Fail safe unit in SIL version

FQM 05.1 – FQM 12.1 /FQMEx 05.1 – FQMEx 12.1

with non safety-related actuators

SQ 05.2 – SQ 12.2/SQR 05.2 – SQR 12.2

SQEx 05.2 – SQEx 12.2/SQREx 05.2 – SQREx 12.2

with actuator controls

AC 01.2/ACExC 01.2

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.

The safety manual is primarily intended for consultants, operators, service staff and managers setting up, operating or maintaining safety instrumented systems (SIS) equipped with FQM / FQMEx fail safe unit. Together with the reference documents, the present safety manual provides all information required for safe SIS integration, operation and maintenance of the FQM / FQMEx fail safe unit.

Reference documents:

- Operation instructions (Assembly, operation, commissioning) for actuator.
- Operation instructions (Assembly, operation, commissioning) Fail safe unit.
- Manual (Operation and setting) AC 01.2/ACExC 01.2 actuator controls.
- Manual (Device integration Fieldbus) AC 01.2/ACExC 01.2 actuator controls.
- Technical data referring to the fail safe unit, the actuator and actuator controls.
- Declaration of incorporation and EU declaration of conformity for the fail safe unit.
- SIL Declaration of Conformity on functional safety (order related)

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

Table of contents

		Page
1.	**Terminology**	**4**
1.1.	Abbreviations and concepts	4
2.	**Application and validity**	**6**
2.1.	Range of application	6
2.2.	Standards	6
2.3.	Valid device types	6
3.	**Architecture, configuration and applications**	**8**
3.1.	Architecture (actuator sizing)	8
3.2.	Configuration (setting)/version	8
3.3.	Further notes and indications on architecture	10
3.4.	Applications (environmental conditions)	10
4.	**Safety instrumented systems and safety functions**	**11**
4.1.	Safety instrumented system including an actuator	11
4.2.	Safety functions	11
4.3.	Safe inputs and outputs	12
4.4.	Redundant system architecture	12
4.5.	Examples of applications	13
4.6.	System representation	14
4.7.	Diagnostic function by the operator	14
4.8.	Internal diagnostics of fail safe unit	15
5.	**Installation, commissioning and operation**	**16**
5.1.	Installation	16
5.2.	Commissioning	18

5.3. Operation 18
5.4. Lifetime 18
5.5. Decommissioning 18
5.6. Disposal and recycling 19

6. Indications 20

7. Signals 21
7.1. Signals via FS module 21
7.2. Status signals via output contacts (digital outputs) of actuator controls 21
7.3. Signals via fieldbus of actuator controls 21

8. Tests and maintenance 22
8.1. Safety equipment: check 22
8.2. Internal actuator monitoring with control via actuator controls 22
8.3. Partial Valve Stroke Test (PVST): execute 23
8.4. Proof test (verification of safe actuator function) 24
8.4.1. ESD operation (Safe OPENING/CLOSING): check 24
8.4.2. ESD operation (Safe OPENING/CLOSING) with additional tripping in case of mains failure: check 25
8.4.3. Safe end position signal: check 26
8.5. Maintenance 27

9. Safety-related figures 28
9.1. Determination of the figures 28
9.2. Specific figures for fail safe unit in SIL version with actuators of SQ .2 series 28

10. Checklists 32
10.1. Commissioning checklist 32
10.2. Proof test checklists 32
10.2.1. Safe ESD safety operation (Safe OPENING/CLOSING) 32
10.2.2. Review and validation of the “Safe end position feedback” safety function 33

11. SIL Declaration of Conformity (example) 36

Index 40

Addresses 41

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**ailure **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.

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)

Actuator controls shall be regarded as **type A** devices 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 %).

Actuator controls shall be regarded as **type B** devices if one or several of the following conditions are met:

- The failure of at least one constituent component is not well defined.
- The fault behaviour 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.

Fail safe operating time/ ESD duration/ Fail safe travel time

The terms fail safe operating time, ESD duration and fail safe travel time are used as synonyms in the documents on the fail safe unit. They specify the operating time required to execute on demand of ESD function (operation via constant force spring) the operation from the opposite end position into the safety end position.

In contrast, the operating time in standard operation specifies the time required to operate the valve via electric actuator from one end position to the opposite end position.

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.

The fail safe unit is part of the actuator and capable to operate the connected valve once into a previously defined safety position and remain in this position without external energy supply.

Hardware, software and configuration of the fail safe unit and the pertaining actuator may 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 fail safe unit.

The user may only deploy the fail safe unit within safety instrumented systems once the following is ensured:

- The fail safe unit may only be operated in low demand mode.
- All materials, environmental and process conditions must be compatible with the manufacturer data and the restrictions by AUMA (refer to technical data sheet and operation instructions in particular).
- All activities specified in this safety manual must be performed and defined restrictions be heeded.
- All application restrictions indicated in the operation instructions, the technical data and the order-related Declaration of Incorporation must be heeded.

When deploying the fail safe unit within a SIS, IEC 61508, IEC 61511 or the applicable product standard must be heeded.

Materials, environmental conditions and process conditions must be compatible with the manufacturer's indications and AUMA's restrictions.

All activities specified in this safety manual must be performed and defined restrictions be heeded.

2.2. Standards

The safety-related part of the fail safe unit was developed and evaluated in compliance with IEC 61508 Ed. 02. Safety figures were calculated and an FMEDA was executed.

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		
Fail safe unit	**Actuator**	**Actuator controls**
FQM 05.1 – FQM 12.1 in SIL-V1.0.00 version	SQ 05.2 – SQ 12.2	AC 01.2
FQMEx 05.1 – FQMEx 12.1 in SIL-V1.0.00 version	SQEx 05.2 – SQEx 12.2	ACExC 01.2

Approved versions and configurations of the safety-relevant part of the fail safe unit are described in AV 06.03.020.xx "Working specifications for FQM in SIL version".

Information In applications with requirements on functional safety, only AUMA fail safe units in SIL version may be used. AUMA fail safe units in SIL version can, among others, be identified by the characters "SIL-V1.0.XX" following the ESD designation: ... on the name plate. "xx" are wildcard characters for a two-digit number.

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



3. Architecture, configuration and applications

3.1. Architecture (actuator sizing)

For actuator architecture (actuator sizing) including a fail safe unit, the maximum torques, run torques and operating times are major factors be 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, defective thyristors, heating up or damage to cables.

→ Imperatively heed the technical data of both actuator and fail safe unit for actuator architecture.

→ Sufficient reserves have to be provided to ensure that the actuator paired with the fail safe unit are capable of reliably opening or closing the valve even in the event of an accident or undervoltage.

For the guaranteed (minimum) torque provided by the fail safe unit during fail safe operation, refer to the technical data pertaining to the product. The maximum torque acting upon the valve is twice the amount indicated in the data. Torque peaks occurring during sudden braking, e.g. while approaching the end position of comparatively rigid valves are, however, excluded. They may also occur when demanding the ESD function and the valve is blocked at the same time (i.e. has already reached the fail safe end position). The excessive torque rate of these torque peaks depends among others on the weight and the rigidity of the valve and may significantly exceed the mentioned factor of 3.

During ESD operation, the constant force spring of the fail safe unit will operate the valve at nominal torque to the end position and maintain the position. This will also apply if a reduced torque (range) was selected for standard operation with the electric actuator.

To prevent valve damage during safety operation, we recommend, depending on the stiffness, sizing the valve to at least 3 times the maximum actuator torque.

During initialisation, no torque may be applied in opposite fail safe direction. For this reason, the fail safe unit is not suitable for applications with butterfly valves in which pressure or torque is applied in opposite fail safe direction while in the safety position.

Like any switch, the end position switches have a certain hysteresis. For this reason, the end position switches are slightly operated prior to reaching the mechanical end stop already signalling the end position. The soft signalling behaviour is identical to leaving the end position, only once they have left the mechanical actuator end position. Precise setting of end positions/end stops can considerably minimise this behaviour.

The torque applied at the actuator side input of the FQM must not exceed the nominal torque indicated in the technical data pertaining to the FQM.

For further environmental conditions such as vibration, temperature, ... which have to be heeded when specifying the architecture, refer to the indications in both technical data and operation instructions

For applications critical to safety, protection against unauthorised operation has to be provided. Depending on the project-specific risk assessment, this may take the form of a special screw, access control (e.g. fence) or other measures.

3.2. Configuration (setting)/version

Configuration (setting) of safety-related functions is defined in the factory during fail safe unit assembly and validated during final inspection. Subsequent modification of the configuration by the plant operator is not permissible. Exception: Setting of the end stops (refer to operation instructions) and – within certain limits – setting of the fail safe operating time (see below).

