the PVST function of AC .2:
 If the AC .2 actuator controls in standard version are configured with PVST input, this input can be used for diagnostics of the safety-relevant part of actuator controls under certain conditions.
 Conditions and required settings:
 - Additional non-interacting end position switches for safe and reliable end position feedback signals are available and wired to the safety PLC.
 - A digital input of actuator controls in standard version (galvanically separated from the other inputs) is configured to the following value: `Execute PVST` (949), or PVST control via an available fieldbus interface.
 - The safety PLC directly controls the PVST or will also receive the control signal if the PVST input is controlled.
 - The PVST is executed with the following operation mode setting: Parameter `PVST operation mode` [M0889] = `End position test`
 - The PVST may only be executed from one of the end positions.
 - Parameter `PVST operating time` [M0890] must be > 4 seconds.
 - The `PVST fault` (953) and `PVST abort` signals (954), as well as one of the AUMA `Faults` or NAMUR `Failure` signals of the actuator controls in standard version are signalled via digital outputs of the actuator controls in standard version or when using a fieldbus interface by the BPCS-PLC to the safety PLC. For this, imperatively apply appropriate measures to ensure the absence of interference to the safety instrumented system (safety PLC).

PVST is either directly requested at the PVST input of the actuator controls in standard version by the safety PLC or the signal for requesting the PVST is also sent to the safety PLC. While the AC .2 actuator controls in standard version perform the PVST, the safety PLC monitors whether

- the actuator was in one of the end positions prior to the PVST (check via safe end position feedback).
- the actuator left one of the end positions within the set PVST operation time (check via safe end position feedback).
- the actuator has returned to the correct end position after completing the PVST (check via safe end position feedback).
- if a fault was signalled during PVST operation time via the SIL output contact (SIL module: `SIL-Fehler/Failure`).

Only if the actuator was in one of the end positions prior to the PVST, has left this end position during the PVST, the actuator controls in standard version has no `PVST fault` (953), no `PVST abort` (954), no AUMA `Faults` or no NAMUR `Failure` signal, as well as no `SIL fault` signalled by the SIL module, the PVST was successful. If this is not the case, the device has to be checked in accordance with the steps indicated in the [Proof test \(verification of safe actuator function\) \[► 31\]](#) chapter.

Note: “Safe end position feedback” includes the end position switches which are directly wired to the customer output and assessed by AUMA within the framework of a Declaration of Incorporation for functional safety (SFC). These switches are not part of the TÜV certification. Contrary to the outputs of the actuator controls in standard version, they can be integrated within the safety instrumented system.



If digital inputs or outputs of actuator controls in standard version are connected to the safety PLC, imperatively ensure sufficient absence of interference of all non-safety-related system components with regard to the safety function. The absence of interference must be guaranteed even in case of standard component faults. For this, galvanic isolation between safety-related and non safety-related system components is important (but not necessarily sufficient).

Performing a PVST includes diagnostics of the safety-related components. This ensures improved safety figures compared to applications without or with minor diagnostics.

8.4 Proof test (verification of safe actuator function)

The proof test serves the purpose of verifying the safety-related functions of the actuator and actuator controls.

Proof tests shall reveal dangerous failures which might remain undetected until a safety function is started and consequently result in a potential danger.



During execution of the proof test, the safety function is unavailable for a short time.

Depending on both version and configuration, the proof test includes the following tests:

1. Check Safe ESD safety operation (Safe OPENING/CLOSING).
2. Check “Actuator monitoring” SIL fault signal.
3. Check Safe ESD reaction for “Motor protection (thermal fault)” signals.
4. Check Safe ESD reaction to “Limit seating with overload protection” (limit and/or torque evaluation).
5. Check Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electromechanical control unit.
6. Check Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electronic control unit and limit switches.
7. Check Safe ESD reaction to “Forced torque seating in end position” (torque after limit evaluation).
8. Check Safe ESD reaction for “no seating” (no evaluation of limit and torque).
9. Check Safe STOP function.
10. Check combination of Safe ESD and Safe STOP function.

The safety-related signal input is appropriately assigned to check the safety-related function. As a consequence, the actuator has to perform the safety function. For a detailed description on the execution of the proof test steps, refer to the following sections and the checklists in the [Proof test checklists \[► 44\]](#) chapter.

Intervals:

A proof test interval describes the time between two proof tests. Functionality must be checked at appropriate intervals. The intervals are to be defined by the plant operator. The probability of failure on demand (PFD) of the safety function depends on the selected proof test interval; in our example, it is valid for $T_{\text{proof}} = 1$ year (refer to [Safety-related figures \[► 39\]](#) chapter).

In any case, the safety-related functions must be checked after commissioning and following any maintenance work or repair as well as at the T_{proof} intervals defined in the safety assessment.

If a fault occurs during proof test, safe function has to be ensured introducing alternative actions. Please contact AUMA Riester GmbH & Co. KG.

The type of proof test to be performed depends on version and configuration of the product. Only the tests applicable have to be performed.



If the safety function has been configured as ESD CLOSE/CLOSE + Safe STOP OPEN/CLOSE or as ESD OPEN/OPEN + Safe STOP OPEN/CLOSE, all relevant tests for Safe ESD and for Safe STOP (as well as for the combination of Safe ESD and Safe STOP) must be executed.



Before starting the test, we recommend reading the respective test procedure at least once.

8.4.1 Preliminary test

As a first test step, the actuator system has to be subjected to a preliminary inspection according to the checklists in the [Proof test checklists \[► 44\]](#) chapter.

8.4.2 Check “Safe OPENING/CLOSING” Safe ESD safety operation

Configuration The test is valid for all versions with Safe ESD function (irrespective of the “SIL seating” configuration). The Safe ESD reaction to the different seating types is verified in separate tests.

Test procedure When switching the *Safe ESDa*/*Safe ESDb* inputs accordingly, safety operation into the configured direction must be triggered.

NOTICE

If “SIL seating” = “no seating” (without end position protection) is configured faulty operation during the test may result in damage to the elements within the safety-related system.

