auma®
Solutions for a world in motion

FUNCTIONAL SAFETY – SIL

Electric actuators for safety-related systems up to SIL 3

AUMA, the globally leading manufacturer of electric actuators for the automation of industrial valves.
AUMA actuators work reliably all around the globe for managing the flow of liquids or gases, powders or granulates. Their use sees them placed in sectors such as in water supply and waste water sector, in power plants, pipelines, refineries, and industrial plants of any kind.

YOUR EXPERT PARTNER FOR ELECTRIC ACTUATORS

Since 1964, the founding year of the company, we have focused on development, the manufacture, sales and service of electric actuators. Our products have become renowned global brands, the reliability, precision and long life of which are truly valued by our customers..

As a medium-sized family owned company, AUMA has grown into a successful global player, giving work to more than 2,600 people worldwide. Our cosmopolitan sales and service network offers you more competent local support in more than 70 countries.

AUMA AUTOMATES VALVES

FUNCTIONAL SAFETY

AUMA offers a broad portfolio of electric actuators qualified for safety-related systems up to SIL 3. Our products contribute to the safe operation of technical systems all around the globe. Internationally renowned test institutes have determined both safety figures and SIL capability for our products.

Besides a basic introduction to the functional safety topic, this brochure will provide you with detailed information on the SIL capability of AUMA products.

Further documents like certificates, inspection certificates, safety figures, or our comprehensive manuals "Functional safety – SIL" are available on request or for download from our website www.auma.com.

CONTENTS

2021.09.15

Safety issues in modern industrial plants gain increasing importance, in particular for plants with high hazard potential within the oil & gas sector, the chemical industry or in power plants.

Today, a clear trend to implement sophisticated safety systems intervening in case of failure can be noted, in particular to monitor processes leading to potential hazards for both persons and the environment. Such systems are used to shut down a plant in case of emergency, for example, to cut off the supply of hazardous substances, provide cooling or open overpressure valves. To reduce hazards emanating from a plant, these systems must perform their safety functions in case of emergency and must not fail.

However, how can plant operators and device manufacturers guarantee that the systems implemented work "safely" and meet the necessary requirements? How can failure risks be assessed?

The standards relating to functional safety, IEC 61508 and IEC 61511, supply the answer. They describe methods for assessing the failure risks of modern and often software controlled systems and for determining the actions for risk reduction.

WHAT DOES FUNCTIONAL SAFETY MEAN?

According to IEC 61508, functional safety relates to systems used to carry out safety functions whose failure would have a considerable impact on the safety of both persons and the environment.

In order to achieve functional safety, a safety function in the event of a failure must ensure that a technical system is led to or maintained in a safe state.

In the process industry, functional safety does not deal with basic dangers of a product or a system such as rotating parts for example, but with hazards which might be caused by a system due to the failure of a safety function.

A major objective of functional safety is to reduce the probability of dangerous failures and consequently to minimise the risk for people and environment to a tolerable level.

Altogether, functional safety – in combination with further actions such as e.g. fire protection, electrical safety or explosion protection – significantly contributes to the overall safety of a system.

RISK REDUCTION BY FUNCTIONAL SAFETY

WHAT IS SIL?

SIL is a term closely linked to functional safety. SIL is the abbreviation for Safety Integrity Level and a measuring unit for risk reduction with safety functions.

The higher the potential hazards from processes or systems, the more demanding the requirements on reliability of safety functions.

IEC 61508 defines four different safety integrity levels, SIL 1 through SIL 4.

SIL 4 has the highest level of safety integrity and SIL 1 the lowest. For each level, specific target failure probabilities are defined which may not be exceeded by the safety function.

Risk assessment is used to determine the required SIL.

AUMA'S ROLE WITHIN THIS CONTEXT

AUMA products are implemented as components into systems which perform safety functions. For this reason and in collaboration with independent test authorities such as TÜV and exida, we examined of which SIL our actuators, actuator controls and gearboxes are capable.

On the basis of the determined safety specifications and figures, plant designers can select the suitable devices for the requested safety integrity demands.

STANDARDS ON FUNCTIONAL SAFETY

THE ORIGINS

Industrial accidents with disastrous consequences such as the Seveso dioxin disaster in 1976, or the Indian Bhopal gas tragedy in 1984, put the worldwide standardisation processes with regard to the safety of technical systems into gear.

At EU level, first the Seveso I, Seveso II and later the so-called Seveso-III-directive 2012/18/EU on the control of major accident hazards involving dangerous substances were issued. These directives aim at the protection of persons, environment and material assets as the primary objective. Furthermore, definite instructions were given for systems with high hazard potential.

National standards on functional safety were first created within this context. The first international standard was issued in 1998 with the IEC 61508.

IEC 61508

IEC 61508 is one of the most important international standards applicable to functional safety for electrical, electronic or programmable electronic components (E/E/PE) executing safety functions. The requirements by the standards are transferred to other e.g. mechanical components where appropriate. A new edition of this standard has been available since 2010.

As a generic basic standard, it is addressed to consultants, operators and device manufacturers and is supplemented by further application specific standards such as IEC 61511 for the process industry.

Concept of risk reduction

The objective of safety-related system implementation is to reduce risks generated by processes and plants. Generally, the standard assumes that it is impossible to exclude all potential risks. However, it offers methods for risk analysis, risk reduction and evaluation of the residual risk.

Requirements for safety-related systems

The standard describes the requirements for safety-related systems or the safety functions and defines the Safety Integrity Level (SIL). Appropriate SIL requirements are consequently deduced for the system components used.

Considering the lifecycle

To minimise the risk of failure, the complete safety lifecycle of components is taken into account, from the specification through implementation until decommissioning.

IEC 61511

This standard includes the application-specific implementation of IEC 61508 for the process industry, in particular the chemical and petrochemical industry. It defines the requirements for safety-related systems used in the process industry for risk reduction. It also uses safety integrity levels SIL 1 to SIL 4 as a measure for the required risk reduction.

This standard mainly addresses consultants and plant operators.

IEC 62061

Dealing with the safety of machinery, the requirements on functional safety derive from IEC 61508. IEC 62061 uses safety integrity levels SIL 1 to SIL 3.

This standard mainly addresses consultants and plant operators.

EN ISO 13849

EN ISO 13849 on the safety of machinery is about the safety requirements on design and integration of safety-related parts of control systems. It provides a classification according to performance levels (PL). PL is a measure for reducing the risk arising from the machine. Performance levels are classified from “a” to “e” where "e" represents the highest PL.

Functional safety in compliance with EN ISO 13849 is often a requirement within hydropower and civil engineering constructions for water applications.

SAFETY-RELATED ASSESSMENT

First of all, the risks emanating from a system or process will have to be analysed to achieve functional safety. The standards IEC 61508 and 61511 supply a recognised method for risk evaluation.

Differentiated safety-related assessments are used to identify the processes leading to actual hazardous events. Consequently, focus can be placed on taking risk reducing actions wherever truly needed.

Identification of hazardous processes

Firstly, processes in plants that could lead to potential hazards for persons and the environment must be examined if they become out of control.

Definition of SIL requirements

Each of the potentially hazardous processes is examined to determine the potential hazard and consequences due to a failure.

A risk graph as shown below can be used to facilitate risk assessment. Depending on the extent and the probability of the risk recurring, it can be established as to whether the process must be protected by a safety function and which safety integrity level (SIL) this safety function must achieve.

Selection of appropriate components

Depending on the required SIL, components for implementing the safety function will be selected.

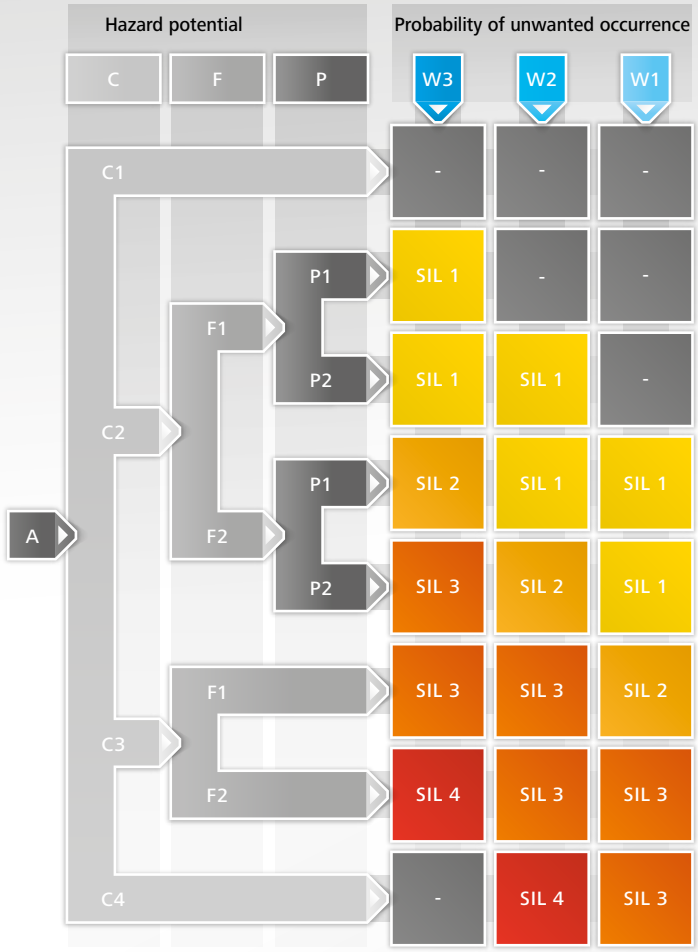
To facilitate this procedure, device manufacturers like AUMA have their devices tested for classification in compliance with the available safety integrity levels.

