FUNCTIONAL SAFETY – SIL
Electric actuators for safety-related systems up to SIL 3
AUMA, the globally leading manufacturer of electric actuators for automating industrial valves. AUMA actuators work reliably all around the globe for managing flow of liquids or gases, powders or granulates: 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 focussed our complete engineering excellence on developing, manufacturing, distributing and servicing electric actuators. Our products have become renowned global brands whereby our customers particularly appreciate their long life, reliability, and highest precision.

As medium-sized family owned company, AUMA have grown to a successful global player, giving work to more than 2,400 people worldwide. Our cosmopolitan sales and service network offers you more competent local support in more than 70 countries.
AUMA’s broad portfolio of electric actuators is qualified for safety-related systems up to SIL 3. Our products contribute to 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.
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. For the first time, 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 or maintained in a safe state.

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 fire protection, electrical safety or explosion protection – significantly contributes to the overall safety of a system.
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 functions.

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 like TÜV and exida, we examined which SIL applies to our actuators, actuator controls and gearboxes.

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

Industrial accidents with disastrous consequences like the Seveso dioxin disaster in 1976 or the Indian Bhopal gas tragedy in 1984 put the worldwide standardisation process relating to safety into gear.

At EU level, first the Seveso I and later the Seveso II directive 96/82/EC 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 prime objective. Furthermore, definite instructions were given for systems with high hazard potential.

To harmonise these directives, national standards on functional safety were first created. The first international standard was issued in 1998 with the IEC 61508. IEC 61508 is still the valid standard on an international level and has meanwhile been updated.

IEC 61508

IEC 61508 is an international standard applicable to functional safety for electrical, electronic or programmable electronic components (E/E/PE) executing safety functions. The requirements by the standards are transplanted to other e.g. mechanical components where appropriate.

The standard is applicable for plant designers and operators as well as device manufacturers.

It serves the purpose of an independent basic standard and is complemented by further standards such as IEC 61511 for the process sector.

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 failure risks, the complete safety lifecycle of components is taken into account, from the specification via implementation until decommissioning.

IEC 61511

This standard includes the user specific implementation of IEC 61508 in particular for the process industry. It defines the requirements for safety-related systems used in the process industry for risk reduction.

This standard mainly applies to plant designers and users.

VALIDITY AND SCOPE OF STANDARDS

Standards IEC 61508 and 61511 are not yet binding within the European Union as they are still not harmonised within an EU directive. However, meeting the requirements presents a significant advantage for plant operators and device manufacturers:

> For plants and systems whose failure could have an impact on the safety of persons and the environment, the functional safety method is considered as "state-of-the-art".

> The standards can be used to fulfil basic requirements of EU directives if referenced by a harmonised European standard or if no harmonised standard is available for the specific application.

> Compliance with standards IEC 61508 and 61511 is increasingly demanded by authorities and insurance companies as proof for risk analysis with sufficient risk reduction.

> When using SIL classified products, plant operators and device manufacturers can be sure that the devices have been evaluated according to international standards and that the defined safety integrity level is met.
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
At first, processes in plants leading to potential hazards for persons and the environment must be examined if they run out of control.

Definition of SIL requirements
Each of the potentially hazardous processes is examined to determine the resulting 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 occurrence probability of the risk it will be defined whether a 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 initiate that their devices are tested for classification in compliance with the available safety integrity levels.

Verification of SIL requirements
On the basis of safety figures of implemented devices, verification is made for each safety function whether the demanded SIL is achieved. If this is not the case, additional actions will have to be taken.
Safety functions are safety 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.

Typical safety functions are, for example, automatic emergency stops for shutting off a device or vessel pressure monitoring and limitation.

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

- Safe OPENING/Safe CLOSING (Emergency Shutdown, ESD)
- Safe standstill/STOP
- Safe end position feedback

SAFE OPENING WITH THE EXAMPLE OF A PRESSURE SAFETY VALVE

For a vessel with potentially excessive pressure hazard, opening the pressure safety valve is considered as safety function.

A sensor continuously checks the vessel pressure. Once the pressure exceeds the preset limit, the safety PLC assumes a system failure and issues an opening signal for the actuator to relief the vessel.