Possible consequences are for example: Valve damage, motor overheating, contactor seizure, defective thyristors, heating up or damage to cables.

- Check “SIL seating” before proof test configuration. The configured type of seating is indicated in the wiring diagram (page 2).
- For actuators with “SIL seating” = “no seating”: **Interrupt safety operation before reaching the end position** (Set *Safe ESDa*/*Safe ESDb* input signals to +24 V DC).
- For the test, the valve should either be in mid-position or at sufficient distance from the end positions.
- In case of damage, the actuator system has to be checked and repaired, if necessary.

Test sequence Refer to checklist in the [Safe ESD safety operation \(Safe OPENING/CLOSING\) – irrespective of the selected control unit \[► 44\]](#) chapter.

8.4.3 Check SIL fault signal “Actuator monitoring”

Configuration This test is required for the following versions or configurations:

- Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
- Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)

Test procedure	If the motor does not rotate within a defined time once safety operation was triggered, a SIL fault must be signalled.
Test sequence	Refer to checklist in the SIL fault signal "Actuator monitoring" – irrespective of the selected control unit [► 45] chapter.
Required material	For this inspection, a white sleeve for handwheel locking device is required (shown on the left). On delivery of the actuator, the sleeve is attached to the handwheel using a cable tie.

Figure 13: on the left: white sleeve, manual drive permanently engaged, on the right: black sleeve, motor operation permanently engaged

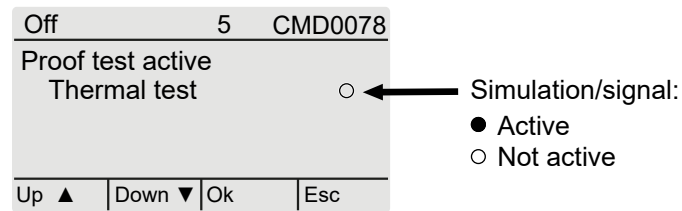


When fitted in the locking device at the handwheel, the white sleeve ensures a permanently engaged handwheel (= handwheel locking device). When fitted in the locking device at the handwheel, the black sleeve ensures a permanently engaged motor. If the white sleeve is fitted, motor operation and consequently executing the Safe ESD OPEN/CLOSE safety function is not possible. To be able to execute the Safe ESD OPEN/CLOSE safety function, the white sleeve has to be removed from the locking device.

8.4.4 Check Safe ESD reaction for "Motor protection (thermal fault)" signals

Configuration	This test is required for the following versions or configurations: • Safe ESD function "Safe CLOSING" (Safe ESD in direction CLOSE) • Safe ESD function "Safe OPENING" (Safe ESD in direction OPEN)
Test procedure	In order to protect against overheating and impermissibly high surface temperatures at the actuator, PTC thermistors or thermostats are embedded in the motor winding. Motor protection trips as soon as the max. permissible winding temperature has been reached. For a safety operation via Safe ESD function, the actuator reaction for motor protection tripping depends on the "SIL motor protection" configuration: • For "SIL motor protection" = active configuration = safety operation is stopped. • For "SIL motor protection" = inactive configuration = safety operation is not stopped. The test is performed by simulating the motor protection signal via AC 01.2 local controls: Required user level: Specialist (4) or higher. M► Diagnostics [M0022] Proof test (motor prot.) [M1021] Simulation value: Thermal test

Figure 14: Display indication on local controls



The simulation (active/inactive) is activated and deactivated by push button **Ok**.

A dot on the display indicates that the simulation is active.

Black dot (●): Motor protection simulation active (thermal fault)

White dot (○): Signal not active

Test sequence Refer to checklist in the [Safe ESD reaction for "Motor protection \(thermal fault\)" signals – irrespective of the selected control unit \[► 45\]](#) chapter.

8.4.5 Check Safe ESD reaction to "Limit seating with overload protection" (limit and/or torque evaluation)

Configuration This test is required for the following versions or configurations:

- Actuator with electromechanical control unit
- One of the following safety functions:
 - Safe ESD function "Safe CLOSING" (Safe ESD in direction CLOSE)
 - Safe ESD function "Safe OPENING" (Safe ESD in direction OPEN)
- Configuration of "SIL seating"
 - = "Limit seating with overload protection"
 - (safety operation is stopped by limit switch tripping **and/or** torque switch tripping (overload protection)).

Test procedure During the test, the reaction of the Safe ESD function to limit switch tripping and/or torque switch tripping during safety operation is checked.

During Safe ESD operation, the actuator has to stop when reaching the position set via limit switching. Safe ESD operation must also be stopped if the tripping torque set via the torque switching is exceeded.

The red test buttons [1] and [2] of the control unit are used for the test. These can be used to operate the switches manually:

Figure 15: Electromechanical control unit



- Turn test button [1] in direction of the WSR/LSC arrow (clockwise closing): Limit switch CLOSE trips.
- Turn test button [1] in direction of the DSR/TSC arrow (counterclockwise opening): Torque switch CLOSE trips.
- Turn test button [2] in direction of the WÖL/LSO arrow (clockwise closing): Limit switch OPEN trips.
- Turn test button [2] in direction of the DÖL/TSO arrow (counterclockwise opening): Torque switch OPEN trips.



If one of the test buttons (TSC/TSO) is turned without performing a safety operation, a SIL fault signal is issued!

Test sequence Refer to checklist in the [Safe ESD reaction to “Limit seating with overload protection” \(limit and/or torque evaluation\)](#) – for actuators with electromechanical control unit [► 46] chapter.

8.4.6 Check Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electromechanical control unit

Configuration This test is required for the following versions or configurations:

- Actuator with electromechanical control unit
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Forced limit seating in end position”
 - (safety operation is stopped by limit switch tripping)

Test procedure During the test, the reaction of the Safe ESD function to limit switch tripping during safety operation is checked.

During Safe ESD operation, the actuator has to stop when reaching the position set via limit switching.