Avoiding systematic faults

To avoid faults which could arise amongst others during planning, implementation, commissioning and operation – for example incorrect sizing or wiring – special fault-avoiding procedures must be heeded and suitable action taken. These actions depend on the SIL level required.

Verification of SIL requirements

On the basis of safety figures of implemented devices as well as the recorded fault-avoiding measures, verification is made for each safety function whether the demanded SIL is achieved. If this is not the case, then additional actions will have to be taken.



Example of a risk graph for a safety-related assessment in compliance with IEC 61508/61511

A Starting point for evaluating risk reduction

C Consequences
C1 Minor injury of a person or minor hazardous environmental impacts
C2 Serious permanent injuries or 1 death
C3 Death of several persons
C4 Multiple deaths

F Avoidance of hazard
F1 Possible under certain circumstances
F2 Almost impossible

P Exposure time of a person at the hazardous location
P1 Rare to frequent
P2 Frequent to permanent

W Probability of unwanted occurrence
W3 Relatively high
W2 Low
W1 Very low

SIL Requested safety integrity level
SIL 1 to SIL 4 Lowest safety requirement to Highest safety requirement

SAFETY FUNCTION AND SAFETY-INSTRUMENTED SYSTEM

WHAT IS A SAFETY FUNCTION?

Safety instrumented functions (SIF) are protective actions activated in case of failure to avoid damage of persons, environment and material assets. Functional safety is achieved if safety functions work reliably in case of failure.

A typical safety instrumented function is the automatic safety shutdown of a process.

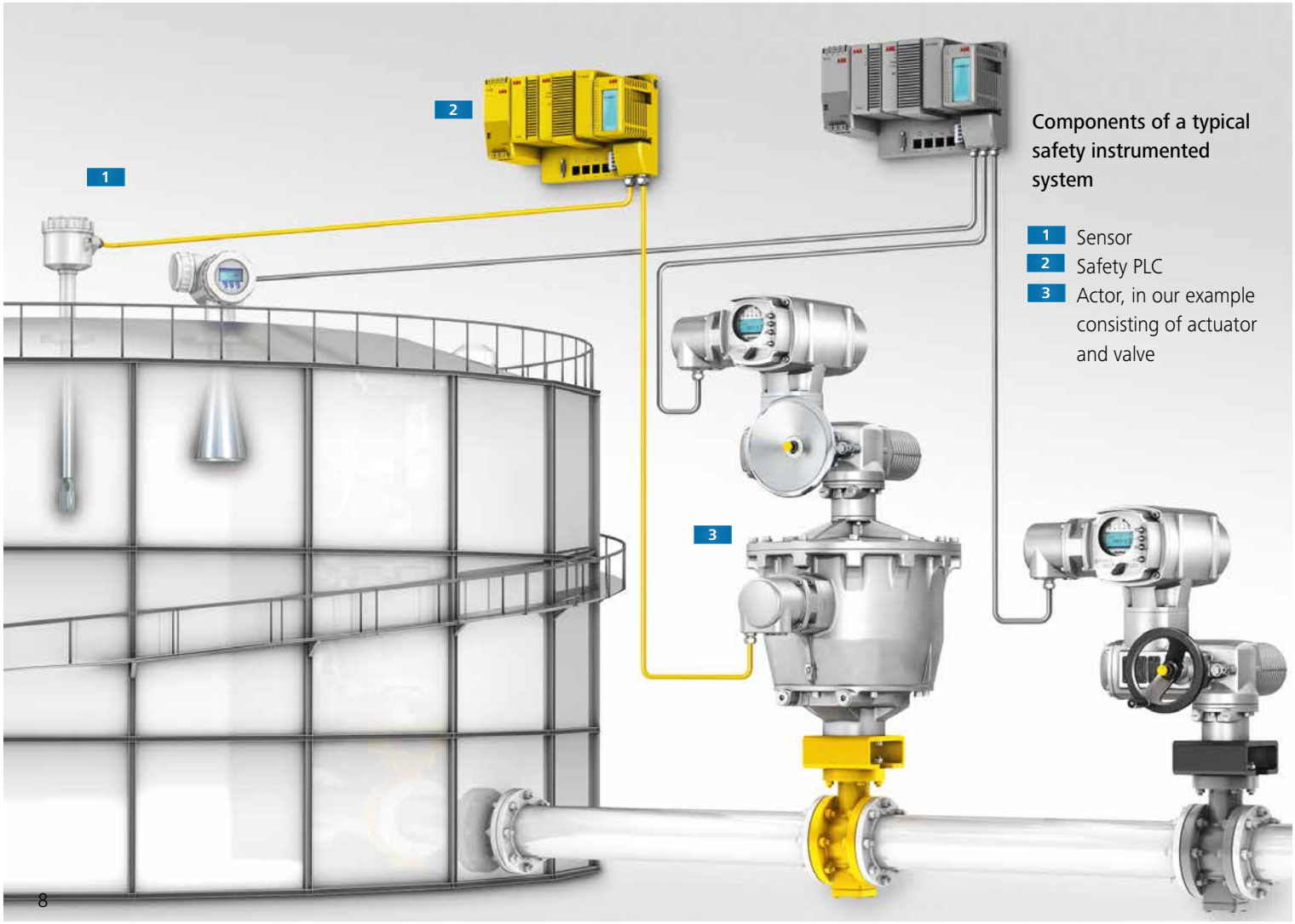
In the valve sector, the following safety functions are of crucial importance:

> Safe OPENING/Safe CLOSING (Emergency Shutdown, ESD)
> Safe Torque Off, STO often called Safe STOP or Stayput
> Safe end position feedback

WHAT IS A SAFETY INSTRUMENTED SYSTEM?

A safety function is implemented by the components of the Safety Instrumented System (SIS). Such a system generally consists of the following components: sensor, host safety PLC and actor. In the valve sector, the actor combines actuator and valve.

When assessing whether a safety instrumented function achieves the required SIL, systematic capability as well as the safety figures of all individual components of the safety instrumented system are considered.



Components of a typical safety instrumented system

1 Sensor
2 Safety PLC
3 Actor, in our example consisting of actuator and valve

CRITERIA FOR RISK REDUCTION

When analysing the potential hazards of a process, the SIL to be met is determined for each safety instrumented function. International standards IEC 61508 and IEC 61511 define the three main criteria the safety instrumented function or the SIS has to comply with to meet the required risk reduction:

> Systematic capability
> Permitted average probability of failure on demand
> Architectural constraints

The criteria are explained in the following.

SYSTEMATIC CAPABILITY

The systematic capability (SC) is to ensure that a component is generally suitable for an SIS with a specific SIL requirement. IEC 61508 defines different methods:

> The first method (Route 1_S in the standard) requires that certain procedures are heeded during development, manufacture and maintenance etc. Thus, systematic faults, like, for example, incorrect sizing or design faults in components are avoided. This method is predominantly applied to devices to be newly developed.

> The second method (route 2_S) is based on the evaluation of field data to obtain evidence that the components are proven in use and to prove the required reliability. This method is in particular applied to device types existing for quite some time and for which a multitude of field data is available.

When selecting components for an SIS, it has to be ensured that all components have the appropriate systematic capability for the required SIL of the overall system.

AVERAGE PROBABILITY OF FAILURE ON DEMAND (PFD AND PFH)

The PFD_{avg} value (average Probability of dangerous Failure on Demand) describes the mean probability of the unavailability to perform the safety function. According to IEC 61508, an allowable range for the probability of failure is defined for each of the four safety integrity levels. SIL 1 represents the lowest level, SIL 4 being the highest level. The higher the safety level, the lower the probability for the failure of a safety function on demand.

The extent of loss is not the only decisive factor in case of failure: The frequency of the expected failure and the therefore respective demand for the appropriate safety function are also important factors.
IEC 61508 distinguishes between low demand, high demand and continuous mode.

Low demand mode

In low demand mode of operation, the safety function is requested maximum once a year. Typically this applies to safety functions for the process industry using actuators.

Only the safety function is taken into account here. An actuator used to perform a safety function as well as "conventional" opening and closing actions may of course open or close a valve more often during normal service. A system failure requiring safe valve closing must however not be expected more than once a year.

Allowed PFD values for low demand mode

Safety integrity level	Allowed PFD_{avg} value (low demand)	Theoretically allowed failures for a safety function on demand
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	Allows one dangerous failure in 10 years
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	Allows one dangerous failure in 100 years
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	Allows one dangerous failure in 1,000 years
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	Allows one dangerous failure in 10,000 years

High demand mode and continuous mode

In high demand mode, the safety function is requested more than once a year. In continuous mode, the safety function is continuously working.

The basic safety calculation parameter for these two operation modes is the probability of failure per hour and indicated as PFH value.

In a first step, PFD and PFH values are calculated for each component of a safety instrumented system. A safety integrity level describes the characteristics of a complete safety function and not of the mere individual component. For this reason, the total value must then be calculated for the safety function on the basis of the PFD or PFH values of the individual components.

