Solutions for a world in motion

Multi-turn actuators
SA(R) 07.2 – SA(R) 16.2/SA(R)Ex 07.2 – SA(R)Ex 16.2
SA(R) 25.1 – SA(R)30.1/SA 35.1 – SA 40.1
SA(R)Ex 25.1 – SA(R)Ex 30.1/SAEx 35.1 – SAEx 40.1
with actuator controls
AM 01.1/AM 02.1/AMExC01.1
SFC version

NOTICE for use!

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

Purpose of the document:

The present document informs about the actions required for using the device in safety-related systems in accordance with IEC 61508 or IEC 61511.

Reference documents:

- exida report no. AUMA 10-12-035 R005E
- Operation instructions (Assembly, operation, commissioning) for actuator

Reference documents are available on the Internet at: http://www.auma.com.

Table of contents

1. Terminology

Information sources

- IEC 61508-4, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions 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. Abbreviations and concepts

To evaluate safety functions, the lambda values or the PFD value (Probability of Dangerous Failure on Demand) and the SFF value (Safe Failure Fraction) are the main requirements. Further figures are required to assess the individual components. These figures are explained in the table below.

Table 1: Abbreviations of safety figures

Abbreviation	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 occurence 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 on demand of a safety function.
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 **I**ntegrity **L**evel

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

Safety function

Function to be implemented by a 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 with specified safety integrity level (SIL) to achieve functional safety.

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 perform 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.

2. Application and validity

2.1. Range of application

AUMA actuators and actuator controls 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

AUMA actuators and actuator controls meet the following requirements:

For “safe end position feedback” safety function: IEC 61508-2:2010

The safety figures of the devices described meet the requirements of IEC 61508 in the respective SIL level with regard to failure rates and architecture requirements. However, this does not imply that all further requirements of IEC 61508 are met.

2.3. Valid device types

The data on functional safety contained in this manual applies to the device types indicated.

Table 2: Overview on suitable device types

Type Actuator	Type Actuator controls	Motor Power supply	Type of duty	Control
SA 07.2 – SA 16.2 SAR 07.2 – SAR 16.2 in SFC version	AM 01.1/ AM 02.1 in SFC version	Any position	S2-15 min S2-30 min S4-25 % S4-50 %	Safe end position feedback
SA 25.1 – SA 40.1 SAR 25.1 – SAR 30.1 in SFC version	AM 01.1/ AM 02.1 in SFC version	Any position	S2-15 min S2-30 min S4-25 % S4-50 %	Safe end position feedback
SAEx 07.2 – SAEx 16.2 SAREx 07.2 – SAREx 16.2 in SFC version	AMExC 01.1 in SFC version	Any position	S2-15 min S2-30 min S4-25 % S4-50 %	Safe end position feedback
SAEx 25.1 – SAEx 40.1 SAREx 25.1 – SAREx 30.1 in SFC version	AMExC 01.1 in SFC version	Any position	S2-15 min S2-30 min S4-25 % S4-50 %	Safe end position feedback

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.

Information

In applications with requirements on functional safety, only AUMA actuator controls and actuators in SFC or SIL version may be used. SFC stands for “Safety Figure Calculated”. This designation identifies AUMA products for which safety figures were calculated on the basis of FMEDA from field data and generic data (for detailed information refer to <Determination of the figures>).
AUMA actuator controls and actuators in SFC version can among others be identified from the letters "SFC" following the type designation on the name plate.

Figure 1: Example of name plate with “SFC” 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: Valve damage, motor overheating, contactor seizure, damage to the electronics, heating up or damage to cables.

→ The actuator technical data must imperatively be observed 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 undervoltage.

Information For the “Safe end position feedback” safety function, heed that signalling is made via mechanical switches. Since these elements have an unavoidable hysteresis, the actuator slightly leaves the end position before the end position signal is deleted. Consequently, there is a marginal range of actuator positions to the safety position, for which the end position is still signalled although the actuator has already left the end position during operation from safety position. 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 evaluating both limit and torque switches for the end position feedback.

Power supply

Information The plant operator is responsible for power supply.