The red test buttons [1] and [2] of the control unit are used for the test. These can be used to operate the switches manually:

Figure 16: Electromechanical control unit



- Turn test button [1] in direction of the WSR/LSC arrow (clockwise closing): Limit switch CLOSE trips.
- Turn test button [2] in direction of the WÖL/LSO arrow (counterclockwise opening): Limit switch OPEN trips.

Test sequence Refer to checklist in the [Safe ESD reaction to “Forced limit seating in end position” \(limit evaluation\)](#) – for actuators with electromechanical control unit [► 47] chapter.

8.4.7 Check Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electronic control unit and limit switches

Configuration This test is required for the following versions or configurations:

- Actuator with electronic control unit and limit switches
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Forced limit seating in end position”
 - (safety operation is stopped by limit switch tripping)

Test procedure	During the test, the reaction of the Safe ESD function to limit switch tripping during safety operation is checked. During Safe ESD operation, the actuator has to stop when reaching the position set via limit switching.
Test sequence	Refer to checklist in the Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electronic control unit and limit switches [► 48] chapter.

8.4.8 Check Safe ESD reaction to “Forced torque seating in end position” (torque after limit evaluation)

Configuration	This test is required for the following versions or configurations: • Actuator with electromechanical control unit • One of the following safety functions: – Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE) – Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN) • Configuration of “SIL seating” = “Forced torque seating in end position” (safety operation is stopped by tripping the torque switches (overload protection). Provided that the respective limit switch tripped before).
Test procedure	During the test, the reaction of the Safe ESD function to torque switch tripping (after limit switch tripping) during safety operation is checked. The red test buttons [1] and [2] of the control unit are used for the test. These can be used to operate the switches manually:

Figure 17: Electromechanical control unit



	• Turn test button [1] in direction of the TSC arrow: Torque switch CLOSE trips. • Turn test button [2] in direction of the TSO arrow: Torque switch OPEN trips.
Test sequence	Refer to checklist in the Safe ESD reaction to Forced torque seating in end position (limit evaluation) – for actuators with electromechanical control unit [► 48] chapter.

8.4.9 Check Safe ESD reaction for “no seating” (no evaluation of limit and torque)

Configuration	This test is required for the following versions or configurations: • Actuators with electronic control unit or actuator with electronic control unit and limit switches. • One of the following safety functions: – Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE) – Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN) • Configuration of “SIL seating” = “no seating” (Safe opening or closing without responding to any protective equipment)
---------------	--

Test procedure For Safe ESD operation, the actuator has to perform the failure operation without interruption. Limit switching and/or torque switching must not stop the failure operation.

NOTICE

If “SIL seating” = “no seating” (without end position protection) is configured faulty operation during the test may result in damage to the elements within the safety-related system.

Possible consequences are for example: Valve damage, motor overheating, contactor seizure, defective thyristors, heating up or damage to cables.

- **Interrupt safety operation before reaching the end position** (Set *Safe ESDb* and *Safe ESDb* input signals to +24 V DC).
- For the test, the valve should either be in mid-position or at sufficient distance from the end positions.
- In case of damage, the actuator system has to be checked and repaired, if necessary.

Test sequence Refer to checklist in the [Safe ESD reaction to “No seating” – for actuators with electromechanical control unit or with electronic control unit with limit switches \[► 49\]](#) chapter.

8.4.10 Check Safe STOP function

Configuration The test applies to the “SIL function” = “Safe STOP OPEN/CLOSE” (Safe STOP) configuration. The seating configuration is not relevant to the test as it has no impact on the Safe STOP function.

Test procedure If the *Safe STOP ZU/CLOSE* or *Safe STOP AUF/OPEN* input signals are switched accordingly, the actuator must stop.

Test sequence Refer to checklist in the [Safe STOP function – irrespective of the selected control unit \[► 50\]](#) chapter.

8.4.11 Check combination of Safe ESD and Safe STOP function

Configuration This test is required for the following versions or configurations:

- One of the following Safe ESD safety functions with any seating configuration:
 - Safe ESD function: “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function: “Safe OPENING” (Safe ESD in direction OPEN)
- Safe STOP function

NOTICE

If “SIL seating” = “no seating” (without end position protection) is configured faulty operation during the test may result in damage to the elements within the safety-related system.

Possible consequences are for example: Valve damage, motor overheating, contactor seizure, defective thyristors, heating up or damage to cables.

- Check “SIL seating” before proof test configuration.
- For actuators with “SIL seating” = “no seating”: **Interrupt safety operation before reaching the end position** (Set *Safe ESDa* and *Safe ESDb* input signals to +24 V DC).
- For the test, the valve should either be in mid-position or at sufficient distance from the end positions.
- In case of damage, the actuator system has to be checked and repaired, if necessary.

Test procedure This test is intended to confirm the correct function of the combination of Safe ESD safety operation and the Safe STOP function.

Test sequence Refer to checklist in the [Combination of Safe ESD and Safe STOP – irrespective of the selected control unit \[► 51\]](#) chapter.

8.5 Maintenance

Maintenance and service tasks may only be performed by authorised personnel who have been trained on functional safety.

After maintenance and service interventions, an additional functional test to validate the safety function is imperatively required. Validation must include at least the tests described in the subsequent chapters:

[Check safety equipment \[► 29\]](#)

[Proof test \(verification of safe actuator function\) \[► 31\]](#)

In case a fault is detected during maintenance, this must be reported to AUMA Riester GmbH & Co. KG.

In the same way, faulty functions and failures of the actuator with AC .2 SIL actuator controls must be documented by the plant operator and reported to AUMA Riester GmbH & Co. KG, to allow assessment within the framework of the management of functional safety and contribution to measures of improvement.

The activities indicated in both this chapter and in the operation instructions in the “Maintenance” chapter must be executed at the defined intervals to preserve the suitability of the actuator with the AC .2 actuator controls in SIL version for use in safety instrumented systems.

- Unless specified otherwise, electromechanical components must be subjected to a functional test after 10 years at the latest and may then be used for another 5 years. Actuator motors have to be replaced after 20 years.
- SIL logic and SIL relay sub-assembly have to be replaced after 10 years; further use is not possible.
- The probability of failure (PFD) must be determined while considering the changed demand interval (useful lifetime).