General functions are set as described in the Operation instructions or the Manual (Operation and setting) AUMATIC AC 01.2.

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

The operating time for fail safe operation can be set – within certain limits:

- In the factory, one of two configurations (10 % or 30 %) is selected for the point from which the fail safe operation is decelerated when approaching the end position (refer to wiring diagram: Switch 30%). This setting cannot be changed.
- Bridges between connections XF 31-34 within the electrical connection can influence the speed of the fail safe operation in four stages: This setting can be changed in the field (on site).

The <Typical fail safe operating times under standard conditions> shows the relation between the typical fail safe operation time under standard conditions (see note below) the configuration of the switch 30% specified in the factory, as well as the configuration of XF 31-34 terminals. The minimum operating time under standard conditions amounts to 50 % of the indicated values, the maximum operating time under standard conditions amounts to 200 % of the indicated values.

Information

- The indicated typical minimum and maximum fail safe operating times refer to a swing angle of 90°.
- The indicated typical minimum and maximum fail safe operating times refer to the absolute end stop setting of the fail safe end position as set in the factory and a load profile in accordance with EN 15714-2:2009 (standard conditions).
- The indicated typical minimum and maximum fail safe operating times require the ESD demand to remain present while the fail safe function is executed (fail safe operation). Should the ESD demand be cancelled while executing the fail safe operation, the actuator will nevertheless run to the fail safe end position. The indicated operating times might, however, not be respected.
- The typical operating time exclusively applies at normal temperature.

For different swing angles, absolute end stop settings in the fail safe end position (even if the swing angle remains unchanged at 90°) and load profiles, the operating time will change accordingly. In this case, the tolerance of the fail safe operating time of –50 %/+100 % does not refer to the values indicated in the <Typical fail safe operating times under standard conditions > table, but to the new typical fail safe operating time generated by the modified configuration. A malfunction of the electric actuator or the actuator controls can also have an impact on the fail safe operating time (refer to <Safety functions> chapter).

Information

If the operating time is changed in the field via XF 31-34 terminals, the following tests and checks must at least be performed:

- Proof test according to <Proof test> chapter.
- Measurement of fail safe operating time during the proof test and/or real service conditions.
- Check whether the measured fail safe operating time meets the values indicated in the <Typical fail safe operating times under standard conditions> table (while observing the Information above) or the requirements of the application.

Table 3:

Typical fail safe operating times under standard conditions (in seconds)								
30% switch	Configuration: 30 %/max. Fail-Safe operating time				Configuration: 10 %/min. Fail-Safe operating time			
Bridge between XF … and XF …	None	XF 31-32	XF 31-33	XF 31-34	None	XF 31-32	XF 31-33	XF 31-34
FQM 05.1	18	22	28	34	09	15	21	29
FQM 07.1	14	18	22	26	08	12	18	23
FQM 10.1	28	35	45	54	15	24	35	47
FQM 12.1	21	27	34	39	13	20	28	35

Configuration options for safety function

Table 4: Configuration options for safety function

Configuration SIL function	Short description	Initiated by	
Safe ESD CLOSE	Safe CLOSING	ESD	ESD or mains failure
Safe ESD OPEN	Safe OPENING	ESD	ESD or mains failure
Safe end position feedback	Signal is issued whether one of both end positions (OPEN/CLOSED) is reached.	–	–

3.3. Further notes and indications on architecture

- Systematic capability is SC03
- A common cause failure (CCF) of 10 % is to be assumed, except if the analysis shows, that a lower CFF can be applied.
- This is a type A device.
- When using a fail safe unit, HFT = 0.
- For required diagnostic actions, refer to chapter <Safety instrumented system including an actuator>.

3.4. Applications (environmental conditions)

When specifying and using the actuators and the fail safe unit 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. Refer to <Specific figures for fail safe unit in SIL version with actuators of SQ .2 series> chapter.

For environmental testing, the fail safe unit was subjected to tests according to the following standards:

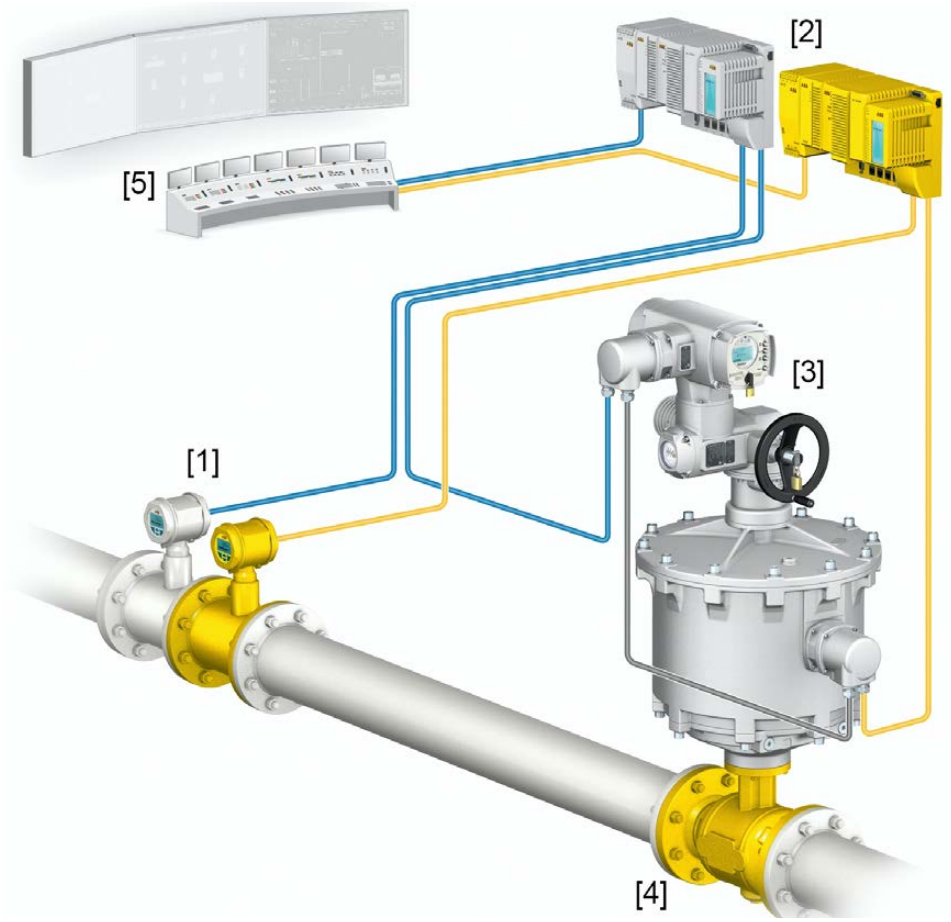
- Dry heat: EN 60068-2-2
- Damp heat: EN 60068-2-30
- Cold: EN 60068-2-1
- Vibration (sinusoidal): IEC 60068-2-6
- Degree of protection test IP68: EN 60529
- Immunity level: EN 61000-6-7
- Emission: EN 61000-6-4

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 2: Typical safety instrumented system



[1] Sensor
[2] Controls (standard and safety PLC)
[3] Actuator with actuator controls and FQM
[4] Valve
[5] DCS

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

For an individual component (e.g. fail safe unit), safety figures are determined. These figures are used to assign the devices to a potential safety integrity level (SIL). The final classification of the safety instrumented system can only be made after assessing and calculating all subsystems.

4.2. Safety functions

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

- Safe ESD OPEN/CLOSE: safe OPENING/CLOSING)
  - Fail safe position: Fail safe unit operates in the defined operating time into the configured fail safe position (OPEN/CLOSED).
  - Safe state is reached if the FQM has operated the mounted valve into the defined safety end position (OPEN/CLOSED) or the safe state is maintained by the FQM.
  - The safety end position is reached if the FQM has reached the internal end stop or the valve end stop at the defined position (OPEN/CLOSED).
- Safe end position feedback
  - Fail safe position: Depending on the application, the fail safe position can differ. Consequently, no true fail safe position can be specified. An unexpected limit switch signal can present a potential danger.

Depending on the configuration, the safe ESD function can be triggered either by a signal (ESD input = 0 V DC) or by mains failure.

The different configuration options of the safety functions are described in the <Configuration (setting)/version> chapter.

It is not possible to interrupt the execution of the safety function “Safe OPENING/CLOSING”.

“Safe OPENING/CLOSING” safety function is only available if the “FS ready” signal is present. Demand of the safety function leads to the removal of the “FS ready” signal. For the signal behaviour of the FS ready NO/FS failure NC outputs, please refer to <Installation> chapter.