SAFE STOP WITH THE EXAMPLE OF A LOCK

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

The Safe STOP safety function can also be used as interlock function. In this case, the lock can only be closed if the "Safe STOP" signal is not applied.
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 the demanded SIL is achieved for a safety function, the safety figures of all individual components forming the safety instrumented system must be considered (please also refer to page 12).

**WHAT IS A SAFETY INSTRUMENTED SYSTEM?**

Components of a typical safety instrumented system

1. Sensor
2. Safety PLC
3. Actor, consisting of actuator and valve
The PFDavg 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 the highest level. The higher the safety level, the lower the allowable probability for the failure of a safety function on demand.

The level of risk is not the only decisive factor for system safety in case of failure. The frequency of the expected failure and thus the respective demand for the appropriate safety function are also important factors.

IEC 61508 distinguishes between low demand and high demand (or continuous) modes of operation.

**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. 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.

**High Demand Mode (or Continuous Mode)**

In operation mode with high or continuous demand mode, the safety function either works continuously or is demanded more than once a year.

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

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Allowed PFDavg value (low demand)</th>
<th>Theoretically allowed failures for a safety function on demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>≥ 10^-2 to &lt; 10^-1</td>
<td>Allows one dangerous failure in 10 years</td>
</tr>
<tr>
<td>SIL 2</td>
<td>≥ 10^-3 to &lt; 10^-2</td>
<td>Allows one dangerous failure in 100 years</td>
</tr>
<tr>
<td>SIL 3</td>
<td>≥ 10^-4 to &lt; 10^-3</td>
<td>Allows one dangerous failure in 1,000 years</td>
</tr>
<tr>
<td>SIL 4</td>
<td>≥ 10^-5 to &lt; 10^-4</td>
<td>Allows one dangerous failure in 10,000 years</td>
</tr>
</tbody>
</table>

In a first step, PFD values are calculated for each component of a safety instrumented system.

A safety integrity level describes however the characteristics of a complete safety function and not of the mere individual component. For this reason, the total PFD value must then be calculated for the safety function on the basis of the PFD values of the individual components.
FAILURE RATES

The analysis of possible failure sources is of significant importance for the safety of a system.

When considering λ, failure rates, distinction is made as to which failures are classified as dangerous and which as safe and consequently without impact on the correct execution of a safety function. Furthermore, the diagnostic coverage of a failure is examined.

SAFE FAILURE FRACTION (SFF)

The SFF value (Safe Failure Fraction) describes the fraction in percent of safe failures and detected dangerous failures related to the total failure rate. Failures are considered as non-hazardous if they cannot put the system in a dangerous state.

The higher the value, the lower the probability of a dangerous system failure. A value of 62 % signifies that 62 out of 100 failures do not have an impact on the safe system function.

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 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

<table>
<thead>
<tr>
<th>SFF (Safe Failure Fraction)</th>
<th>HFT (Hardware Fault Tolerance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>SIL 1</td>
</tr>
<tr>
<td>60 % to &lt; 90 %</td>
<td>SIL 2</td>
</tr>
<tr>
<td>90 % to &lt; 99 %</td>
<td>SIL 3</td>
</tr>
<tr>
<td>≥ 99 %</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>

SFF and HFT for type B devices

<table>
<thead>
<tr>
<th>SFF (Safe Failure Fraction)</th>
<th>HFT (Hardware Fault Tolerance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
</tr>
<tr>
<td>60 % to &lt; 90 %</td>
<td>SIL 1</td>
</tr>
<tr>
<td>90 % to &lt; 99 %</td>
<td>SIL 2</td>
</tr>
<tr>
<td>≥ 99 %</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>

MEAN TIME BETWEEN FAILURES (MTBF)

The mean operating time between failures in years describes the theoretical operating time between two subsequent failures and allows to measure reliability. By no means should this figure be mixed up with lifetime or useful lifetime of the system.
It is always the SIL capability of the entire safety instrumented system and not of an individual component that is crucial to the safety of a safety function! Therefore, consideration of PFD values for the individual components is insufficient.

**SIL CAPABILITY OF A SAFETY FUNCTION**

In the most simple case, the PFD values of the individual components have to be added to determine the SIL capability of a safety function. The resulting PFD value of a safety function is then compared to the allowed total probability of dangerous failure on demand for the required SIL.