AUMA actuators prioritise motor operation to manual operation. This means that the actuator automatically switches to motor operation on demand unless it has been locked in manual operation. However, we recommend activation of motor operation for a short time subsequent to maintenance or service interventions to ensure safe engagement of motor coupling. Furthermore, we recommend locking the handwheel when disengaged to avoid unintentional activation.

9 Safety-related figures

9.1 Determination of the figures

The calculation of the safety-related parameters is based on the indicated safety functions. The assessment of mechanical, electrical and electronic components is based on an FMEDA (Failure Modes, Effects and Diagnostic Analysis). FMEDA is a method to assess the functional safety of a device according to IEC 61508. On the basis of FMEDA, the failure rates and the fraction of dangerous failures of a device are determined.

Experience data and data taken from the exida database for mechanical components is used to calculate failure rates. The electronic failure rates are the base failure rates taken from the SIEMENS Standard SN 29500.

In compliance with table 2 of IEC 61508-1, the average PFD value for systems with “low demand mode” is:

- SIL 2 safety functions: $\geq 10^{-3}$ to $< 10^{-2}$
- SIL 3 safety functions: $\geq 10^{-4}$ to $< 10^{-3}$

Since actuators only represent a part of the overall safety function, the actuator PFD should not account for more than approx. 25 % of the permissible total value (PFD_{avg}) of a safety function. This results in the following values:

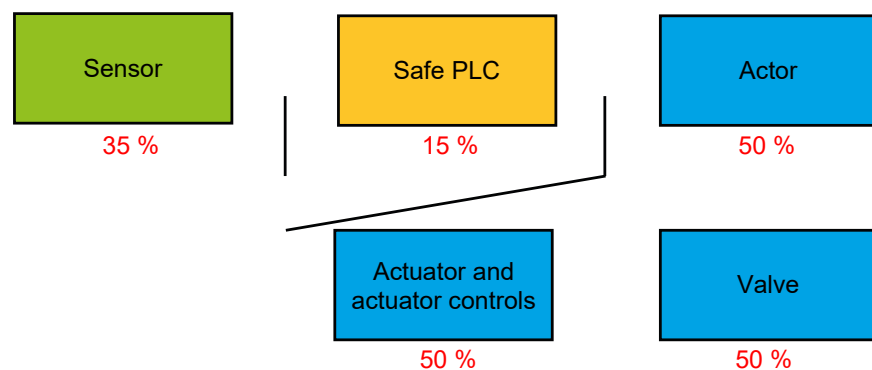
- Actuator PFD for SIL 2 applications: $\leq 2.5E-03$

Electric actuators with actuator controls are classified as type A components with a hardware fault tolerance of 0. The SFF for the type A subsystem should be between 60 % and <90 % according to table 2 of IEC 61508-2 for SIL 2 (subsystems with a hardware fault tolerance of 0).

Figure 18: Non-normative fault distribution assumed by AUMA

Failure rate distribution within the safety instrumented system (SIS)

The limit value of the PFD or the PFH applies to the overall safety system



The power supply of the system is not considered for the calculation of the actuator and the actuator controls.

As previously mentioned in the architecture section, safeguarding power supply and resulting calculations are the responsibility of the plant operator.

The plant operator is responsible for heeding the assumed MTTR, otherwise the data of the quantitative results is no longer valid.



The safety-related figures mentioned in this safety manual are only valid if **all** the conditions stipulated in this safety manual and the mentioned activities are respected.

The PFD values specified in this safety manual are only examples and subject to certain assumptions e.g. on T_{proof} , MTTR, ...

The PFD calculation should always be performed individually for each system using the parameters and conditions applicable for the respective system. The λ_{DU} and λ_{DD} values should be used as input. When observing the proof test procedures indicated in this safety manual, we recommend using a proof test coverage (PTC) of 90 % for the calculations.

9.2 Specific figures for AC 01.2 actuator controls in SIL version with actuators of SA .2 series

The following parameter tables provide the safety figures for the different versions. If one or several of the assumptions indicated below are changed, you have to recalculate the probability of failure on demand (PFD) in particular, but possibly also other parameters.

When determining the PFD values, please note that the stipulated proof test cannot fully restore the system. For this reason, the following data is used for calculation:

- PTC = 90 % (proof test coverage rate [%])
- T_1 = 1 year (proof test interval [h])
- T_2 = 10 years (demand interval = lifetime [h])
- MRT = 72 hours (mean repair time [h])
- Td_ESD = 730 hours
(diagnostic test interval of actuator monitoring (for Safe ESD [h] safety function))
- Td_ESD_AVG = 365 hours (mean duration for failure detection)
- Td_STOP = 0 hours (diagnostic test interval [h])
- MTTR_ESD = 437 hours
- MTTR_STOP = 72 hours

The following formula can be used for the calculation of the PFD_{avg} values:

$$PFD_{avg}(1001) = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DU}(1 - PTC)}{\lambda_D} \left(\frac{T_2}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTR = Td_{avg} + MRT$$

9.2.1 Figures for actuators with conventional output drive types (without extension flange)

The figures indicated in this chapter refer to actuators with one of the following output drive types B, B1-B4, B3D, B4D, C, D or DD, without extension flange. If an extension flange or one of the output drive types A, AG, AK, AF or IB is used, the [Figures for actuators equipped with alternative output drive types \[► 42\]](#) chapter must additionally be observed.



The figures for Safe STOP OPEN or Safe STOP CLOSE, indicated in the subsequent tables, refer to one of the two functions. If a general Safe STOP (inhibit operation in both directions) is to be performed while activating the functions Safe STOP OPEN and Safe STOP CLOSE at the same time, the double failure rate of the respective individual functions (Safe STOP OPEN/CLOSE) must be applied for the assessment.