The operating time for the fail safe unit is defined for a load according to EN15714-2 for a 90° swing angle. Deviating loads or changing swing angles requires new operating time determination.

In case the actuator causes a fault leading to an operation in opposite direction to the fail safe direction, it is likely that the fail safe operating time is extended by the actuator travel time.

Availability of the “Safe end position feedback” safety function is independent from the “FS ready” signal.

“Safe end position feedback” and “Safe OPENING/CLOSING” safety functions are simultaneously available.

In each fail safe unit, only one of the “Safe OPENING” and “Safe CLOSING” safety functions is available.

4.3. Safe inputs and outputs

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

- ESD

Safe outputs:

- FS failure NC (safety function ready/not ready)
- FS ready NO (safety function ready/not ready)
- LSO 19-20=NC (safe end position feed back OPEN)
  LSO 19-21=NO (safe end position feed back OPEN)
- LSC 22-23=NC (safe end position feed back CLOSED)
  LSC 22-24=NO (safe end position feed back CLOSED)

For detailed information on safe inputs and outputs, refer to <Configuration (setting)/version> chapter and <Installation> chapter.

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 actuator with fail safe unit into the safety instrumented system. The decision on the appropriate version depends on the entire system. Considering the illustrated redundant system setup, the actuator paired with actuator controls and fail safe unit complies with Safety Integrity Level SIL 3 for the Safe ESD function according to IEC 61508.

Figure 3: Redundant system with safe ESD for safe CLOSING



Figure 4: Redundant system with safe ESD for safe OPENING



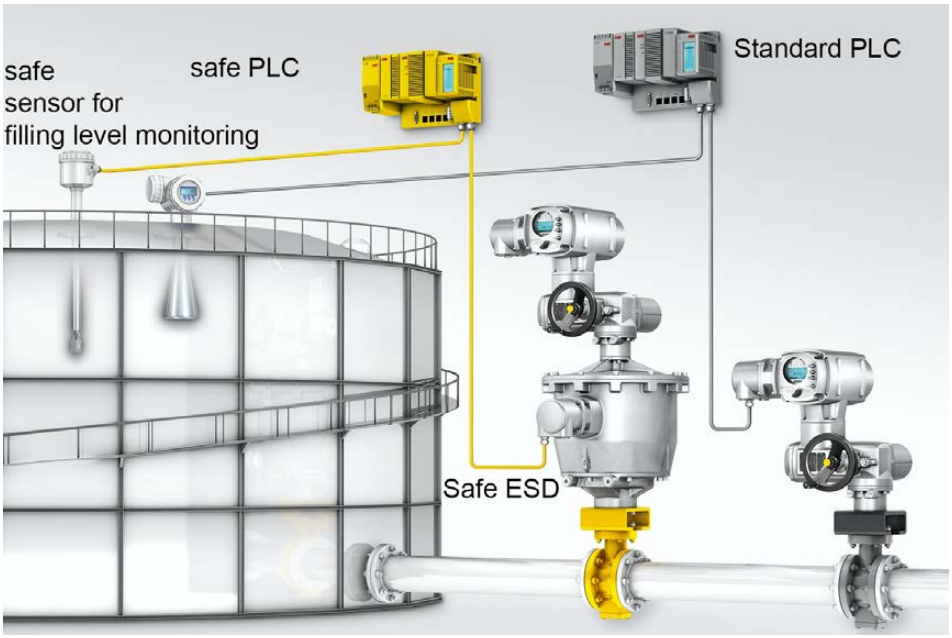
Information There is no reasonable option to create a redundant system for safe end position feedback using two fail safe units.

4.5. Examples of applications

Safe CLOSING of a tank farm using the Safe ESD function

Standard PLC controls the overall system for filling the tank. A system fault occurs if the filling level or the tank pressure exceed the permissible specified level. In this case, the safety PLC immediately closes the valve for tank filling.

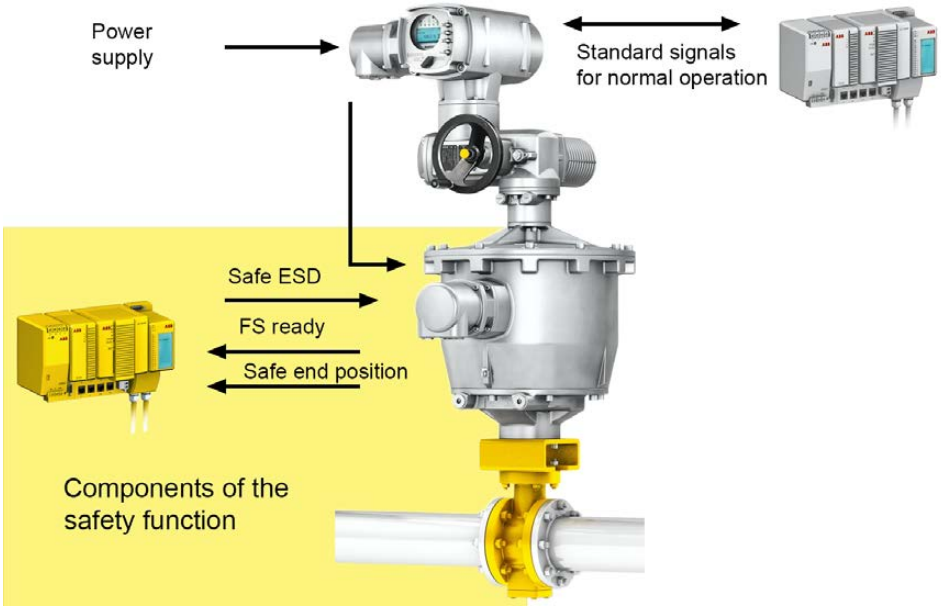
Figure 5: Application example: Overflow protection in a tank farm



4.6. System representation

The representation below shows the simplified design of fail safe unit in SIL version.

Figure 6: Simplified system representation



4.7. Diagnostic function by the operator

In addition to the already available internal diagnostics within the fail safe unit, further diagnostic features are required by the safety PLC. Once a fault has been detected, the system has to be checked immediately and the installation has to be put in a safe state, if required.

The following items are indications for potential FQM faults and must be continuously monitored by the safety PLC:

- If based on the standard operational status of the fail safe unit (“FS ready” signal and ESD high level input), the `FS ready NO`/`FS failure NC` outputs change to “FS fault” signal.

- If a service demand or diagnostic operation (PVST/FVST) was started from the end position and if within the respective available SQ operating time, the end position switch is not released.
- If during automatic initialisation (start by applying ESD high level input) the maximum initialisation time (2 minutes) is exceeded and if subsequently the ESD high level (not requested) is still applied as well as the “FS fault” (fail safe not ready) is signalled.
- If ESD is demanded (ESD low level) and the safety end position is not reached within the maximum defined fail safe operating time (typical operating time –50 %/+100 %).
- If based on the standard operation status of fail safe unit (“FS ready” and ESD high level input), the “Safe OPENING/CLOSING” safety function is requested (ESD low level input) and the FS ready NO output does not change to “FS fault” within the provided reaction time (1 second).

Information

- Reaction time for power supply interruption for respective configuration is up to 10 seconds.
- The “FS fault” signal will not automatically trip the ESD function. The signal indicates that execution of the safety function cannot be guaranteed. Exceptions are if the “FS fault” signal was caused by the constant force spring switch or a fault within the toggle lever so that it can no longer lock the spring. In both cases, the ESD function will be tripped in addition to the “FS fault” signal.
  Even if the FS ready NO/FS failure NC outputs signal an “FS- fault”, standard operation into the fail safe position by means of the electric actuator or an ESD operation on demand of the ESD function at the ESD input of the fail safe unit might still be possible.
- If a fault is detected during one of the diagnostics performed by the operator, the system must immediately be checked and if required the plant be operated to a safe state.

4.8. Internal diagnostics of fail safe unit

The following internal diagnostic features are available within the fail safe unit:

- Internal temperature monitoring, leading to the issue of “FS fault” signal in case of deviation from internally permissible operational temperature.
- Internal voltage monitoring of ESD input, leading to the issue of “FS fault” signal in case of deviation from internally permissible level.
- Internal monitoring of the constant force spring and further mechanical components, leading to the issue of “FS fault” signal in case of deviation from the specifications defined as permissible.
- During initialisation, “high” level is present at the ESD input and the “FS fault” signal is active. An internal diagnostic function of the fail safe unit verifies whether all conditions required for completion of the initialisation are met (in particular: spring fully wound, toggle lever locked). Once these conditions are met, the “FS fault” signal will be replaced by the “FS ready signal”.