3.2. Configuration (setting)

Configuration (setting) of the safety-related functions is performed as described in the operation instructions or in the present manual (functional safety).

Information An exact setting of torque and end position switches for the end positions is imperatively required to ensure correct function of “Safe end position feedback”. For setting details related to the respective switches, please refer to operation instructions.

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 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 3: Overview 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 SAR 07.2 – SAR 16.2 SAEx 07.2 – SAEx 16.2 SAREx 07.2 – SAREx 16.2	≤ 90 rpm	≤ 108 rpm	Self-locking
	≥ 125 rpm	≥ 150 rpm	NOT self-locking
SA 25.1 – SA 30.1 SAR 25.1 – SAR 30.1 SAEx 25.1 – SAEx 30.1 SAREx 25.1 – SAREx 30.1	≤ 90 rpm	≤ 108 rpm	Self-locking
	≥ 125 rpm	≥ 150 rpm	NOT self-locking
SA 35.1 SAEx 35.1	≤ 22 rpm	≤ 26 rpm	Self-locking
	≥ 32 rpm	≥ 38 rpm	NOT self-locking
SA 40.1 SAEx 40.1	≤ 22 rpm	≤ 26 rpm	Self-locking
	≥ 32 rpm	≥ 38 rpm	NOT self-locking

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 basic process control system is executed via the same actuator in addition to the safety function, note that while considering the sum of non-safety instrumented function, required tests and safety function, the defined number of maximum permissible cycles[1)] for the respective actuator as well as the maximum number of starts[2)] may not be exceeded during deployment of the actuator within a safety instrumented system.

Only the “safe end position feedback” safety function can be operated beyond the limitations mentioned above under certain conditions even in operation mode with high demand rate, provided the following requirements and limitations are heeded:

- When considering the sum consisting of non-safety instrumented function, required tests and safety function, the number of maximum cycles of the actuator end position switches as well as the maximum number of starts during actuator deployment are not exceeded in a safety instrumented system.
- When considering the sum consisting of non-safety instrumented function, required tests and safety function, the number of maximum cycles for the respective actuator as well as the maximum number of permissible cycles[1)] or starts[2)] are not exceeded, if appropriate scaling rules are applied.
- Lubrication is checked at regular intervals and the lubricant changed if required, however, at least every 10 years.
- Every 20,000 cycles[1)] or starts[2)] (whatever occurs earlier), the crown wheel and the worm wheel are checked for wear and replaced if required.
- The end user makes sure that a test rate (PVST) is achieved for the “Safe end position feedback” safety function, complying with the demand rate to be expected according to the applicable standards for the respective application.
- All requirements in accordance with the “Technical data for switches” (Y004.619) data sheet are respected. In particular, the permissible minimum and maximum currents and voltages.
- The number of cycles[1)] as well as the number of cycles of each limit and torque switch do not exceed the values stipulated in the table below:

1) Definition of “cycles” according to EN 15714-2:2010
2) Definition of “starts” according to EN 15714-2:2010

Table 4:

	Classes A and B		Class C (Modulation)			
Contact material	Silver	Gold	Silver	Silver	Gold	Gold
Maximum electrical load			30 V/30 mA	250 V AC/5 A	30 V/30 mA	50 V/400 mA
Number of permissible cycles of end position switch as well as cycles according to EN 15714-2:2010	< 20,000	< 20,000	< 100,000	< 20,000	< 100,000	< 20,000

3.5. Further notes and indications on architecture

HFT is 0.

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

For “safe end position feedback”, the actuator can be considered as type A device.

Safety figures

The safety figures relevant for the product supplied as well as potential further restrictions are indicated on the declaration of incorporation. The declaration of incorporation is specific for each order and directly supplied with the order.

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 sheets:

- 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.

4. Safety instrumented systems and safety functions

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

- Safe end position feedback
  An end position signal directly wired to the actuator is available. The safety function is the correct signal whether the actuator is in the requested actuator[3)] end position or not. Only the signal via this signal communication path is safety related. End position feedback via I/O interface relay or a positioner (RWG, MWG, potentiometer, ...) or via a fieldbus interface does not represent a safe end position feedback.

