auma®
Solutions for a world in motion

FUNKTIONALE SICHERHEIT – SIL

Elektrische Stellantriebe für sicherheitsbezogene Systeme bis SIL 3

AUMA ist ein weltweit führender Hersteller von elektrischen Stellantrieben für die Automatisierung von Industriearmaturen. Stellantriebe von AUMA bewähren sich auf der ganzen Welt überall dort, wo Flüssigkeits- oder Gasströme, Pulver oder Granulate reguliert und gesteuert werden: in der Wasserver- und -entsorgung, in Kraftwerken, Rohrleitungsnetzen, Raffinerien ebenso wie in industriellen Anlagen jeder Art.

DIE SPEZIALISTEN FÜR ELEKTRISCHE STELLANTRIEBE

Seit der Unternehmensgründung 1964 konzentrieren wir uns auf die Entwicklung, die Herstellung, den Vertrieb und den Service von elektrischen Stellantrieben. Unsere Produkte haben sich bei unseren Kunden weltweit einen Namen gemacht für Langlebigkeit, Zuverlässigkeit und Präzision.

Als mittelständisches Privatunternehmen hat sich AUMA zu einem erfolgreichen Global Player mit weltweit mehr als 2 600 Mitarbeitern entwickelt. Unser weltumspannendes Vertriebs- und Servicenetzwerk bietet Ihnen kompetente Ansprechpartner in über 70 Ländern.

AUMA AUTOMATISIERT ARMATUREN

FUNKTIONALE SICHERHEIT

AUMA bietet eine breite Palette an elektrischen Stellantrieben, die für sicherheitsbezogene Systeme bis SIL 3 zugelassen sind. Unsere Produkte tragen weltweit zum sicheren Betrieb technischer Anlagen bei. International anerkannte Prüfinstitute haben Sicherheitskennzahlen und SIL-Fähigkeit für unsere Produkte ermittelt.

In dieser Broschüre finden Sie neben detaillierten Informationen über die SIL-Fähigkeit der AUMA Produkte auch eine grundlegende Einführung in das Thema funktionale Sicherheit und SIL.

Weitere Informationen wie Zertifikate, Prüfberichte, Sicherheitskennzahlen oder unsere umfangreichen Handbücher „Funktionale Sicherheit – SIL" können Sie bei uns anfordern oder von unserer Website www.auma.com herunterladen.

INHALT

2021.09.15

Fragen zur Sicherheit von modernen Industrieanlagen gewinnen immer mehr an Bedeutung, insbesondere bei Anlagen mit hohem Gefahrenpotenzial im Öl- und Gas-Bereich, in der chemischen Industrie oder in Kraftwerken.

Zur Überwachung von Prozessen, von denen eine Gefahr für Mensch und Umwelt ausgeht, werden heute zunehmend moderne Sicherheitssysteme eingesetzt, die bei einem Störfall eingreifen. Solche Systeme schalten zum Beispiel im Notfall eine Anlage ab, stoppen die Zufuhr gefährlicher Stoffe, sorgen für Kühlung oder öffnen Überdruckventile. Um die Gefahren, die von einer Anlage ausgehen, zu reduzieren, müssen diese Systeme ihre Sicherheitsfunktion im Notfall zuverlässig ausführen und dürfen nicht ausfallen.

Wie aber können Anlagenbetreiber und Gerätehersteller sicherstellen, dass die eingesetzten Systeme „sicher" arbeiten und die nötigen Anforderungen erfüllen? Wie können Ausfallrisiken beurteilt werden?

Hier geben die Normen zur funktionalen Sicherheit IEC 61508 und IEC 61511 eine Antwort. Sie beschreiben Methoden, um die Ausfallrisiken von modernen, oft softwaregesteuerten Systemen zu beurteilen und Maßnahmen zur Risikoreduzierung zu bestimmen.

WAS IST FUNKTIONALE SICHERHEIT?

Funktionale Sicherheit nach der IEC 61508 bezieht sich auf Systeme, die Sicherheitsfunktionen ausführen und deren Ausfall ein erhebliches Risiko für Mensch und Umwelt darstellt.