Information

The “FS fault” signal will not automatically trip the ESD function. The signal indicates that execution of the safety function cannot be guaranteed. Exceptions are if the FS fault signal was caused by the constant force spring switch or a fault within the toggle lever so that it can no longer lock the spring. In both cases, the ESD function will be tripped in addition to the “FS fault” signal.

Even if the FS ready NO/FS failure NC outputs signal an “FS- fault”, standard operation into the fail safe position by means of the electric actuator or an ESD operation on demand of the ESD function at the ESD input of the fail safe unit might still be possible.

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 must be carried out exclusively by suitably qualified personnel.

Opening covers or unfastening screws is only permitted if the pertaining description is available in this manual or in the operation instructions.

⚠ WARNING

Risk of injury caused by high spring tension!

The fail safe unit includes springs which are subject to high tension. When opening the housing without expert knowledge, the tension release of these springs might be out of control.

→ Do NOT open FQM housing.

The plant operator is responsible for ensuring power supply protection against overvoltage and undervoltage.

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.

Install cables as to keep interference on signal cables to minimum (cable installation in accordance with EMC). The following points should be heeded in particular:

- Signal cables are susceptible to interference. Motor cables are interference sources. Lay cables being susceptible to interference or sources of interference at the highest possible distance from each other.
- Lay signal cables as close to the earth potential as possible to increase the immunity status.
- If possible, avoid laying long cables and make sure that they are installed in areas being subject to low interference.
- Avoid long parallel paths with cables being either susceptible to interference or interference sources.

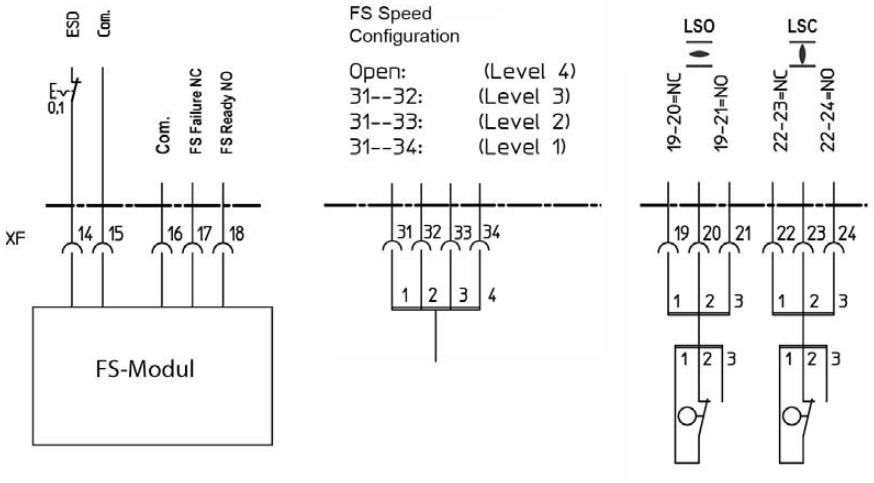
Low temperature version must be deployed for operation at ambient temperatures below -30 °C. Power supply must be provided for the integral heating system.

The fail safe unit may be stored at ambient temperatures between –60 °C and +80 °C. Low temperature version must be deployed for operation at ambient temperatures below -40 °C. Power supply must be provided for the integral heating system.

Safety functions are connected via the FS module integrated in the fail safe unit.

`FS failure NC` and `FS ready NO` outputs must be connected to a SIL 2 compatible input of a safety PLC and assessed.

Figure 7: Connections for safety functions via FS module



Switching behaviour of ESD input:

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

Permissible input voltage range:

- High level: +24 V DC (–15 %/+20 %)
  Current consumption: approx. 1 A, max. 1,2 A
- Low level: max. 5 V DC

Signal behaviour of the FS `ready NO`/FS `failure NC` outputs:

- Safe ESD function is ready, no fault detected by diagnostic tests is present:
  FS `ready NO` output (NO contact) = **closed**
  FS `failure NC` output (NC contact) = **open**
- Safe ESD function is NOT ready or a fault was detected:
  FS `ready NO` output (NO contact) = **open**
  FS `failure NC` output (NC contact) = **closed**

Signal behaviour of LS outputs:

- **End position OPEN reached** (XF 19 – 21 terminals) or **End position CLOSED reached** (XF 22 – 24 terminal), i.e.:
  Output at XF 19-21=NO or XF 22-24=NO (NO contact) terminals = **closed**
  Output at XF 19-20=NC or XF 22-23=NC (NC contact) terminals = **open**

Permissible load at FS `ready NO` and LSO/LSC outputs:

- Voltage range: 5 – 30 V
- Current range 2 – 100 mA

Table 5: Example (refer to wiring diagram pertaining to order)

Designation Wiring diagram	Signal	Customer connections
ESD	Digital input for Safe ESD function	XF 14
Com.	Reference potential for Safe ESD	XF 15
FS Ready NO	NO contact for FS ready/FS fault signals	XF 18
FS Failure NC	NC contact for FS ready/FS fault signals	XF 17
FS ready com.	Reference potential for FS ready/FS fault signals	XF 16
LSO 19-20=NC	NC contact of LSO signal (end position OPEN)	XF 20
LSO 19-21=NO	NO contact of LSO signal (end position OPEN)	XF 21
	Reference potential for LSO signal	XF 19

Designation Wiring diagram	Signal	Customer connections
LSC 22-24=NO	NO contact of LSC signal (end position CLOSED)	XF 24
LSC 22-23=NC	NC contact of LSC signal (end position CLOSED)	XF 23
	Reference potential for LSC signal	XF 22

For further information on FS faults and in particular for troubleshooting support, refer to <Indications> chapter and the operation instructions pertaining to the fail safe unit FQM 05.1 – FQM 12.1/FQMEx 05.1 – FQMEx 12.1.

5.2. Commissioning

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

Information

The following faults may occur if the end stop setting within the fail safe unit or the limit switch setting in the actuator are incorrect or imprecise:

- Valve is not completely closed (if the FQM end stop is reached prematurely)
- No end position feedback signal in spite of closed valve (since limit switches have not tripped)

Information

During Safe ESD function, an operation into the safe position with wound spring is possible irrespective of settings or service condition of electric actuator. This means, the safe fail unit can start operation at any time once the safety function has been triggered.

The safe function must be verified when finalising commissioning. This verification can be made by applying the proof test. Refer to chapter <Proof test (verification of safe actuator function)>

5.3. Operation

Prerequisite for safe operation is the regular maintenance and device checks at the T_{proof} intervals as defined by the operator. The parameters indicated in the <Safety figures> chapter are valid for T_{proof} = 1 year.

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

In case of possible failures or defects of the safety system, 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.

Safety-related parameters are valid for the cycles or modulating steps defined in the technical data specifications 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. These measures must at least include a service by AUMA Riester GmbH & Co. KG.

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.

- Decommissioning may only be performed in FQM fail safe end position (spring unwound).

⚠ WARNING

Risk of injury caused by high spring tension!

The fail safe unit includes springs which are subject to high tension. When opening the housing without expert knowledge, the tension release of these springs might be out of control.

→ Do NOT open FQM housing.

5.6. Disposal and recycling

Our devices have a long lifetime. However, they have to be replaced at one point in time. The devices have a modular design and may, therefore, easily be separated and sorted according to materials used, i.e.:

- various metals
- plastics
- greases and oils

The following generally applies:

- Greases and oils are hazardous to water and must not be released into the environment.
- Arrange for controlled waste disposal of the disassembled material or for separate recycling according to materials.
- Observe the national regulations for waste disposal.

6. Indications

Indications at actuator controls which are only available in combination with fail safe units, are described in the FQM operation instructions.

General indications as well as settings and operation are described in the operation instructions pertaining to the actuator as well as in the Manual (Operation and setting) AC 01.2/ACExC 01.1 actuator controls.

Information

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.

7. Signals

7.1. Signals via FS module

The integral FS module signals a fail safe fault via the fault relay (FS ready NO or FS failure NC outputs). Only these signals may be used in a safety-related system.

For signal behaviour of the FS Ready NO/FS Failure NC outputs and end position signals via LS outputs, please refer to chapter <Installation>.

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

7.2. Status signals via output contacts (digital outputs) of actuator controls

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

Information Status signals via DOUT outputs 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.

Available signals and their signification are described in the operation instructions pertaining to the fail safe unit.

7.3. Signals via fieldbus of actuator controls

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

Information 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.

Available signals and their signification are described in the operation instructions pertaining to the fail safe unit.

8. 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.