ARCHITECTURAL CONSTRAINTS

The architecture of an SIS should be as robust and as fault-tolerant as possible. IEC 61508-2:2010 defines two permissible methods to determine the maximum achievable SIL on the grounds of architectural constraints (AC):

> Route 1_H in IEC 61508 is based on a classification according to a minimum value for the safe failure fraction (SFF) combined with sufficient redundancy in the system architecture on the basis of the hardware fault tolerance (HFT).

> The second method, route 2_H, allows simplified classification on the basis of HFT only. However, further requirements must be met, for example, comprehensive field experience is required for the components used.

Architectural requirements must be met on element level. For the final element, consisting of actuator and valve, it has proved reasonable to consider this combination as single element.

Safe Failure Fraction (SFF)

The SFF value (Safe Failure Fraction) describes the fraction in percentage of safe and detected dangerous failures related to the total failure rate. Failures are considered safe if their occurrence either bring the system into a safe state or maintain the system in the safe state.

The higher the value, the lower the probability of a dangerous system failure.

Hardware fault tolerance (HFT)

HFT (Hardware Fault Tolerance) is the ability of a functional element to further perform a required safety function in spite of the presence of faults or deviations.

A hardware fault tolerance of N means that
N + 1 faults could cause a loss of the safety function. For example with a hardware fault tolerance of 0, a single fault can lead to the failure of the safety function.

In general, HFT can be increased by creating a redundant system architecture (please also refer to page 13).

Device type

IEC 61508 distinguishes between simple and complex devices.

> Simple type A elements
  Type A devices are "simple" units for which the failure behaviour of all components is completely known. They comprise e.g. relays, resistors and transistors, however no complex electronic components such as e.g. microcontrollers.
> Complex type B devices
  Type B devices are "complex" units containing electronic components such as microcontrollers, microprocessors and ASICs. For these components and in particular for software controlled functions, it is highly difficult to completely anticipate all potential faults.

The more complex the device, the higher the requirements

The following tables show that higher requirements apply to type B devices than to type A devices.

SFF and HFT for type A devices (route 1_H)

SFF (Safe Failure Fraction)	HFT (Hardware Fault Tolerance)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % to < 90 %	SIL 2	SIL 3	SIL 4
90 % to < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

SFF and HFT for type B devices (route 1_H)

SFF (Safe Failure Fraction)	HFT (Hardware Fault Tolerance)		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 % to < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

The following parameters are required for the assessment of the different risk reduction criteria:

FAILURE RATES

The analysis of possible failure sources is of significant importance for the safety of a system. Assessment of the failure rate lambda is the basic for the calculation for further safety figures. When considering failure rates (λ), a distinction is made as to which failures are classified as dangerous and which are safe. Consequently without impact on the correct execution of a safety function. Furthermore, the diagnostic coverage of a failure is examined.

Number of safe failures in time (Lambda Safe λ_{safe})

A failure is considered safe if the safety function is initiated or executed due to this failure. The unit Failure In Time (FIT) indicates the number of failures occurring in 10^9 hours: 1 FIT means one failure per 10^9 hours or one failure per 114,000 years.

Number of detected dangerous failures in time (Lambda Dangerous Detected, λ_{DD})

A component failure is classified as dangerous if it might prevent execution of a safety function. The number of detected dangerous failures per 10^9 hours on the basis of diagnostic tests is indicated.

Number of undetected dangerous failures in time (Lambda Dangerous Undetected, λ_{DU})

The number of undetected dangerous failures per 10^9 hours is indicated.

Diagnostic Coverage of Dangerous Failures, DC_D

Fraction of dangerous failures detected by diagnostic tests (λ_{DD}) associated with the total rate of detected dangerous failures in percent.

INTERVAL FOR PROOF TESTS (T_{PROOF})

The safety function must be checked at periodic intervals by means of a proof test. The intervals have to be defined by the plant operator to ensure proper function. This is necessary to reveal and eliminate systematic as well as random failures which have not yet been detected.

The PFD value can be improved by reducing the time between two proof tests.

DETERMINING THE SIL CAPABILITY

It is always the SIL capability of the entire safety instrumented system that is crucial to the safety of a safety function.

SIL CAPABILITY OF A SAFETY FUNCTION

When assessing and classifying a safety function in compliance with IEC 61508, all three major criteria should be considered. Systematic capability, probability of failure on demand and architectural constraints, are decisive. The respective values for the individual components of the SIS have to be considered.

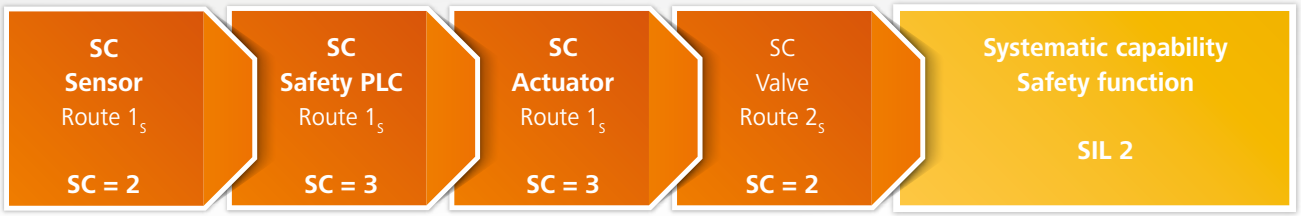
It is imperative to observe that the achievable SIL is always the lowest SIL achieved by the three individual assessments:

Assessment of a safety function

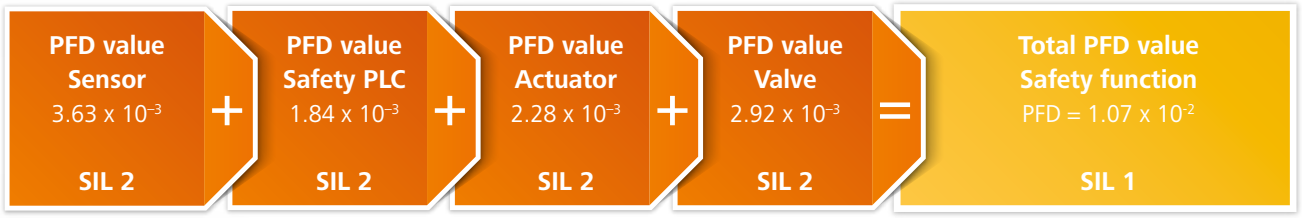
SIF classification related to	maximum achievable SIL
Systematic capability	SIL 2 (SC = 2)
Probability of failure on demand	SIL 1
Architectural constraints	SIL 2
Overall assessment of the safety function	**SIL 1**

Example of determining the maximum achievable SIL of a safety function (for single-channel system architecture)

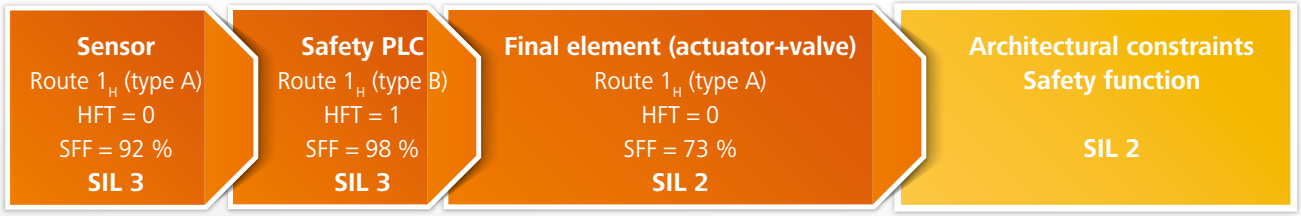
Assessment of systematic capability (SC) of a safety function



Calculation of the total PFD value of a safety function



Calculation of architectural constraints



IMPROVING THE SIL CAPABILITY

Should the assessment show that the selected hardware components do not achieve the requested SIL, then SIL capability can be improved by additional actions such as diagnosis and redundancy.

PARTIAL VALVE STROKE TEST (PVST)

The partial valve stroke test is performed to regularly verify device functionality. Actuator or valve travel a predetermined distance back and forth. Thus testing the operation of the actuator.

PVST is a recognised method to increase the availability of individual components of a safety function. By means of preventive diagnostics, some safety-relevant faults may be detected before they can prevent or impair the execution of a safety function; the probability of failure on demand decreases.

PROOF TEST

This test deals with comprehensive system verification. If the periodic interval between two proof tests is reduced for example from two years to one year, SIL capability may be improved and hidden failures can be detected faster.

REDUNDANCY

Redundant system architecture is used to increase the probability that the safety function is performed in case of emergency. Two or more devices of a safety-related system are subjected to redundant operation.

Depending on the safety requirement, different MooN ("M out of N") configurations may be feasible. For a 1oo2 ("one out of two") configuration, one out of two devices is sufficient to perform the required safety function. 2oo3 ("Two out of three") configuration implies that two out of three devices must function properly.

A redundant system architecture can increase hardware fault tolerance (HFT) and consequently SIL capability. In general, a redundant system structure is implemented for SIL 3 applications according to IEC 61511, e.g. 1oo2.

The actual system architecture depends, however, on the demanded safety function. On the basis of the overall safety function at system level, it must be generally verified whether a set-up with several actuators within the scheduled configuration actually results in HFT > 0.