Table 13: SA .2/SAEx .2 type range with AC 01.2/ACExC 01.2 actuator controls in SIL version
SA 07.2 – SA 16.2 / SAEx 07.2 – SAEx 16.2
Switchgear version: Contactors

Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	185 FIT	570 FIT
$\lambda_{DD}^{1)}$	735 FIT	89 FIT
λ_{DU}	163 FIT	204 FIT
SFF	84 %	76 %
DC	81 %	30 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.69×10^{-3}	1.72×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.57×10^{-4}	1.75×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

Table 14: SA .2 type range with AC 01.2 actuator controls in SIL version
SA 07.2 – SA 16.2 / SAR 07.2 – SAR 16.2
Switchgear version: Thyristors

Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	138 FIT	560 FIT
$\lambda_{DD}^{1)}$	763 FIT	89 FIT
λ_{DU}	172 FIT	152 FIT
SFF	83 %	81 %
DC	81 %	37 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.78×10^{-3}	1.28×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.65×10^{-4}	1.30×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

Table 15: SAEx .2 type range with ACExC 01.2 actuator controls in SIL version
SAEx 07.2 – SAEx 16.2 / SAREx 07.2 – SAREx 16.2
Switchgear version: Thyristor with tripping contactor

Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	176 FIT	599 FIT
$\lambda_{DD}^{1)}$	798 FIT	89 FIT
λ_{DU}	176 FIT	152 FIT
SFF	84 %	81 %
DC	81 %	37 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.82×10^{-3}	1.28×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.69×10^{-4}	1.30×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

Table 16: SA .2/SAEx .2 type range with AC 01.2/ACExC 01.2 actuator controls in SIL version, with heating system

SA 07.2 – SA 16.2 / SAEx 07.2 – SAEx 16.2		
Switchgear version: Contactors		
Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	185 FIT	570 FIT
$\lambda_{DD}^{1)}$	824 FIT	180 FIT
λ_{DU}	164 FIT	205 FIT
SFF	86 %	78 %
DC	83 %	46 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.74×10^{-3}	1.73×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.60×10^{-4}	1.76×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

Table 17: SA .2 type range with AC 01.2 actuator controls in SIL version, with heating system

SA 07.2 – SA 16.2 / SAR 07.2 – SAR 16.2		
Switchgear version: Thyristor		
Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	138 FIT	560 FIT
$\lambda_{DD}^{1)}$	852 FIT	181 FIT
λ_{DU}	173 FIT	153 FIT
SFF	85 %	82 %
DC	83 %	54 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.82×10^{-3}	1.29×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.68×10^{-4}	1.31×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

Table 18: SAEx .2 type range with ACExC 01.2 actuator controls in SIL version, with heating system

SAEx07.2 – SAEx 16.2 / SAREx 07.2 – SAREx 16.2		
Switchgear version: Thyristor with tripping contactor		
Safety function	Safe ESD	Safe STOP OPEN or Safe STOP CLOSE
λ_S	176 FIT	599 FIT
$\lambda_{DD}^{1)}$	887 FIT	181 FIT
λ_{DU}	177 FIT	153 FIT
SFF	85 %	83 %
DC	83 %	54 %
$PFD_{avg} T_{Proof} = 1 \text{ year (1001)}$	1.87×10^{-3}	1.29×10^{-3}
$PFD_{avg} T_{Proof} = 1 \text{ year (1002)}$	1.72×10^{-4}	1.31×10^{-4}
SIL capability	SIL 2 (HFT = 0) SIL 3 (HFT = 1)	SIL 2 (HFT = 0)

1) including detected "annunciation" failures (λ_{AD}) (failures in diagnostic function)

9.2.2 Figures for actuators equipped with alternative output drive types

Certain applications might require the use of an extension flange or one of the output drive types A, AG, AK, AF or IB. Since this is an additional component within the safety chain, the failure rates listed in the subsequent table must additionally be added to the figures as mentioned in the [Figures for actuators with conventional output drive types \(without extension flange\)](#) [► 40] chapter. The remaining safety metrics must be recalculated considering these new failure rates.

Table 19: Additional failure rates for output drive types A, AG, AK, AF, IB and the extension flanges

Type	Additional failure rates		
	λ_s [FIT]	λ_{DD} [FIT]	λ_{DU} [FIT]
Extension flange	0	0	11.5
Output drive types A, AK or AF	0	32.2	20.1
Output drive type AG	0	39.4	20.9
Output drive type IB	0	3.6	28.9

10 Checklists

10.1 Commissioning checklist

Table 20: Checklist 1

1. Actuator and actuator controls are correctly wired?	☐ ✓
2. Limit and torque switching set?	☐ ✓
3. Safe function (depending on the configuration) checked in accordance with the proof test checklists?	☐ ✓
4. Commissioning of basic settings (actuator controls in standard version) performed in accordance with the operation instructions?	☐ Yes ☐ No
☒ ✓ = Executed	

10.2 Proof test checklists

If the proof test is performed according to proof test checklists, the pertaining NO-TICES contained in the [Tests and maintenance \[▶ 29\]](#) chapter have to be observed and a preliminary inspection ([Preliminary inspection checklist \[▶ 44\]](#) chapter) be executed.

10.2.1 Preliminary inspection checklist

The actuator system must be subjected to the following inspections first.

Table 21: Preliminary inspection checklist

1. Visual inspection:	
a) Visual inspection for external damage, leakage and corrosion.	☐ ✓
b) Inspect electrical supply for damage. Check cable entry for correct fit and perform visual inspection of the respective seals.	☐ ✓
c) Check correct fit of the mechanical connections.	
2. Function check	☐ ✓
3. Operate actuator at least once from CLOSED to OPEN and back (or vice versa). During this operation, monitor actuator for conspicuous noise and sluggishness.	☐ ✓
↪ Check end position:	
a) Are the end positions completely reached? (if possible check at valve)	☐ Yes
b) Both end positions are reached and signalled as expected?	☐ No
☒ ✓ = Executed	
☒ Yes = Condition met	
☒ No = Condition not met	
If the answer to one of the questions is no, the safety instrumented system must be checked. Should the mentioned test steps result in findings on functional restrictions, wear or damage, the actuator has to be repaired accordingly and the safety instrumented system has to be subsequently subjected to an inspection.	