Within the lifetime of 10 years or the maximum number of cycles or modulating steps indicated in the <Lifetime> chapter, the fail safe unit will not require any maintenance. However, the required tests (including proof test and online diagnostics in particular) must be performed at specified intervals and in compliance with the procedures and intervals described in the present safety manual.

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.

8.1. 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.

8.2. Internal actuator monitoring with control via actuator controls

The device, consisting of actuator with actuator controls and integral fail safe unit has an internal actuator monitoring. In standard operation, the internal actuator monitoring is automatically executed by operating the actuator from the end position.[1)]Internal actuator monitoring identifies most of the safety-related actuator components of the safe fail unit. If a fault occurred, the fault would be signalled via the output contact of the FS module (`FS ready NO` and `FS failure NC` outputs).

To ensure the exemplary safety figures of the Safe ESD safety function, in particular PFD, specified in the <Safety-related figures> chapter, the device has to be controlled at least once per month via the actuator controls and additionally the output contact assessment of the fail safe module (`FS ready NO` and `FS failure NC` outputs). The safety PLC must monitor if the end position switch signals in the expected order “end position -> no end position -> end position”. If it cannot be ensured that the device is controlled by the actuator controls at least once per month, a <Partial Valve Stroke Test (PVST)> has to be performed instead.

The control signal and the related actuator operation must be applied for the time required to ensure that the end position switch signals the unseating from the end position.

Since diagnostic functions are not exclusively performed within FQM but have to be initiated and/or evaluated by the safety PLC, other diagnostic test intervals are possible as 1 x per month. The consequence, however, is that the safety-related parameters and in particular the PFD will change. Furthermore, for diagnostic test interval selection by the operator, it must be considered, that the test frequency should amount to at least 10 times the demand rate and that – for the ESD safety function – the test interval can never be less than 22 days (refer to next paragraph).

Internal diagnostics of the mechanical elements are designed so that they will be executed every 22 days maximum – even in case of frequent standard operations – thus avoiding excessive wear. To guarantee a test interval e.g. of one month, the operator has to ensure that 22 days up to one month after the last diagnostic operation, either standard operation or a PVST is started from one of the end positions.

An FVST (Full Valve Stroke Test) or a standard operation may replace the PVST provided that the operation is signalled to a safety PLC and the safety PLC is programmed as to control the following test sequence.

1) (`LSC` or `LSO` output opens)

If a safe end position feedback is requested for both end positions, PVST must be started out of both end positions. As an alternative, an FVST can be used for this test.

8.3. Partial Valve Stroke Test (PVST): execute

The PVST procedure is identical for both safety functions.

There are two options for performing the PVST.

1. **Performing the PVST using the standard function of AC .2:**
   In standard operation, the actuator is controlled via the standard PLC and AC .2. For PVST, the operation sequence “end position -> no end position -> end position” is executed. During operation, the safety PLC monitors the following states or events:
   - Is the actuator in one of the end positions prior to the PVST? Monitoring is made via safe end position feedback of FQM.
   - Does the PVST start or is the safety PLC informed about the start of the PVST via the standard PLC or the AC .2?
   - Does the actuator unseat from the end position within the predefined PVST operating time? Monitoring is made via safe end position feedback of FQM.
   - Has the actuator returned to the initial end position once the action is complete? Monitoring is made via safe end position feedback of FQM.
   - Has a fault been signalled via the output contact (FS module: FS `readyFS failure NC`) during PVST operating time?

2. **Performing the PVST using the PVST function of AC .2:**
   If AC .2 actuator controls 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:
   - A digital input of actuator controls (galvanically separated from the other inputs) is configured to the following value: Execute PVST (949)
   - The safety PLC directly controls the PVST or will also receive the control signal if the PVST input is controlled.
   - The PVST is performed with the following operation mode setting: Parameter PVST operation mode M0889 = End position test
   - The PVST may only be performed from one of the end positions.
   - PVST operating time M0890 parameter must be set to ensure that unseating from the end position will always be performed.

   The safety PLC monitors the following states or events while the AC .2 actuator controls execute the PVST.
   - Is the actuator in one of the end positions prior to the PVST? Monitoring is made via safe end position feedback of FQM.
   - Does the PVST start or is the safety PLC informed about the start of the PVST via the standard PLC or the AC .2?
   - Does the actuator unseat from the end position within the predefined PVST operating time? Monitoring is made via safe end position feedback of FQM.
   - Has the actuator returned to the initial end position once the action is complete? Monitoring is made via safe end position feedback of FQM.
   - Has a fault been signalled via the output contact (FS module: FS `ready`) during PVST operating time?

The following applies to both procedures: **The PVST was successful if the following conditions are met:**

- At the beginning of the PVST, the actuator was in one of the two end positions.
- The actuator has unseated from this end position during the PVST.
- At the end of the PVST, the actuator is in the same end position as prior to the PVST.
- The FS module has **not** signalled a fault via the output contact (FS module: FS `ready`) during PVST operating time?

We also recommend assessing PVST fault (953) and PVST abort (954) signals of the actuator controls. Assessment must not necessarily be performed by the safety PLC.

If this is not the case, the device has to be checked in accordance with the steps in the <Proof test> chapter.

8.4. 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 failures which might remain undetected until a safety function is started and consequently result in a potential danger.

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

Prior to starting the proof test procedure/procedures described before, the preliminary tests below must be performed.

- Visual inspection for excessive corrosion and possible damage.
- Checking and if required tightening all screws used in the connection between FQM fail safe unit and SQ part-turn actuator. Tightening torque: FQM 5.1/7.1: 24 Nm, FQM 10.1/12.1: 82 Nm

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

1. Check Safe ESD safety operation (Safe OPENING/CLOSING)
2. Check fail safe fault signal.
3. Check Safe ESD reaction to “safe end position feedback” (assessment of end position switch).

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 of the proof test steps, please refer to the following sections.

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 safety-related figures depend on the selected proof test interval (refer to <Safety-related figures> chapter).

In any case, the safety-related functions must be checked after commissioning and following any maintenance work or repair after changing the fail safe operating time as well as during 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.

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

8.4.1. ESD operation (Safe OPENING/CLOSING): check

Configuration The test is valid for all versions with Safe ESD function.

Test procedure A safety operation in direction of the configured fail safe position must be triggered.

Test sequence

1. Operate actuator into end position OPEN (Safe ESD in direction CLOSE), or into end position CLOSED (Safe ESD in direction OPEN).

   Information: For the test, operation commands (in directions OPEN or CLOSE) can be executed both from Remote (via DCS) and from Local at the controls (via the push buttons of the local controls).

➥ **No** fail safe fault signal may be present (“FS ready” signal).

2. Initiate safety operation:
   → First set ESD input signal to 0 V (low).
   → When leaving the end position, start the operating time measurement.
   ➥ The FQM end position switch indicates the unseating from end position by signal change.
   ➥ A fail safe fault signal (“FS fault” signal) must be issued.
   → Stop operating time monitoring when reaching the fail safe end position.
   ➥ The FQM end position switch indicates that end position has been reached by signal change.
   ➥ The FQM operating time must comply with the indication on the name plate for 90° swing angle or the specified time during commissioning. The permissible operating time tolerance –50 %/+100 %.
   → Check whether valve is completely closed.
3. Once the test is complete, set ESD input signal to +24 V DC (high) .

➥ FQM starts automatic initialisation (spring is wound).

➥ After successful initialisation, the “FS ready” signal is issued once initialisation is complete. Initialisation time must be < 2 minutes.

8.4.2. ESD operation (Safe OPENING/CLOSING) with additional tripping in case of mains failure: check

Configuration

This test applies **in addition** for all versions with additional tripping in case of mains failure of the safety function.

Test procedure

A further safety operation in direction of the configured fail safe position must be triggered through the mains voltage.

Test sequence

1. Operate actuator into end position OPEN (Safe ESD in direction CLOSE), or into end position CLOSED (Safe ESD in direction OPEN).
   Information: For the test, operation commands (in directions OPEN or CLOSE) can be executed both from Remote (via DCS) and from Local at the controls (via the push buttons of the local controls).

➥ **No** fail safe fault signal may be present (“FS ready” signal).

2. Initiate safety operation:
   → Interrupt the FQM power supply.
   Information: Reaction time upon interruption is up to 10 seconds.
   → When leaving the end position, start the operating time measurement.
   ➥ The FQM end position switch indicates the unseating from end position by signal change.
   ➥ A fail safe fault signal (“FS fault” signal) must be issued.
   → Stop operating time monitoring when reaching the fail safe end position.
   ➥ The FQM end position switch indicates that end position has been reached by signal change.
   ➥ The FQM operating time must comply with the indication on the name plate for 90° swing angle or the specified time during commissioning. The permissible operating time tolerance –50 %/+100 %.
   → Check whether valve is completely closed.
3. Restore voltage supply after FQM check.