The figure below shows that even if exclusively SIL 2 classified components are used, it is not guaranteed that the safety function as a whole will also meet SIL 2. This level is only applicable if the total PFD value for all the whole safety function is within the target SIL 2 measure.
Should the calculations 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 function. Actuator or valve travel a predefined distance forth and back. Thus it is tested whether the actuator actually operates.

PVST is a recognised method to increase the availability of individual components of a safety function. This anticipating test allows exclusion of safety-related faults; the probability of dangerous failure on demand is reduced.

**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 can 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 $1002$ ("one out of two") configuration, one out of two devices is sufficient to perform the required safety function, for example. $2003$ ("Two out of three") configuration implies that two out of three devices must function properly. The actual system architecture depends on the demanded safety function.

A redundant system architecture can increase hardware fault tolerance and consequently SIL capability.

In general, a redundant system structure is implemented for SIL 3 applications according of IEC 61511, e.g. $1002$.
For plant designers and plant operators, it is of core importance to exclusively implement components meeting the respective safety requirements. AUMA have determined the safety figures and consequently the SIL capability for AUMA actuators, actuator controls and gearboxes to optimally support our customers with product selection.

Please refer to page 26 for the overview on all assessed AUMA products. Detailed safety figures for selected actuators are listed on page 24.

**ALLOCATED SAFETY FUNCTIONS**

The safety 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.

As core function, actuators serve the purpose to open and close valves. Consequently, AUMA actuator safety functions like Safe OPENING and Safe CLOSING are the major focus.

**SA AND SQ ACTUATORS WITHOUT INTEGRAL CONTROLS**

SA and SQ actuators without integral controls are classified as SIL 2 in the safety functions considered. SIL 3 can be achieved with a redundant system architecture. This also applies to SAR and SQR version for modulating duty as well as SAEx and SQEx for potentially explosive atmospheres.

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

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

For AC .2 and ACExC .2 integral controls in SIL version, the safety functions are executed via a separate board.

Actuators equipped with these controls are classified as SIL 2. SIL 3 can be achieved with a redundant system architecture.

The comprehensive functions of AC .2 is still available in standard operation.

Please also refer to the next pages for further details on AC .2 in SIL version.
**Safe OPENING/Safe CLOSING**
Upon request of the safety function, the actuator travels in direction end position OPEN or end position CLOSED.

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

**Safe standstill/Safe STOP**
Upon request of the safety function, the actuator motor is stopped. Undesired motor starts are prevented.

**Safe end position feedback**
The electromechanical control unit issues a safe signal as soon as one of the end positions OPEN or CLOSED or the tripping torque are reached. Within the framework of the standard, this is not considered as safety function. However in practical applications, it has proven beneficial to supply safety figures for this function.

**SA AND SQ ACTUATORS WITH AC .2 INTEGRAL CONTROLS IN STANDARD VERSION**
Actuators with AC .2 or ACExC .2 integral controls in standard version are classified as SIL 1 in the versions considered.
Safety function configuration can be made at the AC .2 for Safe OPENING/Safe CLOSING (ESD) or Safe STOP.

**SA AND SQ ACTUATORS WITH AM INTEGRAL CONTROLS**
Actuators with AM or AMEx integral controls are classified as SIL 2 in the versions considered. SIL 3 can be achieved with a redundant system architecture.
Safety functions Safe OPENING/Safe CLOSING can be performed either via standard inputs for opening and closing or via a separate EMERGENCY input.

**GK, GST, GS, AND GF GEARBOXES**
Safety figures were also determined for AUMA GK, GST, GS, and GF gearboxes. The considered gearboxes are all classified as SIL 2.
With the AC .2 integral controls in SIL version, AUMA provide modern controls for safety-related systems up to SIL 3. Safety functions are exclusively executed via the safe SIL module. During normal operation, all AC .2 functions are available.

TÜV APPROVALS FOR SIL2/SIL3 APPLICATIONS

You will appreciate the variety of functions and setting options when familiarising with AC .2 integral controls. Freely configurable parallel and fieldbus interfaces allow swift integration into sophisticated distributed control systems. AC .2 controls are ideally suited for 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.