Redundant system for Safe OPENING

Redundant system for Safe CLOSING

AUMA PRODUCTS WITH SIL CLASSIFICATION

For consultants and plant operators, it is of core importance to exclusively implement components meeting the respective safety requirements.

AUMA offers a comprehensive portfolio of products for various SIL requirements. We have determined the safety figures and consequently the SIL capability for selected AUMA actuators, actuator controls and gearboxes to optimally support our customers with product selection.

AUMA PRODUCTS IN SIL VERSION

The products listed below are suitable for highest safety requirements. They have been newly developed and were subjected to complete assessment in accordance with IEC 61508. (refer to page 26).

SA AND SQ ACTUATORS WITH AC .2 ACTUATOR CONTROLS IN SIL VERSION

AC .2 and ACExC .2 actuator controls in SIL version have an additional SIL module specially designed for the execution of the safety function. Actuators equipped with these actuator controls are classified as SIL 2. SIL 3 can be achieved with a redundant system architecture. Certification was performed by TÜV Nord [German certification body].

Safety functions:

> Safe OPENING/Safe CLOSING
> Safe STOP
> Safe end position feedback[1)]

For detailed information, refer to pages 18 to 21.

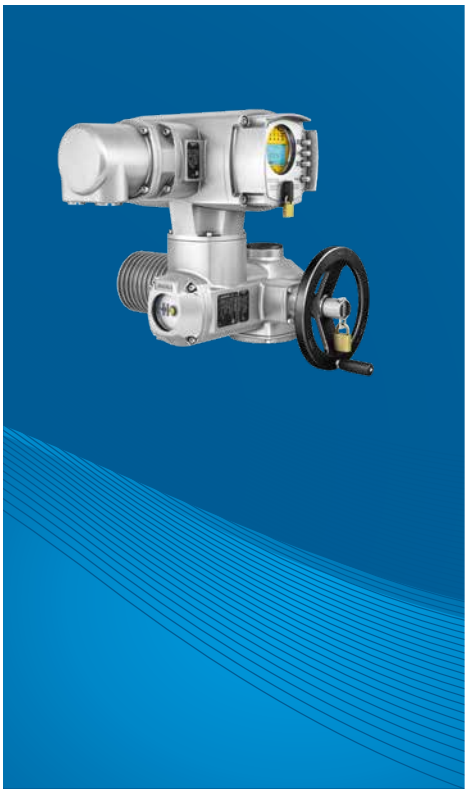
FQM FAIL SAFE UNIT IN SIL VERSION

With the FQM fail safe unit, AUMA offers innovative and safe actuation solutions for operation of valves in case of emergencies during power failures. The device is suitable for safety-related applications up to SIL 2. SIL 3 can be achieved with a redundant system architecture. Certification was performed by exida.

Safety functions:

> Safe OPENING/Safe CLOSING
> Safe end position feedback

For detailed information, refer to pages 22 et seqq.



1 For these products, safe end position feedback is not included in the certificate. A declaration of incorporation has been issued instead.

AUMA PRODUCTS IN SFC VERSION

With the actuators, actuator controls and gearboxes in SFC (Safety Figures Calculated) version, AUMA offers a wide product portfolio for medium and low safety requirements. In close cooperation with exida, AUMA has determined the safety figures for these products within the framework of a hardware assessment based on field experiences and/or generic data. A declaration of incorporation by the manufacturer is available for these products. They offer higher flexibility with regard to configuration options as well as investment cost.

SA AND SQ ACTUATORS WITHOUT INTEGRAL ACTUATOR CONTROLS IN SFC VERSION

SA and SQ actuators without actuator controls are up to SIL 2 capable for the safety functions considered.

Safety functions:

> Safe operation in direction OPEN/CLOSE
> Safe standstill
> Safe end position feedback

For these versions, control functions have to be supplied by the customer.

SA AND SQ ACTUATORS WITH AM .1 AND AC .2 ACTUATOR CONTROLS IN SFC VERSION

Actuators with AM .1 or AC .2 actuator controls are up to SIL 2 capable in the versions considered.

Safety functions:

> Safe end position feedback

GK AND GS .3 GEARBOXES IN SFC VERSION

Safety figures were also determined for AUMA GK and GS .3 gearboxes. The gearboxes considered are up to SIL 2 capable.

Safety functions:

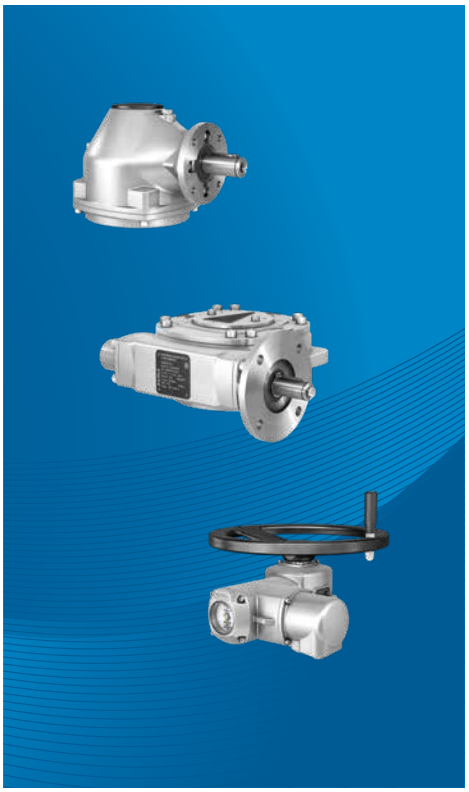
> Safe operation in direction OPEN/CLOSE

WSH LIMIT SWITCHING DEVICE IN SFC VERSION

WSH manual gearboxes with electromechanical control unit are SIL 1 capable.

Safety functions:

> Safe end position feedback



ALLOCATED SAFETY FUNCTIONS

The safety-related figures and thus the SIL capability depend on the safety function performed by the device in case of emergency, with the objective to achieve safe system state.

AUMA actuators are suitable for the following safety functions:

Safe OPENING/Safe CLOSING
(Emergency Shutdown, ESD)
Upon request of the safety function, the actuator travels in direction end position OPEN or end position CLOSED.

These safety functions can generally be combined with a Partial Valve Stroke Test (PVST) as additional diagnostic measure.

Safe Torque Off, STO
often called Safe STOP or Stayput
Upon request of the safety function, the actuator motor is disconnected from the mains. Undesired motor starts from standstill are prevented.

Safe operation in direction OPEN/CLOSE
This safety function is executed by actuators without actuator controls and by gearboxes. On demand, the actuator runs in the respective direction. The valve position is, however, not indicated here.

Safe end position feedback
For this safety function, the actuator is used as sensor within the SIS. The actuator issues a safe signal via the electromechanical control unit as soon as one of the end positions OPEN or CLOSED or the tripping torque are reached.

APPLICATION EXAMPLES OF SAFETY FUNCTIONS

Safe CLOSING
Example of an overfill protection for oil tank
In tank farms, the standard tank filling systems are often protected by additional safety systems designed to prevent overfilling. A safety PLC continuously monitors the filling level within the tank via specific sensors. Once a limit is exceeded, the safety PLC sends an emergency shutdown (ESD) signal to the actuator of the SIS and the valve will be closed.

Safe end position feedback and safe STOP
Example of a lock
Locks are a good example for presenting different safety functions:

For instance, it has to be ensured that the lock gates on one side are completely closed prior to opening the other side. This can be implemented using an actuator with safe end position feedback combined with a safe STOP function as locking function. The locking function ensures that a movement of the lock gate is only enabled if the "Safe STOP" signal is not applied.

If a ship is between the opened lock gates, the Safe STOP safety function can reliably stop the closing of the lock.

OVERVIEW OF AUMA PRODUCTS WITH SIL CLASSIFICATION

Upon request, AUMA will provide you with test reports for all SIL classified AUMA products.