➥ FQM starts automatic initialisation (spring is wound).

➥ After successful initialisation, the “FS ready” signal is issued once initialisation is complete. Initialisation time must be < 2 minutes.

8.4.3. Safe end position signal: check

Configuration This test applies for the “SIL function” configuration = **”Safe end position feedback”**.

Test procedure The end position feedback must be immediately issued once the actuator reaches the end position.

Test sequence

1. Operate FQM via actuator into intermediate position.
   → Check FQM end position switch:
   ➥ End position OPEN not reached signal (output signal inactive), i.e.:
   - LSO 19-20=NC (NC contact) output = closed
   - LSO 19-21=NO (NO contact) output = open
   ➥ End position CLOSED not reached signal (output signal inactive), i.e.:
   - LSC 22-23=NC (NC contact) output = closed
   - LSC 22-24=NO (NO contact) output = open
   ➥ **No** fail safe fault signal may be issued (“FS ready” signal).
2. Start operation command in direction CLOSE.
   → Wait until FQM end position switch trips or end position CLOSED has been reached.
   → Check actuator reaction:
   → Operation stopped when reaching end position switch CLOSED?
   ➥ End position OPEN not reached signal (output signal inactive), i.e.:
   - LSO 19-20=NC (NC contact) output = closed
   - LSO 19-21=NO (NO contact) output = open
   ➥ End position CLOSED reached signal (output signal active), i.e.:
   - LSC 22-23=NC (NC contact) output = open
   - LSC 22-24=NO (NO contact) output = closed
   ➥ **No** fail safe fault signal (“FS ready” signal) must be issued.
3. Start operation command in direction OPEN. Measure operating time from CLOSED to OPEN.
   → Wait until FQM end position switch trips or end position OPEN has been reached.
   → Check actuator reaction:

   3.1 Operation stopped when reaching end position switch OPEN?
   ➥ End position OPEN reached signal (output signal active), i.e.:
   - LSO 19-20=NC (NC contact) output = open
   - LSO 19-21=NO (NO contact) output = closed
   ➥ End position CLOSED not reached signal (output signal inactive), i.e.:
   - LSC 22-23=NC (NC contact) output = closed
   - LSC 22-24=NO (NO contact) output = open
   ➥ **No** fail safe fault signal may be issued (“FS ready” signal).

   3.2 Did measured operating time from end position CLOSED to end position OPEN match the SQ actuator settings?

4. Operate FQM via actuator into intermediate position.
   → Check FQM end position switch:
   ➥ End position OPEN not reached signal (output signal inactive), i.e.:
   - LSO 19-20=NC (NC contact) output = closed
   - LSO 19-21=NO (NO contact) output = open
   ➥ End position CLOSED not reached signal (output signal inactive), i.e.:
   - LSC 22-23=NC (NC contact) output = closed
   - LSC 22-24=NO (NO contact) output = open
   ➥ **No** fail safe fault signal may be issued (“FS ready” signal).

8.5. 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.

9. Safety-related figures

9.1. Determination of the figures

- The calculation of the safety-related parameters 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.
- The failure rates for mechanical parts are taken from the exida database for mechanical components. 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 PFD value for systems with low demand mode is:
  - 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 including the gearbox should not account for more than approx. 40 % of the permissible total value (PFD_{avg}) of a safety function. This results in the following value:
  - PFD actuator + gearbox for SIL 2 applications: ≲ 4.0E-03
- The fail safe unit is classified as type A component 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).

9.2. Specific figures for fail safe unit in SIL version with actuators of SQ .2 series

The safety-related parameters, in particular PFD, depend on the measures and intervals to be defined by the operator (e.g. T_{Proof}, MRT, ...). Since diagnostic functions are not exclusively performed within FQM but have to be initiated and/or evaluated by the safety PLC, the diagnostic test interval can be defined within certain limits by the operator. For this, respect the following:

- The test frequency should equal at least ten times the demand rate
- The test interval for the ESD safety function must be at least 22 days
- The defined test interval must be considered appropriately in the PFD calculation

The following figure tables provide an example of safety figures for the different versions based on the exemplary assumptions regarding Td and T_{proof}. Complete data records of safety-related parameters referred to as examples of all variants are available within the exida test report. For the relevant parameters with regard to the indications made, refer to the pertaining order-related Declaration of Incorporation.

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 = 95 % (proof test coverage rate [%])
  (PTC for performing the proof test described in this manual)
- T_{proof} = 1 year or as indicated (proof test interval [h])
- $T_{mission}$ = 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)
- MTTR = 802 hours

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

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

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

$$MTTR = Td_ESD + MRT$$

Furthermore, the following assumptions were made:

- The failure rates are constant, wear mechanisms are not included.
- Only one individual component fault leads to failure of the overall system.
- Fault propagation is not relevant.
- All components not included in the safety function and which do not have an impact on the safety function are excluded.
- The system is installed in compliance with the manufacturer's instructions (safety manual).
- Faults caused by maintenance functions or improper operation are specific to locations and consequently not included.
- Materials are compatible with the process conditions.
- All devices are operated in low demand mode.
- For ESD function, the actuator is operated at least at the defined diagnostic test interval to perform internal diagnostics.
- The frequency of diagnostic operations (PVST/FVST) depends on the intervention demanded by the SIS (proof test interval) and the applicable standards.
- The frequency of diagnostic operations is limited internally to 22 days by the FQM to anticipate wear. More frequent operations are easily possible. However, internal diagnostics is not executed by the FQM.
- Only the variants and functions described for the FQM fail safe unit are used for safety applications.
- Internal and external diagnostic options are specified in the safety manual.
- A PVST is executed for the safety function as diagnostic measure.
- Manual operation is not part of the safety function and was consequently not considered.
- The listed electronic failure rates apply for typical service voltage conditions in industrial field environments with temperature limits within the manufacturer evaluation and a mean temperature of 40 °C (35 °C ambient temperature plus internal heating up) across a longer time period. For higher average temperatures, the failure rates shall be multiplied using a field feedback factor of 1.5 for 50 °C, 2.5 for 60 °C and 5 for 80 °C.
- The system limit for failure considerations with regard to FQM is the valve coupling.
  Safe end position feedback is the feedback signal indicating that the coupling has reached the respective position. However, no assessment can be made on potential valve failures.

The following tools were used for calculating the safety figures.

- SILcal V8.0.14 – 64bit
- Microsoft Excel 14.0.7227.5000 – 32 bit

ESD safety function with PVST

Table 6: Safety instrumented figures and failure rates according to IEC 61508-2: 2010

Fault category	Key performance indicators[1)]
λ_{SD}	0
λ_{SU}	273 FIT
λ_{DD}	672 FIT
λ_{DU}	513 FIT
Total failure rate (safety function)	1,458 FIT
SFF[2)]	64 %
DC	56 %
PTC	95 %
SIL AC[3)]	SIL2 (HFT = 0), SIL3 (HFT = 1)
MTBF (years)	51
PFD(T_{Proof}) = 1 year	3.83E-03
PFD(T_{Proof}) = 3 years	8.1E-03
PFD(T_{Proof}) = 5 years	1.24E-02

1) The analysis was performed assuming that PVST faults can be detected by monitoring the end position switch via a safety PLC.
2) To determine the overall SFF (safe failure fraction), the overall final sub-system must be evaluated. The indicated figure is for reference only.
3) SIL AC (architectural restrictions) means, that the calculated values are within the range for hardware architecture restrictions of the respective SIL.

Safe end position with PVST safety function

Table 7: Safety instrumented figures and failure rates according to IEC 61508-2: 2010/IEC 62061

Fault category	Key performance indicators[1)]
λ_{SD}	0
λ_{SU}	0
λ_{DD}	62 FIT
λ_{DU}	39 FIT
Total failure rate (safety function)	101 FIT
SFF[2)]	61 %
DC	61 %
PTC	95 %
SIL AC / SILCL	SIL2
PFD(T_{Proof}) = 1 year	3.0E-04
PFD(T_{Proof}) = 3 years	6.23E-04
PFD(T_{Proof}) = 5 years	9.47E-04

1) The analysis was performed assuming that PVST faults can be detected by monitoring the end position switch via a safety PLC.
2) To determine the overall SFF (safe failure fraction), the overall final sub-system must be evaluated. The indicated figure is for reference only.