10.2.2 Safe ESD safety operation (Safe OPENING/CLOSING) – irrespective of the selected control unit

Proof test checklist for version or configuration:

- Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
- Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Irrespective of type of seating

Also valid for combination of Safe ESD with Safe STOP.

Table 22: Checklist 2

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Operation command in direction OPEN executed?	☐ ✓	2. Operation command in direction CLOSE executed?	☐ ✓

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Does actuator stop and run in direction CLOSE up to end position CLOSED?	☐ Yes ☐ No	↳ Check actuator reaction: Does actuator stop and run in direction OPEN up to end position OPEN?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No
4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.3 SIL fault signal “Actuator monitoring” – irrespective of the selected control unit

Proof test checklist for version or configuration:

- Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
- Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Irrespective of type of seating

Also valid for combination of Safe ESD with Safe STOP.

Table 23: Checklist 3

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Handwheel engaged and locked (white sleeve fitted in locking device for the handwheel)?	☐ ✓	2. Handwheel engaged and locked (white sleeve fitted in locking device for the handwheel)?	☐ ✓
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check SIL module signal behaviour: SIL fault signal within 4 seconds? (SIL-Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: SIL fault signal within 4 seconds? (SIL-Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No
4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
5. Motor operation engaged (white sleeve removed from locking device and black sleeve fitted if required) and actuator was briefly and successfully run in motor operation?	☐ ✓	5. Motor operation engaged (white sleeve removed from locking device and black sleeve fitted if required) and actuator was briefly and successfully run in motor operation?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.4 Safe ESD reaction for “Motor protection (thermal fault)” signals – irrespective of the selected control unit

Proof test checklist for version or configuration:

- Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
- Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Irrespective of type of seating

Also valid for combination of Safe ESD with Safe STOP.

Table 24: Checklist 4

Configuration SIL motor protection active		Configuration SIL motor protection inactive	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Selector switch in position 0 (OFF)?	☐ ✓	2. Selector switch in position 0 (OFF)?	☐ ✓
3. Simulation value: Thermal test selected in parameter Proof test (motor prot.) M1021 (required user level: Specialist (4))? Display indicates: CMD0078 Thermal test ○ (white dot)	☐ ✓	3. Simulation value: Thermal test selected in parameter Proof test (motor prot.) M1021 (required user level: Specialist (4))? Display indicates: CMD0078 Thermal test ○ (white dot)	☐ ✓
4. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	4. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
5. Motor protection simulation activated via push buttons Ok? Display indicates: CMD0079 Thermal test ● (black dot)	☐ ✓	5. Motor protection simulation activated via push buttons Ok? Display indicates: CMD0078 Thermal test ● (black dot)	☐ ✓
↳ Check actuator reaction: Was safety operation stopped?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation was not stopped?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No
6. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	6. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
7. Was the simulation reset or simulation menu quitted and the selector switch reset to the initial position?	☐ ✓	7. Was the simulation reset or simulation menu quitted and the selector switch reset to the initial position?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.5 Safe ESD reaction to “Limit seating with overload protection” (limit and/or torque evaluation) – for actuators with electromechanical control unit

Proof test checklist for version or configuration:

- Actuator with electromechanical control unit
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Limit seating with overload protection”

Also valid for combination of Safe ESD with Safe STOP.

Table 25: Checklist 5

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Is switch compartment opened?	☐ ✓	2. Is switch compartment opened?	☐ ✓
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
4. Limit switch CLOSE operated and held down until step 5.1 was executed? (Test button [1] turned in direction of the arrow WSR?)	☐ ✓	4. Limit switch OPEN operated and held down until step 5.1 was executed? (Test button [2] turned in direction of the arrow WÖL?)	☐ ✓
↳ Check actuator reaction: Was safety operation stopped?	☐ Yes ☐ No	↳ Check actuator reaction: Was safety operation stopped?	☐ Yes ☐ No

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
5.2 Was actuator operated via local controls or from RE-MOTE to end position OPEN and then to end position CLOSED?	☐ ✓	5.2 Was actuator operated via local controls or from RE-MOTE to end position OPEN and then to end position CLOSED?	☐ ✓
5.3 Was actuator operated to mid-position or at sufficient distance from the end positions?	☐ ✓	5.3 Was actuator operated to mid-position or at sufficient distance from the end positions?	☐ ✓
6. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	6. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
7. Torque switch CLOSE operated and held down until step 8 was executed? (Test button [1] turned in direction of the arrow DSR?)	☐ ✓	7. Torque switch OPEN operated and held down until step 8 was executed? (Test button [2] turned in direction of the arrow DÖL?)	☐ ✓
↳ Check actuator reaction: Was safety operation stopped? Display illuminated in red?	☐ Yes ☐ No	↳ Check actuator reaction: Was safety operation stopped? Display illuminated in red?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No
8. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	8. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
9. Torque fault of actuator controls in standard version acknowledged?	☐ ✓	9. Torque fault of actuator controls in standard version acknowledged?	☐ ✓
10. Switch compartment closed?	☐ ✓	10. Switch compartment closed?	☐ ✓
☑ ✓ = Executed ☑ Yes = Condition met ☑ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.6 Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electromechanical control unit

Proof test checklist for version or configuration:

- Actuator with electromechanical control unit
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Forced limit seating in end position”

Also valid for combination of Safe ESD with Safe STOP.