Actuator / Gearbox	Actuator controls	Version	Safety function	Maximum possible safety requirement		
				for HFT[1]	according to IEC 61508	acc. to ISO 13849
FQM 05.1 SIL – FQM 12.1 SIL with SQ 05.2 – SQ 12.2 FQMEx 05.1 SIL – FQMEx 12.1 SIL with SQEx 05.2 – SQEx 12.2	AC 01.2 (standard) ACExC 01.2 (standard)	SIL	Safe OPENING/CLOSING (ESD) (without external power supply)	HFT = 0 HFT = 1	SIL 2 (with PVST) SIL 3 (with PVST)	
			Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
SA 07.2 – SA 16.2 SAR 07.2 – SAR 16.2 SAEx 07.2 – SAEx 16.2 SAREx 07.2 – SAREx 16.2	AC 01.2 SIL ACExC 01.2 SIL	SIL	Safe OPENING/CLOSING (ESD)	HFT = 0 HFT = 1	SIL 2 (with PVST) SIL 3 (with PVST)	
			Safe STOP	HFT = 0 HFT = 1	SIL 2 SIL 3	
			Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)[3]	PL c (with PVST)[3] PL d/e (with PVST)[2] [3]
	Without actuator controls	SFC	Safe operation in direction OPEN/CLOSE	HFT = 0	SIL 2 (with PVST)	
			Safe standstill	HFT = 0	SIL 2	
			Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
	AM 01.1/02.1 AMExC 01.1 AMExB 01.1	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
	AC 01.2 (standard) ACExC 01.2 (standard)	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
SQ 05.2 – SQ 14.2 SQR 05.2 – SQR 14.2 SQEx 05.2 – SQEx 14.2 SQREx 05.2 – SQREx 14.2	AC 01.2 SIL ACExC 01.2 SIL	SIL	Safe OPENING/CLOSING (ESD)	HFT = 0 HFT = 1	SIL 2 (with PVST) SIL 3 (with PVST)	
			Safe STOP	HFT = 0 HFT = 1	SIL 2 SIL 3	
			Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (SIL 1 for SQ 14.2)(with PVST)[3]	PL c (with PVST)[3] PL d/e (with PVST)[2] [3]
	Without actuator controls	SFC	Safe operation in direction OPEN/CLOSE	HFT = 0	SIL 2 (with PVST)	
			Safe standstill	HFT = 0	SIL 2	
			Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (SIL 1 for SQ 14.2) (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
	AM 01.1/02.1 AMExC 01.1	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (SIL 1 for SQ 14.2) (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
	AC 01.2 (standard) ACExC 01.2 (standard)	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (SIL 1 for SQ 14.2) (with PVST)	PL c (with PVST) PL d/e (with PVST)[2]
SA 25.1 – SA 40.1 SAR 25.1 – SAR 30.1 SAExC 25.1 – SAExC 40.1 SARExC 25.1 – SARExC 30.1	Without actuator controls	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d (with PVST)[2]
	AM 01.1/02.1 AMExC 01.1 AMExB 01.1	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d (with PVST)[2]
	AC 01.2 (standard) ACExC 01.2 (standard)	SFC	Safe end position feedback	HFT = 0 HFT = 1	SIL 2 (with PVST)	PL c (with PVST) PL d (with PVST)[2]
GK 10.2 – GK 40.2	Not relevant	SFC	Safe operation in direction OPEN/CLOSE	HFT = 0	SIL 2 (with PVST)	
GS 50.3 – GS 250.3	Not relevant	SFC	Safe operation in direction OPEN/CLOSE	HFT = 0	SIL 2 (with PVST)	
WSH 10.2 – WSH 16.2 WSHEx 10.2 – WSHEx 16.2	Not relevant	SFC	Safe end position feedback	HFT = 0	SIL 1	PL c

1 Hardware fault tolerance
HFT = 0 is achieved for example by a single-channel system "1oo1" ("one out of one").
HFT = 1 is achieved for example by a redundant system "1oo2" ("one out of two"). However, it must be generally verified at system level, whether HFT > 0 is actually achieved by the use of several actuators.

2 Leading to further requirements on system level, in particular redundancy and diagnostic measures
(which PL is achieved must be assessed on system level)

3 Declaration of Incorporation in collaboration with exida; is not part of the certificate

AC. 2 ACTUATOR CONTROLS IN SIL VERSION

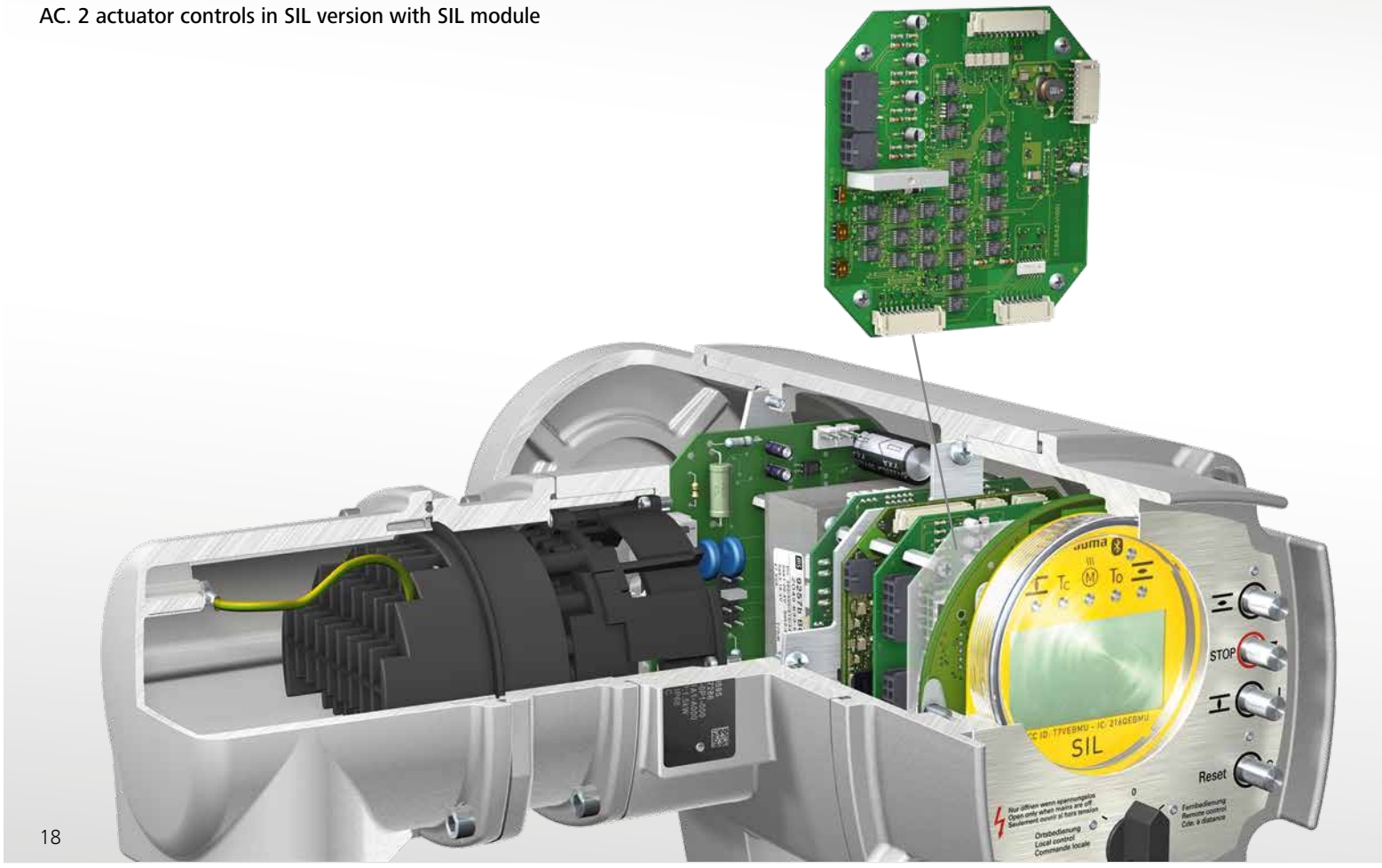
With the AC .2 actuator controls in SIL version, AUMA provides modern controls for safety-related systems up to SIL 3. Safety functions are exclusively executed via the safe SIL module. During standard operation, all AC .2 functions are available.

TÜV CERTIFICATE FOR SIL 2/SIL 3 APPLICATIONS

You will appreciate the variety of functions and setting options when familiarising with AC .2 actuator controls. Freely configurable parallel and fieldbus interfaces allow swift integration into sophisticated distributed control systems. AC .2 controls are ideally suited to complex control functions. Additional diagnostic functions like operating data logging and lifetime factor monitoring increase safety and availability of the actuator.

Thanks to the SIL module developed by AUMA, these functions can also be used for SIL 2 and SIL 3 applications. SA and SQ actuators equipped with AC .2 in SIL version are certified by TÜV Nord and approved for safety-related systems up to SIL 3 (SC = 3, SIL 3 in redundant version 1oo2/HFT = 1).

AC. 2 actuator controls in SIL version with SIL module



THE SIL MODULE

The SIL module consists in an additional electronic board, responsible for executing the safety functions. This board is used in AC .2 and ACExC .2 actuator controls in addition to the standard logic.

The SIL module integrates comparatively simple components such as transistors, resistors and capacitors for which the failure modes are completely known. Therefore, AC .2 in SIL version is classified as a type A device. Determined safety figures allow implementation in SIL 2 and even in SIL 3 (SC = 3) applications (provided the availability as redundant architecture – 1oo2).

PRIORITY OF THE SAFETY FUNCTION

If a safety function is requested in the event of an emergency while some functions are executed via the standard logic, the standard logic of AC .2 will be by-passed and the safety function be performed via the SIL module. The safety functions always overrule standard operation.