AC. 2 INTEGRAL CONTROLS IN SIL VERSION

AC. 2 controls in SIL version with SIL module
The SIL module is an additional electronic board, responsible for executing the safety functions. This board is inserted into AC .2 and ACEx .2 integral controls.

If a safety function is requested in the event of an emergency, the standard logic of AC .2 is by-passed and the safety function is performed via the SIL module.

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 type A device. Determined safety figures allow implementation in SIL 2 applications and even in SIL 3 (provided the availability as redundant architecture - 1oo2).

Actuators equipped with AC .2 in SIL version combine two functions in one system. On the one hand, standard AC .2 functions can be used for “normal operation”. On the other hand, the integral SIL module performs the safety functions which always overrule normal operation. This is ensured due to the fact that the standard controls logic is by-passed when a safety function is requested.

If an actuator with AC .2 in SIL version is used as pure safety system, control via standard PLC is made obsolete.
FUNCTIONS OF THE SIL MODULE

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 in configured directions OPEN or CLOSE. 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 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 CLOSE are reached, 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 CLOSE are reached irrespective of the torque applied.

> Forced torque seating in end position
   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 (it can be configured either for opening or for closing)
- 1 input for Safe STOP or release in direction OPEN
- 1 input for Safe STOP or release in direction CLOSE
- 1 output to signal a SIL collective failure
- 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 failure signal, are indicated by means of symbols and texts on the AC.2 display.
Safety figures were determined to allow sound and reliable statements about the SIL capability of AUMA devices. Standards IEC 61508 and IEC 61511 suggest two procedures which differ: Hardware assessment and complete assessment.

Hardware assessment
AUMA have initiated a hardware assessment on the basis of already proven products. These include SA and SQ actuators, AM and AC .2 integral controls in standard version as well as GS and GF gearboxes.

Complete evaluation
As a matter of fact, development of AC .2 integral controls in SIL version has been completely assessed by TÜV Nord [German certification body]. Evaluation was made not only of the random faults but also the systematic faults in all phases of the product lifecycle, from product specification until decommissioning.

HARDWARE ASSESSMENT FOR EXISTING PRODUCTS

For assessment of established components, standards IEC 61508 and IEC 61511 provide statements on appropriateness on the basis of device hardware assessment.

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

The basis for the hardware assessment of AUMA actuator controls was generic data, for AUMA actuators experience data was used.
**Generic data**

Generic data collections are statistically determined failure rates for individual components listed in special databases called "reliability data books". Examples are Siemens SN 29500 Standard or the exida handbook.

The safety figures for electronic components used in AUMA products in particular in AUMA actuator controls were determined on the basis of the exida handbook.

**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.

Data gained during the last ten years was used to determine the safety figures for AUMA actuators.

**FMEDA**

According to IEC 61508 standard, 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.

Fault scenarios and the respective probability of occurrence is examined by means of FMEDA. Furthermore, analysis is made 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$_D$).
AC .2 integral controls in SIL version is a development which has been subjected to an overall assessment in compliance with IEC 61508. The total system consisting of SA .2 actuator and AC .2 actuator controls in SIL version has been evaluated. Certification was performed by TÜV Nord.

**What was tested?**

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

The chart below explains the basic principle of an overall assessment in compliance with IEC 61508. Systematic as well as random faults of a product are considered.

<table>
<thead>
<tr>
<th>Systematic faults</th>
<th>Random faults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basically avoidable</td>
<td>Basically unavoidable</td>
</tr>
<tr>
<td>Objective: Fault avoidance</td>
<td>Objective: Faults control</td>
</tr>
</tbody>
</table>

**Systematic faults**

In general, systematic faults can be avoided since they are usually development faults or failures in manufacture. By means of a Functional Safety Management System, possible fault sources are searched for and appropriate actions are taken to avoid systematic faults.

**Functional Safety Management System**

A Functional Safety Management (FSM) system can be considered as extension to a Quality Management system. The described regulations and definitions allow elimination of a large fraction of systematic fault sources.