Table 8: Safety instrumented figures according to ISO 13849-1

Fault category	**Fault rates**
$MTTF_d$ (years)	1,130 (high)
DC	61 % (low)
Category (CAT)	CAT 1 or CAT 2
Performance Level (calculated)	3.89E-08 1/h
Performance level (reached)[1)]	PL = c

1) The overall safety-related electrical, electronic and programmable electronic control system (SRECS) for machines must be assessed to determine the overall performance level reached. The performance level is indicated for reference only. The calculated performance level is important.

10. Checklists

10.1. Commissioning checklist

Table 9: Commissioning checklist

1. Fail safe unit, actuator and actuator controls correctly wired?	□ ✓
2. Actuator limit and torque switching setting complete?	□ ✓
3. End positions of fail safe unit correctly set?	□ ✓
4. Safe function (depending on the configuration) checked in accordance with the proof test checklists?	□ ✓
5. Commissioning of basic settings (actuator controls) 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 NOTICES contained in the <Tests and maintenance> chapter have to be observed. The test step sequence must be respected.

10.2.1. Safe ESD safety operation (Safe OPENING/CLOSING)

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)

Table 10: Proof test checklist

Configuration Safe CLOSING (ESD in direction fail safe position CLOSED)	✎	**Configuration Safe OPENING (ESD in direction fail safe position OPEN)**	✎
1. Actuator in end position OPEN?	□ ✓	1. Actuator in end position CLOSED?	□ ✓
2. Fail safe fault signal? FS failure NC (NC contact) output = open (“FS ready” signal)	□ ✓	2. Fail safe fault signal? FS failure NC (NC contact) output = open (“FS ready” signal)	□ ✓
3. ESD input signal set to 0 V (low)? (execute operating time measurement)	□ ✓	3. ESD input signal set to 0 V (low)? (execute operating time measurement)	□ ✓
↪ Check reaction of fail safe unit: FQM operates in direction CLOSE? (start of operating time measurement)	□ Yes □ No	↪ Check reaction of fail safe unit: FQM operates in direction OPEN? (start of operating time measurement)	□ Yes □ No
FQM reaches end position CLOSED? (Operating time measurement complete.)	□ Yes □ No	FQM reaches end position OPEN? (Operating time measurement complete.)	□ Yes □ No
FQM operating time corresponds to indications on name plate for 90° swing angle or the configured operating time? Operating time [–50 %/+ 100 %]	□ Yes □ No	FQM operating time corresponds to indications on name plate for 90° swing angle or the configured operating time? Operating time [–50 %/+ 100 %]	□ Yes □ No
↪ Check FS module signal behaviour: Fail safe fault signal? FS failure NC (NC contact) output = close (“FS fault” signal)	□ Yes □ No	↪ Check FS module signal behaviour: Fail safe fault signal? FS failure NC (NC contact) output = close (“FS fault” signal)	□ Yes □ No
4. ESD input signal set to +24 V (high)? Start of time measurement.	□ ✓	4. ESD input signal set to +24 V (high)? Start of time measurement.	□ ✓

Configuration Safe CLOSING (ESD in direction fail safe position CLOSED)	✎	**Configuration Safe OPENING (ESD in direction fail safe position OPEN)**	✎
FQM starts automatic initialisation (spring is wound)	□ ✓	FQM starts automatic initialisation (spring is wound)	□ ✓
↪ Check FS module signal behaviour: Once initialisation is complete, the fail safe fault signal changes to: FS failure NC (NC contact) output = open (“FS ready” signal) Time measurement complete, 2 minutes not exceeded.	□ Yes □ No	↪ Check FS module signal behaviour: Once initialisation is complete, the fail safe fault signal changes to: FS failure NC (NC contact) output = open (“FS ready” signal) Time measurement complete, 2 minutes not exceeded.	□ Yes □ 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.			

Additional proof test checklist for version or configuration:

- Safe ESD function: “Safe CLOSING" (Safe ESD in direction CLOSE) with additional tripping in case of mains failure
- Safe ESD function: “Safe OPENING" (Safe ESD in direction OPEN) with additional tripping in case of mains failure
- Irrespective of type of seating

Table 11: Additional proof test checklist

Configuration Safe CLOSING with additional tripping in case of mains failure (ESD in direction fail safe position CLOSED)	✎	**Configuration Safe OPENING with additional tripping in case of mains failure (ESD in direction fail safe position OPEN)**	✎
1. Actuator in end position OPEN?	□ ✓	1. Actuator in end position CLOSED?	□ ✓
2. Fail safe fault signal? FS failure NC (NC contact) output = open (“FS ready” signal)	□ ✓	2. Fail safe fault signal? FS failure NC (NC contact) output = open (“FS ready” signal)	□ ✓
3. Power supply (mains) of FQM interrupted? (execute operating time measurement)	□ ✓	3. Power supply (mains) of FQM interrupted? (execute operating time measurement)	□ ✓
↪ Check reaction of fail safe unit: FQM operates in direction CLOSE? (start of operating time measurement)	□ Yes □ No	↪ Check reaction of fail safe unit: FQM operates in direction OPEN? (start of operating time measurement)	□ Yes □ No
FQM reaches end position CLOSED? (Operating time measurement complete.)	□ Yes □ No	FQM reaches end position OPEN? (Operating time measurement complete.)	□ Yes □ No
FQM operating time corresponds to indications on name plate for 90° swing angle or the configured operating time? Operating time [–50 %/+ 100 %]	□ Yes □ No	FQM operating time corresponds to indications on name plate for 90° swing angle or the configured operating time? Operating time [–50 %/+ 100 %]	□ Yes □ No
↪ Check FS module signal behaviour: Fail safe fault signal? FS failure NC (NC contact) output = close (“FS fault” signal)	□ Yes □ No	↪ Check FS module signal behaviour: Fail safe fault signal? FS failure NC (NC contact) output = close (“FS fault” signal)	□ Yes □ No
4. Power supply (mains) of FQM restored? Start of time measurement.	□ ✓	4. Power supply (mains) of FQM restored? Start of time measurement.	□ ✓
FQM starts automatic initialisation (spring is wound)	□ ✓	FQM starts automatic initialisation (spring is wound)	□ ✓
↪ Check FS module signal behaviour: Once initialisation is complete, the fail safe fault signal changes to: FS failure NC (NC contact) output = open (“FS ready” signal) End of time measurement, 2 minutes were not exceeded.	□ Yes □ No	↪ Check FS module signal behaviour: Once initialisation is complete, the fail safe fault signal changes to: FS failure NC (NC contact) output = open (“FS ready” signal) End of time measurement, 2 minutes were not exceeded.	□ Yes □ No

10.2.2. Review and validation of the “Safe end position feedback” safety function

Proof test checklist for execution or configuration of one of the subsequent safety functions:

- “Safe end position feedback” safety function
- Applies also for combination with of Safe ESD in direction OPEN/CLOSE.

Table 12: Proof test checklist

Configuration **Fail safe position OPEN and CLOSED (safety position OPEN and CLOSED)**	✎
1. Actuator in mid-position or at sufficient distance from the end positions?	□ ✓
↪ check FQM end position switch: • **End position OPEN not reached** signal (output signal inactive), i.e.: LSO 19-20=NC (NC contact) output = **closed** LSO 19-21=NO (NO contact) output = **open** • **End position CLOSED not reached** signal (output signal inactive), i.e.: LSC 22-23=NC (NC contact) output = **closed** LSC 22-24=NO (NO contact) output = **open** ↪ **No** fail safe fault signal may be present (“FS ready” signal).	□ Yes □ No
2. Operation command in direction CLOSE executed?	□ ✓
↪ Check actuator reaction: Operation was triggered?	□ ✓
3. Wait until FQM end position switch tripping. ↪ Check actuator reaction: Operation stopped when reaching end position switch CLOSED? • **End position OPEN not reached** signal (output signal inactive), i.e.: LSO 19-20=NC (NC contact) output = **closed** LSO 19-21=NO (NO contact) output = **open** • **End position CLOSED reached** signal (output signal active), i.e.: LSC 22-23=NC (NC contact) output = **open** LSC 22-24=NO (NO contact) output = **closed** ↪ **No** fail safe fault signal may be present (“FS ready” signal).	□ Yes □ No
4. Operation command in direction OPEN executed?	□ ✓
↪ Check actuator reaction: Operation was triggered? Start of operating time measurement.	□ ✓
5. Wait until FQM end position switch tripping. ↪ Check actuator reaction: Operation stopped when reaching end position switch OPEN? Operating time measurement complete. • **End position OPEN reached** signal (output signal active), i.e.: LSO 19-20=NC (NC contact) output = **open** LSO 19-21=NO (NO contact) output = **closed** • **End position CLOSED not reached** signal (output signal inactive), i.e.: LSC 22-23=NC (NC contact) output = **closed** LSC 22-24=NO (NO contact) output = **open** ↪ **No** fail safe fault signal may be present (“FS ready” signal).	□ Yes □ No
Operating time for operation from end position CLOSED in direction OPEN corresponds to the actuator configuration.	□ Yes □ No
6. Operate FQM via actuator into intermediate position. Actuator in mid-position or at sufficient distance from the end positions?	□ ✓

Configuration **Fail safe position OPEN and CLOSED (safety position OPEN and CLOSED)**	✎
↪ check FQM end position switch: • **End position OPEN not reached** signal (output signal inactive), i.e.: LS 19-20=NC (NC contact) output = **closed** LSO 19-21=NO (NO contact) output = **open** • **End position CLOSED not reached** signal (output signal inactive), i.e.: LSC 22-23=NC (NC contact) output = **closed** LSC 22-24=NO (NO contact) output = **open** ↪ **No** fail safe fault signal may be present (“FS ready” signal).	□ Yes □ 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.