3) Please note that safety figures only include the components of the actuator . Further components (e.g. integrity of external controls, gearboxes, valve shaft, other valve components....) are not considered with the AUMA safety figures related to this product

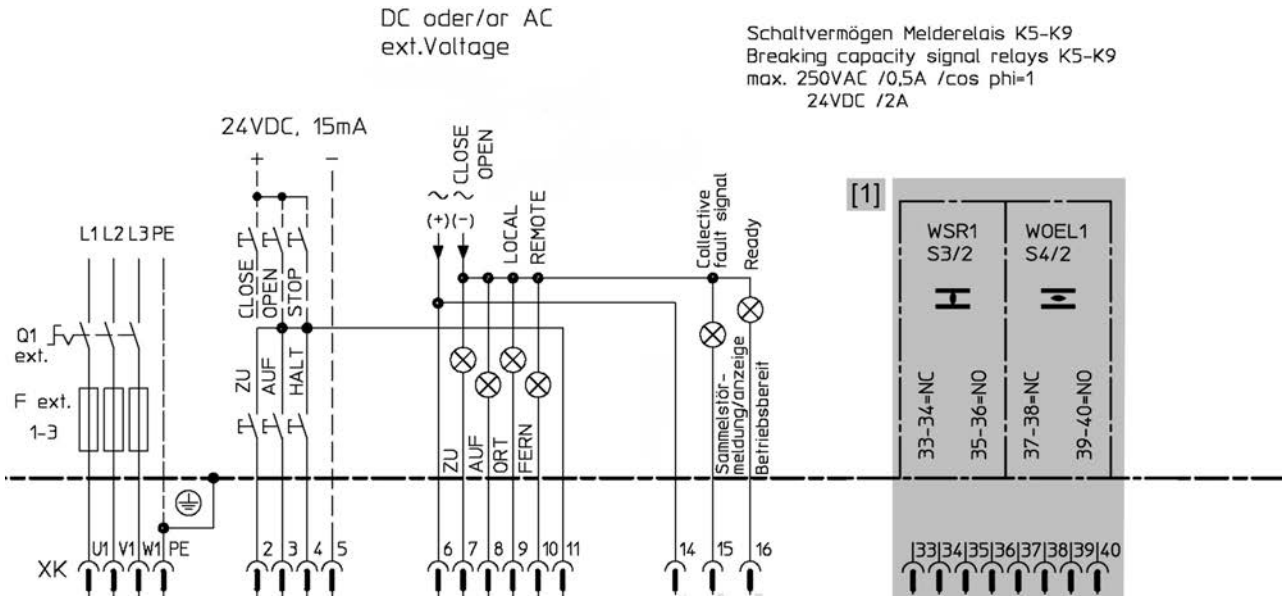
5. Installation, commissioning and operation

Information 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.

5.1. Installation

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.

Figure 2: Wiring diagram example with safe end position feedback



[1] Limit switches for safe end position feedback

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

Information Valve position indication is made via potentiometer or 4 – 20 mA signals. However, this is not part of the determination of safety figures.

5.2. Commissioning

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

After commissioning, the safe actuator function must be verified.

5.3. Operation

Regular maintenance and device checks in the T_{proof} intervals as defined by the plant operator are the basis for safe operation.

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

5.4. Lifetime

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

Safety-related figures are valid for the cycles or modulating steps defined in the technical data specifications and for typical periods of up to 10 years (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 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 operator who will have to take appropriate and suitable measures. Please contact us if you need support in identifying suitable measures.

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 regular requirements.

6. Tests and maintenance

Test 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.

Information

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

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

6.1. Safety equipment: check

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 to avoid systematic faults. Policies and strategies for achieving safety as well as different activities during the safety life cycle should be defined.

6.2. Proof test (verification of safe actuator function)

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

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

For checking the safety-related function, the output of safe end position feedback is appropriately checked.

Information

All installed and used safety functions within the actuator must be checked and all test steps performed in compliance with the pertaining checklists.

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.