---

**Basic principle of an overall assessment**

**Functional Safety Management (FSM) System**

- Diagnosis, redundancy

**Faults not avoided**

- **Faults are avoided**

**Determination of safety figures**

---

**DETERMINATION OF SAFETY FIGURES FOR AUMA PRODUCTS**
Random faults
Random faults are for example due to external disturbance and are considered as basically unavoidable. Therefore, methods have to be introduced to manage these faults as far as possible.

Appropriate actions are e.g. additional system monitoring and system diagnostic as well as redundant architecture.

Determining the safety figures
The residual faults in spite of all risk reduction actions have to be 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 supplied to the customer.

At AUMA, this procedure is identical to the pure hardware assessment (refer to page 21).
SAFETY FIGURES FOR SELECTED AUMA PRODUCTS

In the following, please find an extract of safety figures for selected actuators and actuator controls.

The safety figures depend on the safety function since the definition of the safe condition can differ and thus different means of consideration are required. For actuators with integral controls, safety figures depend furthermore on the wiring diagram version due to the fact that different elements with differing failure rates are used. Altogether, safety figures for approx. 150 different versions were determined.

Please contact us for further details.

MULTI-TURN ACTUATORS SA/SAR 07.2 – SA/SAR 16.2 AND SAEX/SAREX 07.2 – SAEXC/SAREXC 16.2
WITHOUT INTEGRAL CONTROLS

<table>
<thead>
<tr>
<th>Exida report</th>
<th>AUMA 10/03-053 R066 [F1]</th>
<th>AUMA 10/03-053 R066 [F2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety function</td>
<td>Safe OPENING/Safe CLOSING</td>
<td>Safe OPENING/Safe CLOSING with PVST (1)</td>
</tr>
<tr>
<td>( \lambda_{\text{safe}} )</td>
<td>367 FIT</td>
<td>367 FIT</td>
</tr>
<tr>
<td>( \lambda_{\text{PD}} )</td>
<td>0 FIT</td>
<td>162 FIT</td>
</tr>
<tr>
<td>( \lambda_{\text{DU}} )</td>
<td>203 FIT</td>
<td>41 FIT</td>
</tr>
<tr>
<td>DC(0)</td>
<td>0 %</td>
<td>80 %</td>
</tr>
<tr>
<td>MTBF</td>
<td>200 years</td>
<td>200 years</td>
</tr>
<tr>
<td>SFF</td>
<td>64 %</td>
<td>92 %</td>
</tr>
<tr>
<td>( T_{\text{[proof]}} = 1 \text{ year} )</td>
<td>( \text{PFD}_{\text{avg}} = 1.05 \times 10^{-3} )</td>
<td>( \text{PFD}_{\text{avg}} = 4.96 \times 10^{-4} )</td>
</tr>
<tr>
<td>( T_{\text{[proof]}} = 2 \text{ years} )</td>
<td>( \text{PFD}_{\text{avg}} = 1.92 \times 10^{-3} )</td>
<td>( \text{PFD}_{\text{avg}} = 6.55 \times 10^{-4} )</td>
</tr>
<tr>
<td>( T_{\text{[proof]}} = 5 \text{ years} )</td>
<td>( \text{PFD}_{\text{avg}} = 4.53 \times 10^{-3} )</td>
<td>( \text{PFD}_{\text{avg}} = 1.13 \times 10^{-3} )</td>
</tr>
<tr>
<td>SIL capability (2)</td>
<td>SIL 2 (1oo1)/SIL 3 (1oo2)</td>
<td>SIL 2 (1oo1)/SIL 3 (1oo2)</td>
</tr>
</tbody>
</table>

MULTI-TURN ACTUATORS SA/SAR 07.2 – SA/SAR 16.2
WITH AC 01.2 ACTUATOR CONTROLS IN SIL VERSION

Data for a multi-turn actuator with contactors as switchgear are referenced to as an example.