11. 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	Safety Function	Controls type/wiring diagram
FQM 05.1 – FQM 12.1 or FQMEx 05.1 – FQMEx 12.1 in version SIL V1.0.00	Fail Safe OPEN/CLOSE (ESD) with PVST	FQM series in version SIL V1.0.00 with end position switches directly wired to the customer connection and TPA 34xxAB32xxxxxx or TPA 36xxAB32xxxxxx or TPA 34xxCB32xxxxxx or TPA 36xxCB32xxxxxx or TPA 48xxAB32xxxxxx or TPA 51xxAB32xxxxxx or TPA 48xxCB32xxxxxx or TPA 51xxCB32xxxxxx (x = variable)

The above mentioned version achieves the following Hardware Safety Integrity:

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

For further details, please refer to supplement overleaf.

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

Date

---
i.A. Jörg Isenberg
Product Management

Date

Sample - not valid for SIL/PL assessment

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	2019-07-24

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)	Fail Safe OPEN/CLOSE (ESD) with PVST		
Device type according to IEC 61508-2	☒ Type A	☐ Type B	
Operating mode	☒ Low Demand Mode	☐ High Demand or Continuous Mode	
Type of evaluation	☒	Evaluation by FMEDA according to IEC 61508-2	
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG	AUMA 14/07-095 R013	

Hardware Integrity				
Hardware integrity for "Fail Safe OPEN/CLOSE" (ESD) with PVST	Single channel use with PVST FQM 05.1 – FQM 12.1 (HFT = 0)	☐ SIL1 capable	☒ SIL2 capable	☐ SIL3 capable

Safety function	Fail Safe OPEN/CLOSE (ESD) with PVST
λ_{SAFE} *1)	273 FIT
λ_{DD} *1)	672 FIT
λ_{DU} *1)	513 FIT
MTBF - Mean Time Between Failures	51 years
SFF - Safe Failure Fraction	64 %
PFD_{avg} *2) with T[Proof] = 1 year	3,83 E-03

Restrictions

- Imperatively comply with any information given in the safety manual.
- The safety figures for the "Fail Safe OPEN/CLOSE" (ESD) function are only valid if the end position switches **directly** wired to the customer connection are used for end position evaluation.
- Frequent diagnostic via Partial Valve Stroke Test (PVST) out of end position controlled by the Safety PLC is necessary. The frequency has to be defined by the end user in accordance with the applicable standards, the restrictions given in the safety manual and the defined Proof Test interval.
- For the PVST only evaluation of the switches directly connected from the FQM to the customer connector is permissible.
- Evaluation of the collective fault signal output contact of the FQM (FS ready/failure signal) is necessary.
- The failure rates are valid for the useful life of the individual components of the "Fail Safe OPEN/CLOSE" (ESD) with PVST function of the Fail Safe Unit.
- The SIL / PL has to be evaluated for the complete (sub-)system. The numbers listed are for reference only.

Sample - Not valid for SIS/SIF assessment

*1) FIT = Failure In Time, Number of failures per 10^9 h
*2) PFD_{avg} = Probability of a failure on demand (average)

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	Safety Function	Controls type/wiring diagram
FQM 05.1 – FQM 12.1 or FQMEx 05.1 – FQMEx 12.1 in version SIL V1.0.00	Safe End Position Feedback with PVST	FQM series in version SIL V1.0.00 with end position switches directly wired to the customer connection and TPA 34xxxB32xxxxxx or TPA 36xxxB32xxxxxx or TPA 48xxxB32xxxxxx or TPA 51xxxB32xxxxxx (x = variable)

The above mentioned version achieves the following Hardware Safety Integrity:

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

For further details, please refer to supplement overleaf.

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

---
i.A. Jörg Isenberg
Product Management

Date

Date

Sample - not valid for SIL/PL assessment

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	2019-07-24

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 with PVST	
Device type according to IEC 61508-2	☒ Type A	☐ Type B
Operating mode	☒ Low Demand Mode	☐ High Demand or Continuous Mode
Type of evaluation	☒	Evaluation by FMEDA according to IEC 61508-2
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG	AUMA 14/07-095 R013

Hardware Integrity				
Hardware integrity for Save End Position Feedback with PVST	Single channel use with PVST FQM 05.1 – FQM 12.1 (HFT = 0)	☐ SIL1 capable	☒ SIL2 capable	☐ SIL3 capable

Safety function	Safe End Position Feedback with PVST
λ_{SAFE} *1)	0 FIT
λ_{DD} *1)	62 FIT
λ_{DU} *1)	39 FIT
MTBF - Mean Time Between Failures	97 years
SFF - Safe Failure Fraction	61 %
PFD_{avg} *2) with T[Proof] = 1 year	3,0 E-04

According to ISO 13849-1 the following Safety Metrics are achieved*3):

Safety function	Safe End Position Feedback with PVST
$MTTF_D$	1130 years (high)
DC	61 % (low)
Calculated Performance Level	3,89 E-08 1/h
Achieved Performance Level (CAT 1) *3)	PL = „c“ capable

Restrictions

- Imperatively comply with any information given in the safety manual.
- The safety figures for the Safe End Position Feedback with PVST are only valid if the end position switches **directly** wired to the customer connection are used for end position evaluation.
- Frequent diagnostic via Partial Valve Stroke Test (PVST) out of end position controlled by the Safety PLC is necessary. The frequency has to be defined by the end user in accordance with the applicable standards, the restrictions given in the safety manual and the defined Proof Test interval.
  For the PVST only evaluation of the switches directly connected from the FQM to the customer connector is permissible.
- Evaluation of the collective fault signal output contact of the FQM (FS ready/failure signal) is necessary.
- The failure rates are valid for the useful life of the individual components of the Safe End Position Feedback with PVST of the Fail Safe Unit.
- The SIL / PL has to be evaluated for the complete (sub-)system. The numbers listed are for reference only.

Sample, not valid for SIS/SIF assessment

*1) FIT = Failure In Time, Number of failures per10^9 h
*2) PFD_{avg} = Probability of a failure on demand (average)
*3) 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

A
Actuator definition 8
Actuator monitoring internal 22
Ambient conditions 10
Architecture 8

C
Certificate 36
Checklists 32, 32
Commissioning 18
Commissioning checklist 32
Configuration 8

D
DC 4
Declaration of Conformity 36
Decommissioning 18
Device types 6
Diagnostic coverage (DC) 4
Digital outputs 21
Disposal 19

E
Examples of applications 13

F
Fieldbus (signals) 21
Figures, safety-related 28

H
HFT 4

I
Indications 20
Installation 16
Interval for proof test 4

L
Lambda values 4, 28
Lifetime 18
Low demand mode 28

M
Maintenance 27
Mean Time Between Failures (MTBF) 4
MRT (Mean Repair Time) 5
MTBF 4
MTTR (Mean Time To Restoration) 5

O
Operation 18

P
Partial Valve Stroke Test (PVST) 23
PFD 4
PFD for actuator 28
Probability of failure 4
Proof test 5, 24, 24
Proof test checklists 32

R
Range of application 6
Recycling 19

S
Safe failure fraction (SFF) 4, 28
Safety function 4
Safety functions 11
Safety instrumented function (SIF) 4
Safety instrumented system 11
Safety instrumented system (SIS) 4
Safety-related system 4
Service conditions 10
Setting 8
SFF 4
Signals 21
SIL 4
Standards 6
Status signals 21

T
Tests 22
T proof 4