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

6.2.1. Preliminary tests

The actuator system has to be subjected to a visual inspection first. The system should be checked for outside damage and corrosion. Furthermore, the electrical and mechanical connections should be checked and the actuator inspected for unusual noises while operating the actuator at least a complete travel from CLOSED to OPEN and back.

6.2.2. Review and validation of the “Safe end position signal” safety function

Test sequence (check-list)

1. Operate actuator to end position OPEN – Is the end position OPEN signalled via Safe end position signal?
2. Unseat actuator out of end position OPEN – Is the safe end position signal OPEN cancelled?
3. Operate actuator again to end position OPEN – Is the end position OPEN signalled again via Safe end position signal?
4. Operate actuator to end position CLOSED – Is the end position CLOSED signalled via Safe end position signal?
5. Unseat actuator out of end position CLOSED – Is the safe end position signal CLOSED cancelled?
6. Operate actuator again to end position CLOSED – Is the end position CLOSED signalled again via Safe end position signal?

7. During the complete procedure, no fault signal at collective fault signal output contact K9?
8. Separately check collective fault signal output contact K9 – Reaction to simulated fault?

   Information: The collective fault output contact K9 can be activated via manual torque switch test using the test buttons. Refer to the relevant chapter in the operation instructions.

6.3. Diagnostics via Partial Valve Stroke Test (PVST) / Reaction Monitoring (RM)

Regular actuator diagnostics is required using diagnostics facilities. Diagnostics should be performed at least 10 times more often than the proof test. This diagnostic comprises a specific actuator movement relating to an appropriate travel and subsequent evaluation whether the actuator reacts as expected. The individual safety functions are described in more detail below.

The actuator movement required for diagnostics can be initiated on purpose (PVST). If the actuator is operated regularly by conventional process control, this movement can be used for the purpose of diagnostics (RM). In any case, it is required that monitoring and assessment of RM or PVST is performed by the logic unit of the safety instrumented system.

Safety function Safe end position feedback:

- Actuator movement can be requested via any input.
- Assessment whether the safety function signals as desired has to be performed at the end position switches wired directly to the customer connection.
- The actuator is required
  - To be either positioned in one of both end positions prior to starting the test run. The test run is performed out of the end position and back to this end position.
  - Or to be at a sufficient distance from both end positions prior to starting the test run. The test run is performed into an end position and out of this end position.

In both cases, the travel distance must sufficient to allow for full tripping of the end position switch. It must be checked whether the end position switch signals the expected position both at the beginning, during and at the end of the test.

- Furthermore, test run monitoring must be dynamic. This means a dynamic test whether the signal change corresponds to the expected value.

Monitoring and assessment of PVST must be ensured by the logic unit of the safety instrumented system.

Information If PVST is performed out of or into one of both end positions, only the contact of this end position is checked for correct operation. If both end position switches (OPEN/CLOSE) are safety relevant, a full stroke test can be performed, for example.

6.4. Maintenance

Maintenance and service tasks may only be performed by authorised personnel who have been trained on functional safety (refer to chapter 5).

Once maintenance and service tasks have been finished, the functional test must be completed by a validating process of the safety function including at least the tests described in the <Safety equipment: check> and <Proof test (verification of safe actuator function)> chapters.

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

Information AUMA actuators prioritise motor operation to manual operation. This means that the actuator automatically switches to motor operation if requested. However, we recommend activating motor operation after any maintenance and service interventions.

7. Safety-related figures

7.1. Determination of the safety-related figures

- The calculation of the safety figures is based on the indicated safety functions. Hardware assessments are based on Failure Modes, Effects and Diagnostic Analysis (FMEDA). FMEDA is a step to assess functional device safety in compliance with IEC 61508. On the basis of FMEDA, the failure rates and the fraction of safe failures of a device are determined.
- Experience data and data taken from the exida database for mechanical components is used to calculate mechanical failure rates. The electronic failure rates as base failure rates are taken from the SIEMENS Standard SN 29500.
- In compliance with table 2 of IEC 61508-1, the average target PFD values for systems with low demand mode are:
  - SIL 1 safety functions: ≥ 10^{-2} to < 10^{-1}
  - SIL 2 safety functions: ≥ 10^{-3} to < 10^{-2}
  - SIL 3 safety functions: ≥ 10^{-4} to < 10^{-3}

  Since actuators only represent a part of the overall safety function, the actuator PFD value 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 1 applications: ≤ 2.50E-02
  - Actuator PFD for SIL 2 applications: ≤ 2.50E-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 <60 % according to table 2 of IEC 61508-2 for SIL 1 (subsystems 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).