Table 26: Checklist 6

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Is switch compartment opened?	☐ ✓	2. Is switch compartment opened?	☐ ✓
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
4. Limit switch CLOSE operated and held down until step 5.1 was executed? (Test button [1] turned in direction of the arrow WSR?)	☐ ✓	4. Limit switch OPEN operated and held down until step 5.1 was executed? (Test button [2] turned in direction of the arrow WÖL?)	☐ ✓
↳ Check actuator reaction: Was safety operation stopped?	☐ Yes ☐ No	↳ Check actuator reaction: Was safety operation stopped?	☐ Yes ☐ No

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
5.2 Was actuator operated via local controls or from REMOTE to end position OPEN and then to end position CLOSED?	☐ ✓	5.2 Was actuator operated via local controls or from REMOTE to end position OPEN and then to end position CLOSED?	☐ ✓
6. Switch compartment closed?	☐ ✓	6. Switch compartment closed?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.7 Safe ESD reaction to “Forced limit seating in end position” (limit evaluation) – for actuators with electronic control unit and limit switches

Proof test checklist for version or configuration:

- Actuator with electronic control unit and limit switches
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Forced limit seating in end position”

Also valid for combination of Safe ESD with Safe STOP.

Table 27: Checklist 7

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	2. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↪ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↪ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
3. Wait until actuator limit switch trips. ↪ Check actuator reaction: Was safety operation stopped when reaching limit switch CLOSE?	☐ Yes ☐ No	3. Wait until actuator limit switch trips. ↪ Check actuator reaction: Was safety operation stopped when reaching limit switch OPEN?	☐ Yes ☐ No
4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	4. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.8 Safe ESD reaction to Forced torque seating in end position (limit evaluation) – for actuators with electromechanical control unit

Proof test checklist for version or configuration:

- Actuator with electromechanical control unit
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
 - = “Forced torque seating in end position”

Also valid for combination of Safe ESD with Safe STOP.

Table 28: Checklist 8

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Was actuator operated to end position CLOSED via actuator controls in standard version (until limit switch has tripped)?	☐ ✓	1. Was actuator operated to end position OPEN via actuator controls in standard version (until limit switch has tripped)?	☐ ✓
2. Is switch compartment opened?	☐ ✓	2. Is switch compartment opened?	☐ ✓
3. + 4. Was torque switch CLOSE operated and the safety operation initiated for operated switch? (Test button [1] turned in direction of the arrow DSR?) (Safe ESDa and Safe ESDb input signals set to 0 V (low)?)	☐ ✓	3. + 4. Was torque switch OPEN operated and the safety operation initiated with operated switch? (Test button [2] turned in direction of the arrow DÖL?) (Safe ESDa and Safe ESDb input signals set to 0 V (low)?)	☐ ✓
↳ Check actuator reaction: Was safety operation not tripped?	☐ Yes ☐ No	↳ Check actuator reaction: Was safety operation not tripped?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: No SIL fault signal? (SIL Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: No SIL fault signal? (SIL Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No
5. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓	5. Safe ESDa and Safe ESDb input signals set to +24 V DC (high)?	☐ ✓
6. Switch compartment closed?	☐ ✓	6. Switch compartment closed?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.9 Safe ESD reaction to “No seating” – for actuators with electromechanical control unit or with electronic control unit with limit switches

Proof test checklist for version or configuration:

- Actuator with electromechanical control unit or actuator with electronic control unit and limit switches:
- One of the following safety functions:
 - Safe ESD function “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function “Safe OPENING” (Safe ESD in direction OPEN)
- Configuration of “SIL seating”
= “No seating”

Also valid for combination of Safe ESD with Safe STOP.



For version of electronic control unit with limit switches, steps 6 – 9 are obsolete.

Table 29: Checklist 9

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Is switch compartment opened?	☐ ✓	2. Is switch compartment opened?	☐ ✓
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation initiated?	☐ Yes ☐ No
4. Was limit switch CLOSED operated? (Test button [1] turned in direction of the arrow WSR?)	☐ ✓	4. Was limit switch OPEN operated? (Test button [2] turned in direction of the arrow WÖL?)	☐ ✓
↳ Check actuator reaction: Safety operation was not stopped?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation was not stopped?	☐ Yes ☐ No
5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high) prior to reaching the end position.	☐ ✓	5.1 Safe ESDa and Safe ESDb input signals set to +24 V DC (high) prior to reaching the end position.	☐ ✓

Configuration Safe CLOSING (ESD in direction CLOSE)		Configuration Safe OPENING (ESD in direction OPEN)	
5.2 Was actuator operated via local controls or from REMOTE to end position OPEN and then to end position CLOSED?	☐ ✓	5.2 Was actuator operated via local controls or from REMOTE to end position OPEN and then to end position CLOSED?	☐ ✓
5.3 Was actuator operated to mid-position or at sufficient distance from the end positions?	☐ ✓	5.3 Was actuator operated to mid-position or at sufficient distance from the end positions?	☐ ✓
6. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	6. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
7. Torque switch CLOSE was operated? (Test button [1] turned in direction of the arrow DSR?)	☐ ✓	7. Torque switch OPEN was operated? (Test button [2] turned in direction of the arrow DÖL?)	☐ ✓
↳ Check actuator reaction: Safety operation was not stopped? Display illuminated in red?	☐ Yes ☐ No	↳ Check actuator reaction: Safety operation was not stopped? Display illuminated in red?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: SIL fault signal? (SIL Fehler/Failure output (NC contact) = closed)	☐ Yes ☐ No
8. Safe ESDa and Safe ESDb input signals set to +24 V DC (high) prior to reaching the end position.	☐ ✓	8. Safe ESDa and Safe ESDb input signals set to +24 V DC (high) prior to reaching the end position.	☐ ✓
9. Torque fault of actuator controls in standard version acknowledged?	☐ ✓	9. Torque fault of actuator controls in standard version acknowledged?	☐ ✓
10. Switch compartment closed?	☐ ✓	10. Switch compartment closed?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.10 Safe STOP function – irrespective of the selected control unit

Proof test checklist for execution or configuration:

“SIL function” = “Safe STOP OPEN/CLOSE” (safe stop) configurations.

Also valid for combination of Safe ESD with Safe STOP. If both safety functions, Safe STOP OPEN and Safe STOP CLOSE are used, both columns of checklist 10 must be processed.