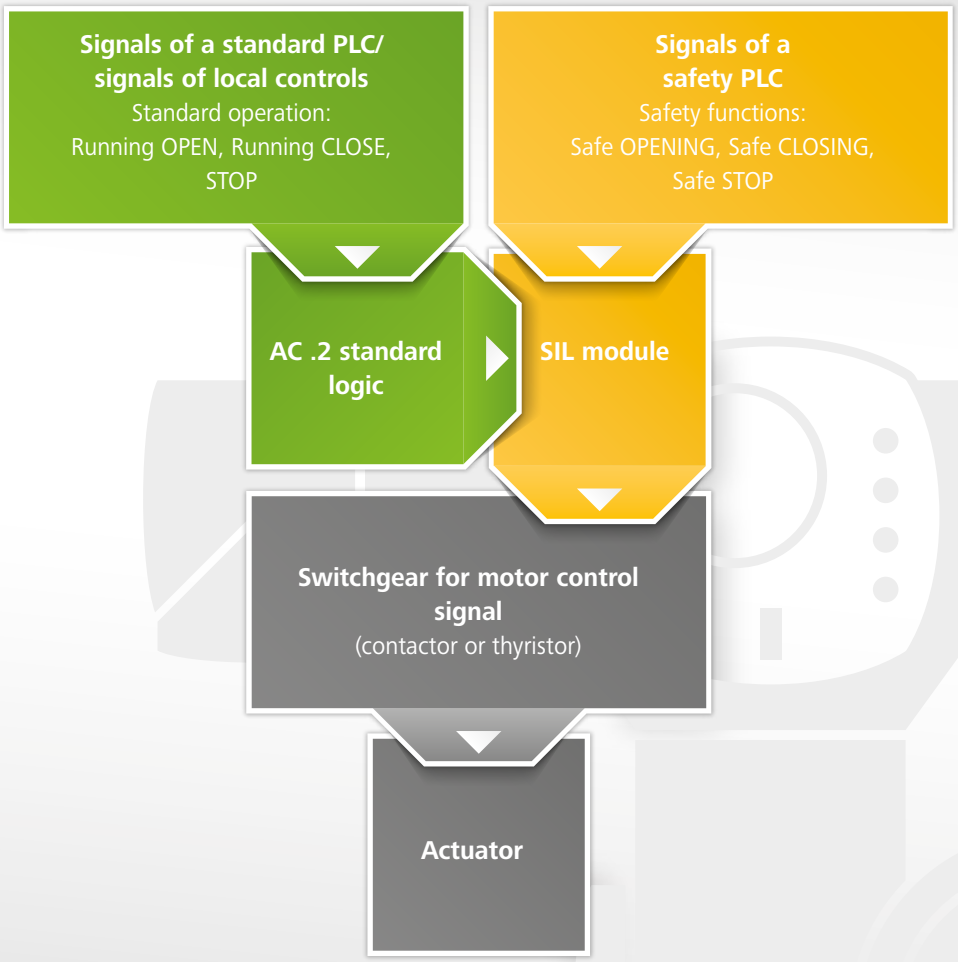
TYPICAL SYSTEM ARCHITECTURE

Actuators with AC .2 actuator controls in SIL version offer various options for system architecture:

Physically separated SIS
In most cases, an SIS is completely physically separated from standard process control. This means that an actuator with AC .2 in SIL version is exclusively designated for the execution of the safety function. A second, standard version actuator will operate the valve during normal operation.

Combination of SIS and normal operation
An actuator with AC .2 actuator controls in SIL version can generally be used for both execution of the safety function and process control during normal operation: AC .2 is controlled via two host controls (PLC), a standard PLC and a safety PLC classified as SIL approved PLC.

However, additional requirements to be observed for both design and integration have been defined in IEC 61511 for this specific application.



Priority of the safety function
Even in standard operation, the signals within the AC .2 in SIL version are always sent via the SIL module. This includes operation commands or any other signal from the standard PLC or the local controls. If a safety function is requested via a safety PLC, the SIL module ensures immediate and prioritised execution.

AC. 2 ACTUATOR CONTROLS IN SIL VERSION

CONFIGURATION OPTIONS

AC .2 in SIL version are characterised by many configuration options. All customised settings are preset in the factory: Which safety function must be performed? At which point to interrupt travel? These settings are made via the DIP switches of the SIL module.

Safety functions
The following safety functions can be performed using the AC .2 in SIL version:

> Safe OPENING/CLOSING
(Safe ESD, Emergency Shut Down)
Actuator runs to configured end position OPEN or CLOSED. The redundant signal input procures additional safety.

> Safe STOP
For this safety function, an operation command issued by the standard PLC in directions OPEN or CLOSE is only performed if an additional enable signal by the SIL module is applied.
If this is not the case, the operation in directions OPEN or CLOSE is stopped or even suspended.

> Safe OPENING/CLOSING combined with Safe STOP
In this case, Safe OPENING/Safe CLOSING function is prioritised.

In addition, safe end position feedback via actuator is possible.

Seating criteria
Like for normal operation, the criteria for actuator seating can be defined for safety functions. While the seating criteria serve the purpose of protecting both valve and actuator in normal operation, the request of a safety function can impose opening or closing of the valve, irrespective of any damage incurred for both actuator or valve.

Overall, the following seating criteria are available for the safety functions:

> Limit seating with overload protection
As soon as the preset switching points in end positions OPEN or CLOSED are reached, actuator controls automatically switch off the actuator. If excessive torque is applied during travel, e.g. due to a trapped object within the valve, the actuator is switched off to protect the valve prior to reaching the end position.

> Forced limit seating in end position
Actuator only stops once end positions OPEN or CLOSED are reached irrespective of the torque applied.

> Forced torque seating
Actuator only stops when reaching the set end position and the preset torque end position.

> No seating
In this instance, torque and limit switches are by-passed to force valve opening or closing. To avoid motor burn-out, we recommend using AC .2 in SIL version with thermal protection function.

MONITORING ACTUATOR OPERATION

Electromechanical monitoring of actuator operation via the SIL module is used to test system reliability. If the actuator does not start within a predefined time after an operation command, the SIL module activates the SIL collective failure signal.

This running monitoring is also active in normal operation.

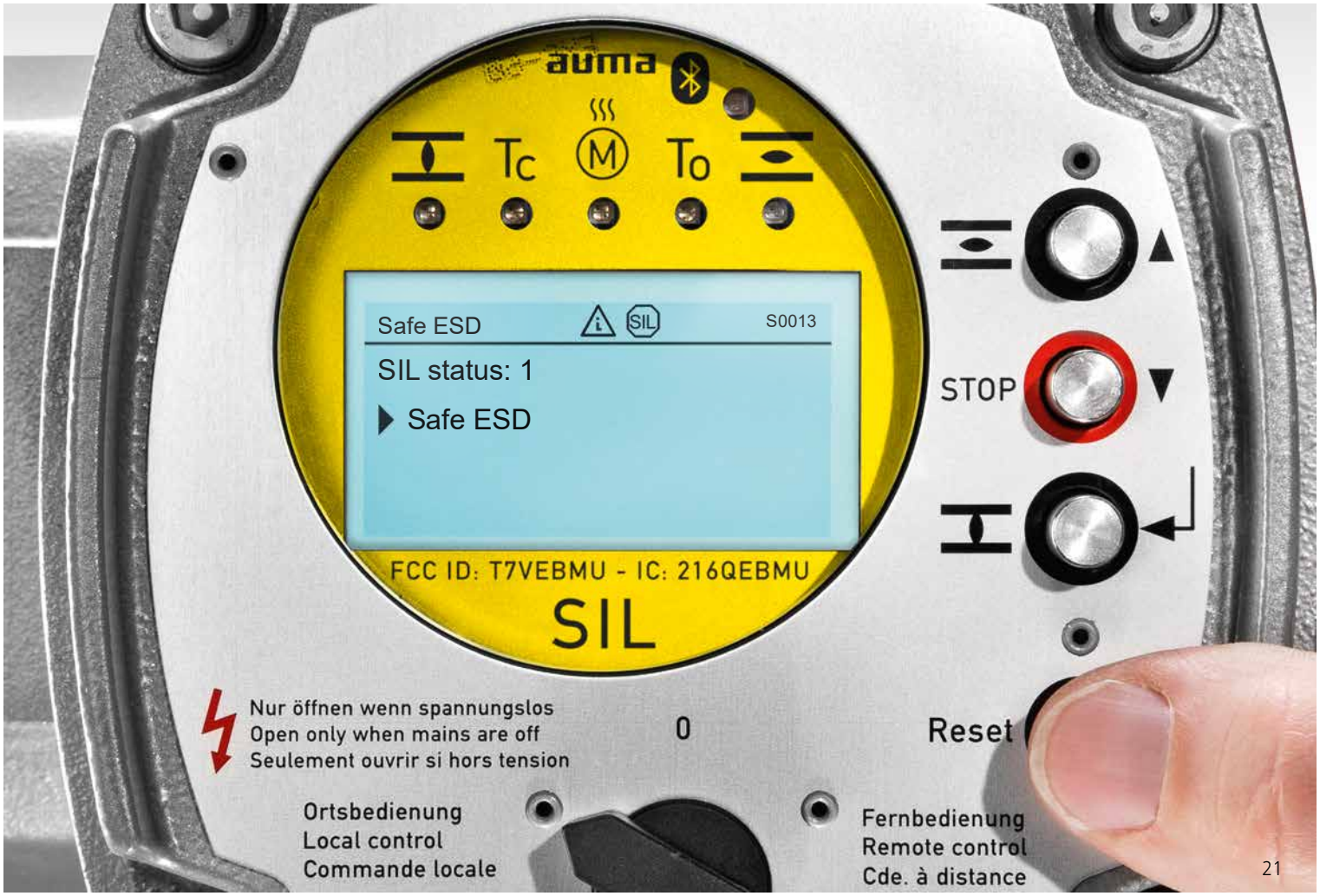
SAFE INPUTS AND OUTPUTS

The SIL module provides three safe inputs and two safe outputs:

> 1 redundant input for Safe OPENING/Safe CLOSING
(can be configured either for opening or for closing)
> 1 input for Safe STOP or enable in direction OPEN
> 1 input for Safe STOP or enable in direction CLOSE
> 1 output to signal a SIL collective fault
> 1 output to signal "system ready"

DISPLAY SUPPORT

Any information about the SIL module status, like performing a safety function or presence of a SIL collective fault signal, are indicated by means of symbols and texts on the AC .2 display.