The PFD values specified in the declarations of incorporation and 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 calculation using proof test coverage (PTC) of 90 %.[4)].

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 eliminating faults within the MTTR, otherwise the data of the quantitative results is no longer valid.

NOTICE

The safety figures mentioned in this safety manual and in the declarations of incorporation are only valid if all the conditions stipulated in this safety manual and in the declarations of incorporation and the mentioned activities are respected. At the same time, the restrictions regarding the validity and standard conformity stipulated in the declarations of incorporation must be heeded.

4) For the example calculations within this manual and the declarations of incorporation, different PTC values were sometimes used as calculation basis.

8. SIL Declaration of Conformity (example)

AUMA Riester GmbH & Co. KG
Aumastr. 1
79379 Muellheim, Germany
www.auma.com

Tel +49 7631 809-0
Fax +49 7631 809-1250
info@auma.com

auma®
Solutions for a world in motion

SIL Declaration of Conformity / SIL Declaration of Incorporation

Functional Safety according to IEC 61508

This document is only valid with order number imprinted by AUMA!

AUMA order no. _____

We herewith confirm that the products manufactured and distributed by AUMA Riester GmbH & Co. KG listed below have been subjected to an evaluation based on Failure Modes, Effects and Diagnostic Analysis (FMEDA) according to IEC 61508-2:2010.

Actuator type	Controls type/wiring diagram
SA 07.2 – SA 16.2 or SAR 07.2 – SAR 16.2 or SAEx 07.2 – SAEx 16.2 or SAREx 07.2 – SAREx 16.2 or SAV 07.2 – SAV 16.2 or SARV 07.2 – SARV 16.2 or SAVEx 07.2 – SAVEx 16.2 or SARVEx 07.2 – SARVEx 16.2 all in version SFC	AUMA MATIC AM 01.1/AMExC 01.1 or AUMATIC AC 01.2/ACExC 01.2 or AUMATIC ACV 01.2/ACVExC 01.2 in version SFC with end position/ torque switches directly wired to the customer connection or AUMA NORM (no control unit) with end position/torque switches directly wired to the customer connection.

The above mentioned versions achieves the following safety integrity level for the "Safe End Position Feedback":

Hardware Safety Integrity	
Single channel use (HFT = 0)	SIL 1 capable
Single channel use with PVST (HFT = 0)	SIL 2 capable

For further details, please refer to supplement overleaf.

---
i.V. Michael Noll
Functional Safety Management Representative

---
i.A. Jörg Isenberg
Product Management

Date

Date

This declaration does not contain any guarantees. The safety instructions in product documentation supplied with the devices must be observed. Non-concerted modification of the devices voids this declaration.

auma® Solutions for a world in motion	**Supplement** **SIL Declaration of Conformity/** **SIL Declaration of Incorporation** Functional Safety according to IEC 61508	2019-02-25

Manufacturer	
Manufacturer	AUMA Riester GmbH & Co. KG
Address	Aumastr. 1, 79379 Muellheim/Germany

General			
Device designation and permissible types	See page 1		
Safety function(s)	Safe End Position Feedback		
Device type according to IEC 61508-2	☒ Type A	☐ Type B	
Operating mode	☒ Low Demand Mode	☐ High Demand or Continuous Mode	
Safety manual	On demand		
Type of evaluation	☒	Evaluation by FMEDA according to IEC 61508-2	
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG		
Test report and test report version	Based on AUMA 10/12-035 R005E	V3R1	

SIL Integrity				
Hardware safety integrity for the "Safe End Position Feedback" (The calculated values are within the range for the corresponding SIL. However this does not imply that all related IEC 61508 requirements are fulfilled.)	Single channel use (HFT = 0)	☒ SIL1 capable	☐ SIL2 capable	☐ SIL3 capable
	Single channel use with PVST (HFT = 0)	☐ SIL1 capable	☒ SIL2 capable	☐ SIL3 capable