<table>
<thead>
<tr>
<th>TÜV certificate</th>
<th>SEBS-A. 120728/13 V1.0</th>
<th>SEBS-A. 120728/13 V1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety function</td>
<td>Safe ESD (Safe OPENING/Safe CLOSING)</td>
<td>Safe STOP</td>
</tr>
<tr>
<td>( \lambda_{\text{safe}} )</td>
<td>185 FIT</td>
<td>591 FIT</td>
</tr>
<tr>
<td>( \lambda_{\text{PD}} )</td>
<td>766 FIT</td>
<td>89 FIT</td>
</tr>
<tr>
<td>( \lambda_{\text{DU}} )</td>
<td>167 FIT</td>
<td>200 FIT</td>
</tr>
<tr>
<td>DC(0)</td>
<td>82 %</td>
<td>30 %</td>
</tr>
<tr>
<td>MTBF</td>
<td>46 years</td>
<td>48 years</td>
</tr>
<tr>
<td>SFF</td>
<td>85 %</td>
<td>77 %</td>
</tr>
<tr>
<td>( T_{\text{[proof]}} = 1 \text{ year} )</td>
<td>( \text{PFD}_{\text{avg}} = 2.01 \times 10^{-3} )</td>
<td>( \text{PFD}_{\text{avg}} = 1.69 \times 10^{-3} )</td>
</tr>
<tr>
<td>SIL capability (2)</td>
<td>SIL 2 (1oo1)/SIL 3 (1oo2)</td>
<td>SIL 2 (1oo1)/SIL 3 (1oo2)</td>
</tr>
</tbody>
</table>

1 Partial Valve Stroke Test must be executed at least once a month.
2 SIL capability means that the calculated data is within the range for the appropriate SIL, but does not mean that all relevant conditions of IEC 61508 are fulfilled.
3 SIL 3 can be achieved by redundant system architecture (1oo2 “one out of two”).

24
**Figure Explanation**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| $\lambda_{\text{safe}}$ | **Lambda safe** – number of safe failures per unit of time  
Indicates the failure rate, i.e. the number of failures of a component per unit of time. The failure rates are required to calculate the probabilities of failure on demand.  
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.  
The failure is considered as safe or without hazard provided the occurrence does not place the system into a dangerous state. |
| $\lambda_{\text{DD}}$ | **Lambda Dangerous Detected** – Number of detected dangerous failures per unit of time  
Indication is made of the number of detected dangerous failures per $10^9$ hours on the basis of diagnostic tests.  
A component failure is classified as dangerous if it prevents execution of a safety function. |
| $\lambda_{\text{DU}}$ | **Lambda Dangerous Undetected** – Number of undetected dangerous failures per unit of time  
Indication is made of the number of undetected dangerous failures per $10^9$ hours. |
| $\text{DCD}$ | **Diagnostic Coverage of Dangerous Failures**  
Fraction of dangerous failures detected by diagnostic tests $\lambda_{\text{DD}}$ associated with the total rate of dangerous failures in percent. |
| $\text{MTBF}$ | **Mean Time Between Failure** – Mean operating time between failures  
Describes the operating time between two subsequent component failures. The pure MTBF indication refers to the reliability of a device. |

<table>
<thead>
<tr>
<th>Figure</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| SFF | **SFF Safe Failure Fraction** – Fraction of safe failures  
Describes the percentage fraction of safe failures which means those failures which either do not lead to dangerous system failure or which can be detected by means of diagnostic tests.  
The higher the value, the lower the probability of a dangerous system failure. A value of 62 % means that 62 of 100 failures within the system are non-critical in view of safe function. |
| $T_{\text{proof}}$ | **Interval for proof tests**  
The safety figures are valid for a defined operating time. Thereafter, a proof test is imperatively required to restore the device to its designed functionality.  
The PFD value can be improved by reducing the time between two proof tests. However, time intervals of less than one year do not make sense. |
| $PFD_{\text{avg}}$ | **Probability of Failure on Demand**  
Mean probability of the inability to perform the safety function on demand. |
| SIL capability | Allocation to the appropriate safety integrity level by means of the component $PFD_{\text{avg}}$ value or, if applicable, by means of limitations for system architecture. The basis is the $T_{\text{proof}}$ interval of one year.  
For defining the SIL of an overall safety instrumented system, the PFD values of all components must be added (please also refer to page 12). |

**FURTHER INFORMATION**

This brochure aims at introducing the topic of functional safety. If you wish further information on the subject, please also refer to:

> Standard IEC 61508 parts 1 – 7
> Standard IEC 61511 parts 1 – 3
> Special publication “Funktionale Sicherheit” [functional safety] by Josef Börcsök
Upon request, AUMA will supply you with test reports or declarations of incorporation for all SIL classified AUMA products. Please refer to sample data on page 24.