FQM FAIL SAFE UNIT IN SIL VERSION

Availability of the safety function even during power failure is often requested.

With the FQM fail safe unit, AUMA offers innovative and safe actuation solutions for opening or closing valves in case of emergencies during power failures.

EXIDA CERTIFICATE FOR SIL 2/SIL 3 APPLICATIONS

FQM fail safe units in SIL version were certified by exida and may be used for safety related applications up to SIL 2 for single-channel system architecture and up to SIL3 for redundant system architecture.

The FQM fail safe unit is always used in combination with an SQ part-turn actuator and AC .2 actuator controls. The fail safe unit is also available in an explosion-proof and fireproof version.

Versatile implementation

AUMA actuators with FQM fail safe unit are particularly suited to automate butterfly valves as well as ball and plug valves at a swing angle of 90° (±10°). They are used in the most diverse industries, for example, within water reservoirs, they prevent leakage in the case of burst pipes. In cooling systems, they protect against overheating in case of conventional cooling system failure. Steam generating boilers in power plants and fire protection measures in tunnels are further typical examples.

Applications in the oil & gas industry

In the petrochemical industry, demands are particularly high. Explosion-proof and fireproof fail safe units cater for the required safety level. Typical applications include overflow protection in a tank farm, drainage protection in tanks and pipelines or use in gas regulating and metering stations.

MECHANICAL SOLUTION FOR UTMOST SAFETY

The innovative technology offers various advantages: The torque required in an emergency is provided via the energy mechanically stored in a constant force spring. No electrical power is required for fail safe operation.

The constant force spring motor provides a constant torque during fail safe operation across the complete travel. During standard operation, the constant force spring is disengaged and is not operated. As a consequence, actuator sizing can be relatively small.

Another advantage is the adjustable operating speed: It will be be reduced prior to reaching the end position so that the valve is operated slowly and softly into the end position. This avoids pressure peaks within the pipeline and protects the valve.

SAFETY FUNCTIONS

The following safety functions can be implemented by means of the FQM fail safe unit in SIL version:

> Safe OPENING/CLOSING
(Safe ESD, Emergency Shut Down)
FQM fail safe unit runs to configured end positions OPEN or CLOSED. For single-channel system architecture, this safety function achieves SIL 2 (SC = 3, 1oo1/HFT = 0) and for redundant system architecture SIL 3 (SC = 3, 1oo2/HFT = 1).

> Safe end position feedback
Safe end position feedback in accordance with SIL 2 can be achieved for single-channel system architecture via SIL qualified end position switches within the FQM fail safe unit. The signal can also be read in case of actuator power failure.

INITIATION OF A FAIL SAFE OPERATION

The following criteria for initiating fail safe operation are possible for a fail safe unit in SIL version:

> Emergency Shutdown (ESD) signal of a safety PLC
> Power failure OR ESD signal of a safety PLC

Fail safe operation is directly initiated within the FQM. This is independent of AC .2 actuator controls. The constant force spring is activated during fail safe operation and transmits the generated torque to the valve by means of a planetary gearing.

Application example: Overflow protection with FQMEx fail safe unit in SIL version
If it has to be ensured that the overflow protection should be fully operable in the event of power failure, the SIS can be implemented with FQMEx fail safe unit.

SIS and standard operation system are usually completely separated (refer to top right illustration). A standard PLC controls the entire tank filling system via a filling level sensor and a standard version actuator with pertaining valve. The valve of the SIS is OPEN during standard operation. The safety PLC continuously monitors the filling level within the tank via specific sensors. Once a specified limit has been exceeded, the safety PLC assumes a failure and sends an Emergency shutdown signal directly to the FQM fail safe unit. Fail safe operation is initiated and the valve of the SIS is closed.

SIS and standard operation system can in principle be combined (refer to bottom right illustration). However, it has to be verified for each application whether the IEC 61511 requirements on such a combined system are fully met.

SIL capability was determined to allow sound and reliable statements about suitability of AUMA products for safety relevant applications. IEC 61508 standard suggests two procedures which differ: Hardware assessment and complete assessment.

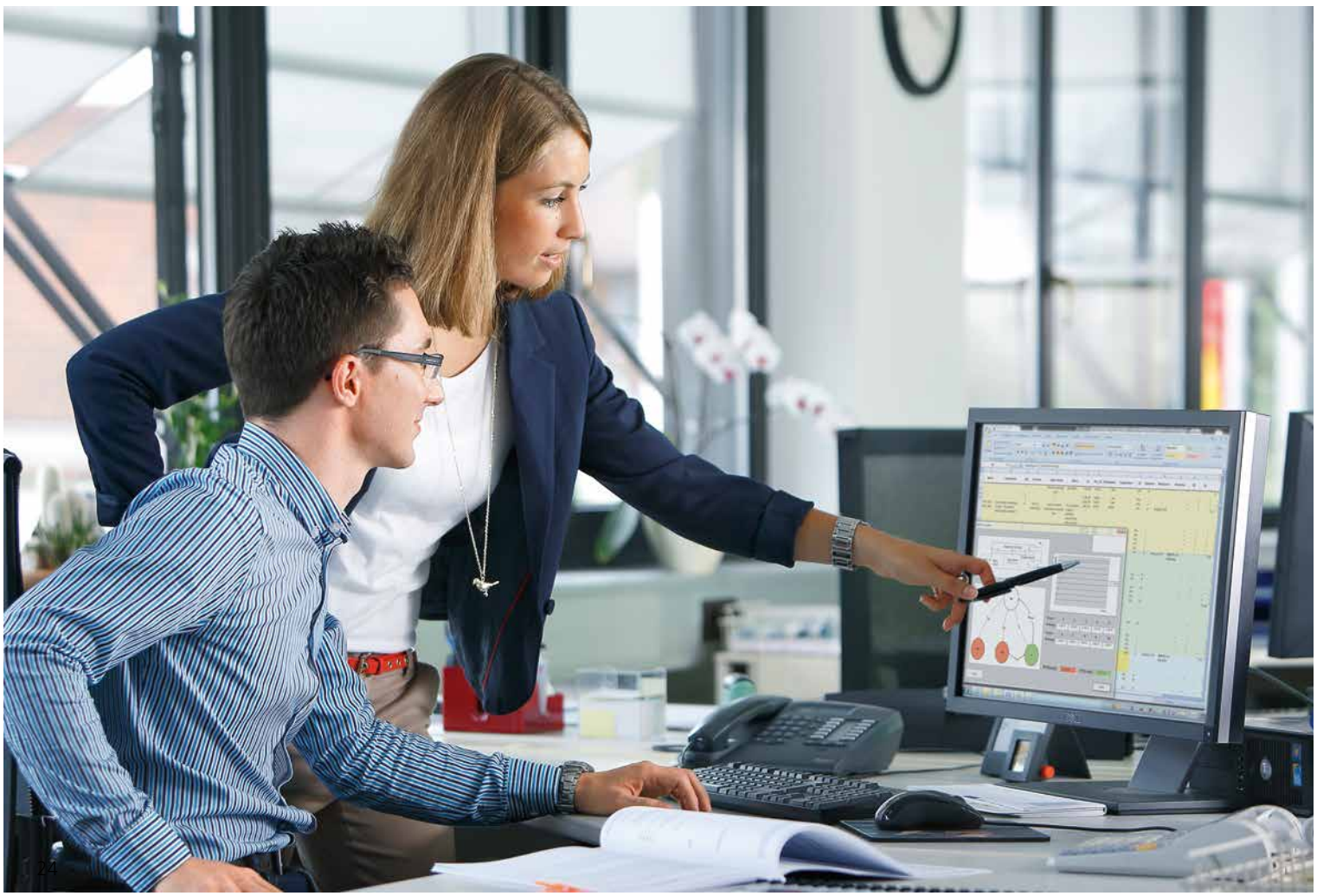
Hardware assessment

Assessment for existing AUMA products was made by hardware assessment based on field experience. This includes SA and SQ actuators as well as GK gearboxes, for example. For further information, please refer to page 25.

Complete assessment

The newly developed AC .2 actuator controls in SIL version and FQM fail safe unit in SIL version have been subjected to complete assessment. The relevant fault-avoiding measures in compliance with IEC 61508 were applied in all phases of the product life cycle, from product specification right through to decommissioning. For further information, please refer to page 26.

DETERMINATION OF SIL CAPABILITY FOR AUMA PRODUCTS



For assessment of pre-existing components, IEC 61508 standard provides statements on suitability on the basis of device hardware assessment.

Safety figures are determined for the various components which are used to perform SIL classification.

Generic data

Generic data collections are statistically determined failure rates for individual components. They are listed in special databases called "reliability data books". For assessment of electronic components used in AUMA products, generic data by exida and from SN 29500 Siemens standard were used, for example.

Experience data

For mechanical components, little generic data is available. Experience data, e.g. fault feedback signals during warranty period and test results, is used to draw conclusions about the reliability of the components concerned.