Safety function	Safe End position Feedback	Safe End position Feedback with PVST
λ_{SAFE} *1)	0 FIT	0 FIT
λ_{DD} *1)	0 FIT	135 FIT
λ_{DU} *1)	165 FIT	30 FIT
DC_D *2)	0 %	82 %
MTBF - Mean Time Between Failures	195 years	195 years
SFF - Safe Failure Fraction	0 %	82 %
PFD_{avg} *3) with T[Proof] = 1 year	1,38E-03	3,56E-04

According to ISO 13849-1 the following Safety Metrics are achieved*4):

Safety function	Safe End Position Feedback	Safe End Position Feedback with PVST
$MTTF_D$	694 years (high)	694 years (high)
DC	0% (none)	82 % (low)
Calculated Performance Level	1,65E-07 1/h	2,96E-08 1/h
Achieved Performance Level*4)	CAT 1: PL = „c" capable	CAT 1 or 2: PL = „c" capable

*1) FIT = Failure In Time, Number of failures per10^9 h
*2) DC_D = Diagnostic Coverage (dangerous)
*3) PFD_{avg} = Probability of a failure on demand (average)
*4) Depending on the application and possible external diagnostics a higher DC and therefore also a higher category and a higher Performance level might be possible to achieve.

auma® Solutions for a world in motion	**Supplement** **SIL Declaration of Conformity/** **SIL Declaration of Incorporation** Functional Safety according to IEC 61508	2020-02-25

Restrictions

- The safety figures for Safe End Position Feedback function are only valid if the end position switches **directly** wired to the customer connection are used for end position evaluation.
- In "low demand mode" diagnostic of these switches at least 10 times more frequent than the demand rate and the proof test rate via Partial Valve Stroke Test (PVST) (operation mode "end position test" of safety handbook or equivalent) controlled by the Safety PLC is necessary for the safety function "Safe End Position Feedback with PVST".
- The failure rates are only valid if safety switches with extension "-S or "-SIL" are used (e.g. characteristics 8-S, 8.2-S, ...)
- The failure rates are only valid for the useful lifetime (see safety handbook)
- The average operation temperature is assumed to be no higher than 40 °C. If the actual ambient temperatures exceed an average of +40 °C, the lambda values have to be incremented by a safety factor.
- The SIL/PL has to be evaluated for the complete (sub)system. The numbers listed are for reference only.

High demand mode is feasible for the safe end position feedback if the following is observed:

- the total number of strokes and cycles allowed for the used actuator type is not exceeded during the useful lifetime and
- the total number of cycles of the end position feedback does not exceed 100.000 during the useful lifetime if control voltages/currents of maximum 30 V AC/DC and 30 mA are applied and
- the total number of cycles of the end position feedback does not exceed 20.000 during the useful lifetime if control voltages/currents of up to 250 V AC/DC and 5A are applied for switches with silver contacts and
- the total number of cycles of the end position feedback does not exceed 20.000 during the useful lifetime if control voltages/currents of up to 50 V AC/DC and 400mA are applied for switches with gold contacts and
- every 20.000 cycles of the end position feedback the crown wheel and worm wheel are checked for wear and exchanged if necessary and
- the user has to ensure that for the safety function "Safe End Position Feedback" a test rate (PVST) per the requirements of the applicable standard(s) is achieved.
- the grease is exchanged at least every 10 years or earlier if necessary.

*1) FIT = Failure In Time, Number of failures per10^9 h
*2) DC_D = Diagnostic Coverage (dangerous)
*3) PFD_{avg} = Probability of a failure on demand (average)
*4) Depending on the application and possible external diagnostics a higher DC and therefore also a higher category and a higher Performance level might be possible to achieve.

Index

AUMA Riester GmbH & Co. KG

P.O. Box 1362
DE 79373 Muellheim
Tel +49 7631 809 - 0
Fax +49 7631 809 - 1250
info@auma.com
www.auma.com

Y006.653/003/en/1.21