<table>
<thead>
<tr>
<th>Actuators / Gearboxes</th>
<th>Actuator controls</th>
<th>SIL capability</th>
<th>Safety function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA/SAR 07.2 – 16.2</td>
<td>without controls</td>
<td>SIL 2(^{1)})</td>
<td>Safe OPENING/CLOSING (ESD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIL 3(^{2)})</td>
<td>Safe standstill/STOP</td>
</tr>
<tr>
<td>AM 01.1/02.1</td>
<td>SIL 2(^{1)})</td>
<td>Safe end position feedback</td>
<td></td>
</tr>
<tr>
<td>AMExC 01.1</td>
<td>SIL 2(^{1)})</td>
<td>Safe OPENING/CLOSING (ESD)</td>
<td></td>
</tr>
<tr>
<td>AMExB 01.1</td>
<td>SIL 3(^{2)})</td>
<td>Safe standstill/STOP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safe end position feedback</td>
<td></td>
</tr>
<tr>
<td>AC 01.2 in SIL version</td>
<td>SIL 2(^{1)})</td>
<td>Safe OPENING/CLOSING (ESD)</td>
<td></td>
</tr>
<tr>
<td>ACExC 01.2 in SIL version</td>
<td>SIL 2(^{1)})</td>
<td>Safe standstill/STOP</td>
<td></td>
</tr>
<tr>
<td>AC 01.2 (standard)</td>
<td>SIL 1(^{1)})</td>
<td>Safe end position feedback</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIL 2(^{1)})</td>
<td>Safe OPENING/CLOSING (ESD)</td>
<td></td>
</tr>
</tbody>
</table>

| SA/SAR 07.1 – 16.1    | without controls  | SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
|                       |                   | SIL 3\(^{2)}\)    | Safe standstill/STOP |
| AM 01.1/02.1          | SIL 2\(^{1)}\)    | Safe end position feedback |
| AMExC 01.1            | SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| AMExB 01.1            | SIL 3\(^{2)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |
| AC 01.1               | SIL 1\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| ACExC 01.1            | SIL 2\(^{1)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |

| SQ/SQR 05.2 – 14.2    | without controls  | SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
|                       |                   | SIL 3\(^{2)}\)    | Safe standstill/STOP |
| AM 01.1/02.1          | SIL 2\(^{1)}\)    | Safe end position feedback |
| AMExC 01.1            | SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| AMExB 01.1            | SIL 3\(^{2)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |
| AC 01.2 in SIL version| SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| ACExC 01.2 in SIL version| SIL 2\(^{1)}\) | Safe standstill/STOP |
| AC 01.2 (standard)    | SIL 1\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| ACExC 01.2 (standard) | SIL 2\(^{1)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |

| SG/SGR 05.1 – 12.1    | without controls  | SIL 1\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
|                       |                   | SIL 2\(^{1)}\)    | Safe standstill/STOP |
| AM 01.1/02.1          | SIL 1\(^{1)}\)    | Safe end position feedback |
| AMExC 01.1            | SIL 2\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| AMExB 01.1            | SIL 2\(^{1)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |
| AC 01.1               | SIL 1\(^{1)}\)    | Safe OPENING/CLOSING (ESD) |
| ACExC 01.1            | SIL 2\(^{1)}\)    | Safe standstill/STOP |
|                       |                   | Safe end position feedback |

| GK 10.2 – 25.2        | not relevant      | SIL 2\(^{1)}\)    | not relevant |
| GST 10.1 – 40.1       | not relevant      | SIL 2\(^{1)}\)    | not relevant |
| GS 50.3 – 250.3, GS 315 – 500 | not relevant | not relevant |
| GF 50.3 – 250.3       | not relevant      | SIL 2\(^{1)}\)    | not relevant |

1 One-channel system, “1oo1” (“one out of one”)
2 Redundant system, “1oo2” (“one out of two”)
3 Depending on wiring diagram and safety function
AUMA Riester GmbH & Co. KG
Aumastr. 1,
79379 Muellheim
Germany
Tel +49 7631-809-0
Fax +49 7631-809-1250
riester@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