Table 30: Checklist 10

Safe stop in direction OPEN Safe STOP OPEN		Safe stop in direction CLOSE Safe STOP CLOSE	
1. Is the actuator in mid-position or at sufficient distance from the end positions? ↳ If required: Change the command channel (LOCAL or REMOTE) used for this test to push-to-run operation.	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions? ↳ If required: Change the command channel (LOCAL or REMOTE) used for this test to push-to-run operation.	☐ ✓
2. Operation command in direction OPEN executed via actuator controls in standard version in push-to-run operation?	☐ ✓	2. Operation command in direction CLOSE executed via actuator controls in standard version in push-to-run operation?	☐ ✓
3. Safe STOP ZU/CLOSE input signal set to 0 V (low)? ↳ Check actuator reaction: Does actuator continue its operation in direction OPEN?	☐ ✓ ☐ Yes ☐ No	3. Safe STOP AUF/OPEN input signal set to 0 V (low)? ↳ Check actuator reaction: Does actuator continue its operation in direction CLOSE?	☐ ✓ ☐ Yes ☐ No
↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No
4. Safe STOP AUF/OPEN input signal set to 0 V (low)? ↳ Check actuator reaction: Does actuator stop?	☐ ✓ ☐ Yes ☐ No	4. Safe STOP ZU/CLOSE input signal set to 0 V (low)? ↳ Check actuator reaction: Does actuator stop?	☐ ✓ ☐ Yes ☐ No
↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: No SIL fault signal? (SIL-Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No
5. Safe STOP AUF/OPEN and Safe STOP ZU/CLOSE input signals set to +24 V DC (high)?	☐ ✓	5. Safe STOP AUF/OPEN and Safe STOP ZU/CLOSE input signals set to +24 V DC (high)?	☐ ✓
6. If the control of the standard commands (LOCAL or REMOTE) has been changed from self-retaining to push-to-run operation for the test: Restore original status.	☐ ✓	6. If the control of the standard commands (LOCAL or REMOTE) has been changed from self-retaining to push-to-run operation for the test: Restore original status.	☐ ✓

Safe stop in direction OPEN Safe STOP OPEN		Safe stop in direction CLOSE Safe STOP CLOSE	
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			

10.2.11 Combination of Safe ESD and Safe STOP – irrespective of the selected control unit

Proof test checklist for version or configuration:

- One of the following Safe ESD safety functions with any seating configuration:
 - Safe ESD function: “Safe CLOSING” (Safe ESD in direction CLOSE)
 - Safe ESD function: “Safe OPENING” (Safe ESD in direction OPEN)
- Safe STOP function

Table 31: Checklist 11

Safe stop in direction CLOSE Safe CLOSING (ESD in direction CLOSE)		Safe stop in direction OPEN Safe OPENING (ESD in direction OPEN)	
1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓	1. Is the actuator in mid-position or at sufficient distance from the end positions?	☐ ✓
2. Safe STOP ZU/CLOSE input signal set to 0 V (low)?	☐ ✓	2. Safe STOP AUF/OPEN input signal set to 0 V (low)?	☐ ✓
3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓	3. Safe ESDa and Safe ESDb input signals set to 0 V (low)?	☐ ✓
↳ Check actuator reaction: Was safety operation initiated in direction CLOSE?	☐ Yes ☐ No	↳ Check actuator reaction: Was safety operation initiated in direction OPEN?	☐ Yes ☐ No
↳ Check SIL module signal behaviour: No SIL fault signal? (SIL Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No	↳ Check SIL module signal behaviour: No SIL fault signal? (SIL Fehler/Failure output (NC contact) = open)	☐ Yes ☐ No
4. Safe ESDa, Safe ESDb, Safe STOP AUF/OPEN and Safe STOP ZU/CLOSE input signals set to +24 V DC (high)?	☐ ✓	4. Safe ESDa, Safe ESDb, Safe STOP AUF/OPEN and Safe STOP ZU/CLOSE input signals set to +24 V DC (high)?	☐ ✓
☒ ✓ = Executed ☒ Yes = Condition met ☒ No = Condition not met If the answer to one of the questions is no, the safety instrumented system must be checked.			



In addition to this test, all other proof tests relating to the individual safety functions (Safe STOP or ESD) in this manual have to be performed for the combination of Safe ESD and Safe STOP.

Index

A

Actuator sizing	8
Ambient conditions	12
Architecture	8

B

Brake	11
-------	----

C

Checklists	44
Commissioning	21
Commissioning checklist	44
Configuration	9

D

DC	5
Decommissioning	22
Device type	6
Diagnostic coverage	5
Digital outputs	27
Display (indications)	26

E

Examples of applications	17
--------------------------	----

F

Failures	5
Fieldbus (signals)	28
Figures	39

H

HFT	5
-----	---

I

Indications	26
Indications on display	24
Installation	19
Internal actuator monitoring	29
Interval for proof test	5

L

Lambda values	5, 40
Lifetime	22
Low demand mode	39

M

Maintenance	38
MRT (Mean Repair Time)	6
MTBF	5
MTTR (Mean Time To Restoration)	6

N

Not ready REMOTE - indication on display	25
--	----

O

Operation	22
-----------	----

P

Partial Valve Stroke Test (PVST)	29
PFD	5
PFD actuator	39
Preliminary inspection checklist	44
Probability of failure	5
Proof test	5, 31
Proof test checklists	44
PTC (Proof Test Coverage)	6

R

Range of application	7
----------------------	---

S

Safety function	5
Safety functions	14
Safety instrumented function (SIF)	5
Safety instrumented system	14
Safety instrumented system (SIS)	5
Safety-related system	5
Self-locking	11
Service conditions	12
Setting	9
SFF	5
SIL	5
Standards	7
Status signals	27
Status SIL – Indications on the display	24

T

T proof	5
Tests	29
Troubleshooting	26
Type of duty	12

W

Warnings – indication on display	24
----------------------------------	----



Solutions for a world in motion.

AUMA Riester GmbH & Co. KG

Location Muellheim

Aumastr. 1

79379 Muellheim, Germany

Tel +49 7631 809 - 0

Fax +49 7631 809 - 1250

info@auma.com

www.auma.com