FMEDA

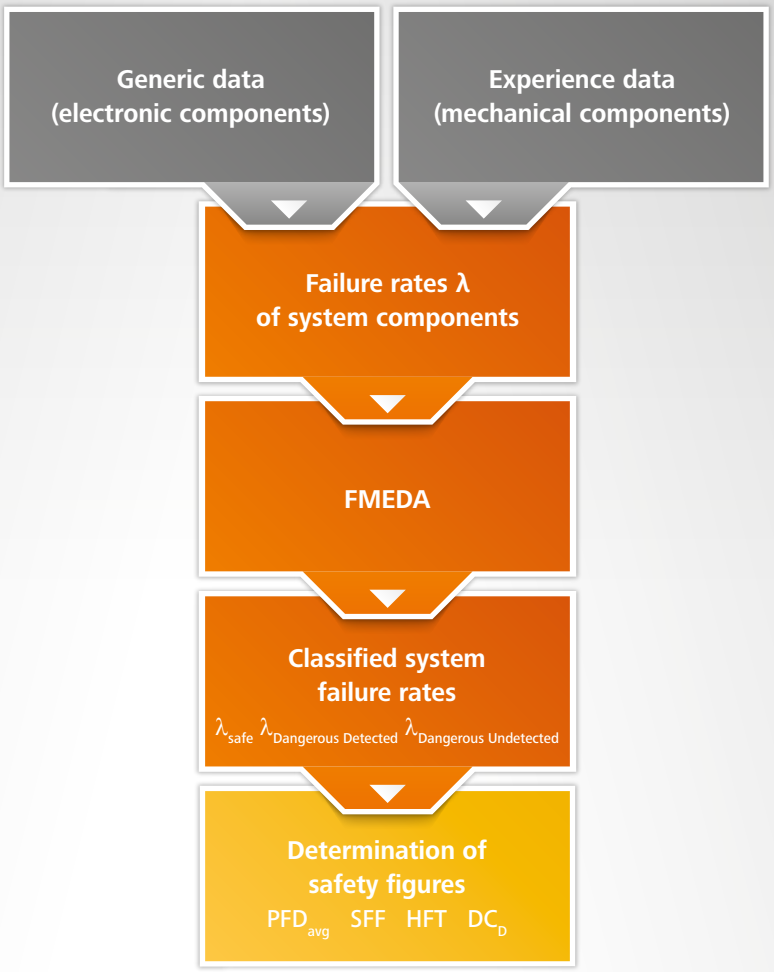
FMEDA (Failure Mode Effects and Diagnostic Analysis) is a recognised method to calculate safety figures in compliance with IEC 61508.

This analysis is made in defined steps, recorded and transparent at any time.

Failure scenarios and the respective probability of occurrence is examined by means of FMEDA. Furthermore, analysis is made as to whether potential faults are dangerous for the safety function and whether they can be diagnosed and thus identified.

The obtained failure rates are used to calculate the average probability of failure on demand (PFD_{avg}) as well as further safety figures such as safe failure fraction (SFF) and diagnostic coverage (DC_D).

Determining the safety figures



AC .2 actuator controls in SIL version and FQM fail safe unit in SIL version are new developments subjected to complete assessment in compliance with IEC 61508.

AC 01.2 in SIL version was certified by TÜV Nord and FQM in SIL version by exida.

What was tested?

Compared to mere hardware assessment of pre-existing products, the overall assessment includes tests and certifications of development and production procedures for systematic fault avoidance where possible.

Generally speaking, systematic faults are faults occurring e.g. during specification, development, production, commissioning, operation or maintenance. They are basically avoidable.

Functional Safety Management System

For avoidance of systematic faults, AUMA uses a Functional Safety Management (FSM) system. The FSM system can be considered as extension to a quality management system. Rules and definitions described within the framework of this system are used to avoid potential fault sources to the greatest extent possible. Furthermore actions are taken to detect and eliminate all remaining systematic fault sources in due time to prevent the occurrence of hazardous situations.

Determining the safety figures

The remaining random faults in spite of all risk reduction actions are subject to quantitative recording for assessing the residual risk. For this purpose, safety figures such as the probability of failure for the products are determined and provided to the customer.

At AUMA, this procedure is identical to the mere hardware assessment (refer to page 25).

DETERMINATION OF SIL CAPABILITY FOR AUMA PRODUCTS

TÜV NORD

DAkkS Deutsche Akkreditierungsstelle D-ZE-11074-01-00

Certificate

No. 1435.IM.155027/19 V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies

AUMA Riester GmbH & Co. KG
Aumastraße 1
79379 Müllheim, Germany

that the

electric actuator system with the actuators SA(R)07.1 – SA(R)16.1/ SA(R)ExC 07.1 – SA(R)ExC16.1, SA(R)07.2 – SA(R)16.2/ SA(R)Ex07.2 – SA(R)Ex16.2 and SQ(R)05.2- SQ(R)14.2/ SQ(R)Ex05.2- SQ(R)Ex14.2 with the actuator controls AC01.2/ACExC01.2 in SIL version

with the safety functions „Safe Emergency Shut Down (ESD)" and „Safe Stop" meets the requirements listed in the following standard.

- DIN EN 61508-1/-2: 2011, capable up to SIL 2 (HFT = 0) and SIL 3 (HFT ≥ 1)
- IEC 61508-1/-2: 2010, capable up to SIL 2 (HFT = 0) and SIL 3 (HFT ≥ 1)

Certification program Leittechnik (SEB-ZE-SEECERT-VA-320-20, Rev. 5.1 / 04.19)

Base of certification is the report 1435.IM.155027/19TB in the valid version.

This certificate entitles the holder to use the pictured safety approved mark.

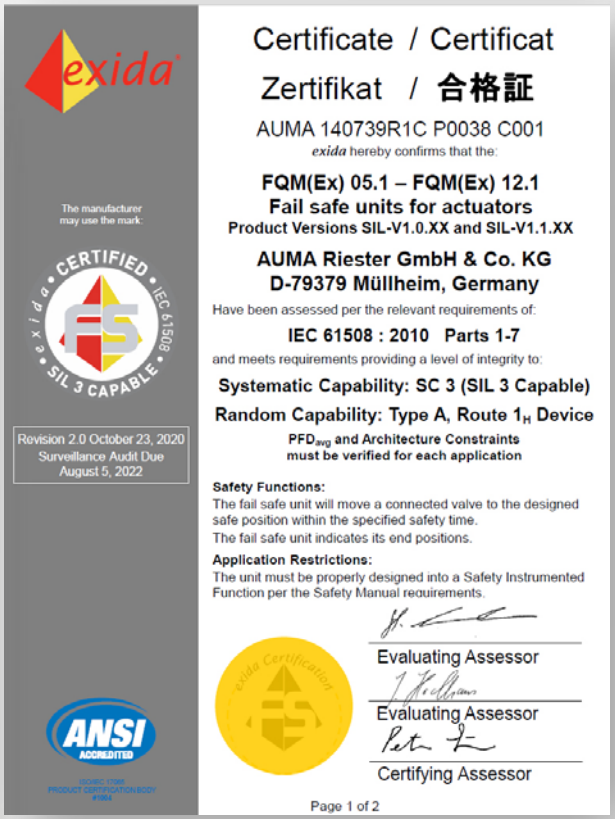
Valid until: 2024-12-17
File reference: 8117657310

Hamburg, 2019-12-17

Bianca Pfuff

TÜV NORD Safety Approved Electric Actuator System DIN EN 61508-1/-2: 2011 IEC 61508-1/-2: 2010 capable up to SIL 3

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany



exida

The manufacturer may use the mark:

CERTIFIED IEC 61508 SIL 3 CAPABLE

Revision 2.0 October 23, 2020
Surveillance Audit Due
August 5, 2022

ANSI ACCREDITED

Certificate / Certificat
Zertifikat / 合格証

AUMA 140739R1C P0038 C001

exida hereby confirms that the:

FQM(Ex) 05.1 – FQM(Ex) 12.1
Fail safe units for actuators
Product Versions SIL-V1.0.XX and SIL-V1.1.XX

AUMA Riester GmbH & Co. KG
D-79379 Müllheim, Germany

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 1_H Device

PFD_{avg} and Architecture Constraints must be verified for each application

Safety Functions:
The fail safe unit will move a connected valve to the designed safe position within the specified safety time.
The fail safe unit indicates its end positions.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Evaluating Assessor

Certifying Assessor

Page 1 of 2

ASK OUR EXPERTS

Selecting the right component for the implementation of a safety instrumented system is always challenging; merely calculating the probability of failure is not sufficient. The individual marginal conditions have to be examined and assessed.

Our experts look back on long standing experience with the use of electric actuators in safety instrumented systems. We are pleased to assist you in designing your SIS or selecting the appropriate actuator.

Please do not hesitate to contact us. We look forward to discussing different options with you.

USE OUR DOCUMENTATION

AUMA provides detailed and comprehensive material on functional safety.

You may request the following documents from AUMA:

> Declarations of incorporation
> Safety figures
> Safety manuals with checklists

The following documents on SIL classified actuators, actuator controls and gearboxes are directly available from www.auma.com:

> Manuals and operation instructions
> Technical data
> Product certificates

THIS IS SUPPORT BY AUMA

auma®
Solutions for a world in motion

AUMA Riester GmbH & Co. KG
Aumastr. 1
79379 Muellheim
Germany
Tel +49 7631 809-0
Fax +49 7631 809-1250
info@auma.com

AUMA subsidiaries and
representatives are implanted in more than 70 countries.
For detailed contact information,
please refer to our website.
www.auma.com