Um funktionale Sicherheit zu erreichen, muss eine Sicherheitsfunktion bei einem Störfall dafür sorgen, dass eine technische Anlage in einen sicheren Zustand geführt wird oder in einem sicheren Zustand bleibt.

In der Prozessindustrie geht es bei der funktionalen Sicherheit also nicht um die grundsätzlichen Gefahren eines Produkts oder einer Anlage, wie zum Beispiel rotierende Teile, sondern um die Gefahren, die auf Grund eines Ausfalls einer Sicherheitsfunktion von einer Anlage ausgehen können.

Ziel der funktionalen Sicherheit ist es, die Wahrscheinlichkeit gefährlicher Ausfälle und damit auch die Risiken für Mensch und Umwelt auf ein vertretbares Maß zu reduzieren.

Insgesamt leistet die funktionale Sicherheit – gemeinsam mit weiteren Maßnahmen, wie zum Beispiel dem Brandschutz, der elektrischen Sicherheit oder dem Explosionsschutz – einen wichtigen Beitrag zur Gesamtsicherheit einer Anlage.

RISIKOREDUZIERUNG DURCH FUNKTIONALE SICHERHEIT

WAS IST SIL?

SIL ist ein Begriff, der mit der funktionalen Sicherheit in enger Verbindung steht. SIL steht für Sicherheits-Integritätslevel (engl. Safety Integrity Level) und ist eine Maßeinheit für die Risikoreduzierung durch Sicherheitsfunktionen.

Je größer die Gefahren sind, die von einem Prozess oder einer Anlage ausgehen, desto höher sind die Anforderungen an die Zuverlässigkeit der Sicherheitsfunktionen.

Die IEC 61508 definiert vier verschiedene Sicherheitsanforderungsstufen, SIL 1 bis SIL 4.

SIL 4 stellt dabei die höchsten Anforderungen an die Sicherheit, SIL 1 die niedrigsten. Für jeden dieser Level sind spezifische Ausfallwahrscheinlichkeiten definiert, die eine Sicherheitsfunktion nicht überschreiten darf.

Welcher SIL erforderlich ist, kann anhand einer Risikobeurteilung ermittelt werden.

WELCHE ROLLE SPIELT AUMA?

AUMA Produkte werden als Komponenten in Systemen eingesetzt, die Sicherheitsfunktionen ausführen. Daher haben wir – in Zusammenarbeit mit unabhängigen Prüfinstituten wie TÜV und exida – untersucht, für welchen SIL unsere Stellantriebe, Stellantriebs-Steuerungen und Getriebe geeignet sind.

Anhand der dabei ermittelten Spezifikationen und Sicherheitskennzahlen können Anlagenplaner die passenden Geräte für die jeweiligen Sicherheitsanforderungen auswählen.

NORMEN ZUR FUNKTIONALEN SICHERHEIT

DIE URSPRÜNGE

Es waren Industrieunfälle mit verheerenden Folgen, wie der Dioxin-Unfall von Seveso 1976 oder das Unglück im indischen Bhopal 1984, die weltweit Normungsprozesse zur Sicherheit von technischen Anlagen in Gang setzten.

So entstanden zum Beispiel auf EU-Ebene zunächst die Seveso I-, die Seveso II- und später die sogenannte Seveso-III- oder Störfall-Richtlinie (Richtlinie 2012/18/EU) zur Beherrschung der Gefahren bei Unfällen mit gefährlichen Stoffen. Mit diesen Richtlinien wurde der Schutz von Mensch, Umwelt und Sachwerten als oberstes Ziel festgeschrieben. Zudem wurden konkrete Vorgaben für Anlagen mit hohem Gefahrenpotenzial erlassen.

In diesem Kontext entstanden in der Folge zunächst nationale Normen zur funktionalen Sicherheit. Seit 1998 steht mit der IEC 61508 hier erstmals eine international gültige Norm zur Verfügung.

IEC 61508

Die IEC 61508 ist eine der wichtigsten weltweit gültigen Normen zur funktionalen Sicherheit von elektrischen, elektronischen oder programmierbar elektronischen Systemen (E/E/PES), die Sicherheitsfunktionen ausführen. Die Normanforderungen werden – wo zutreffend – auch auf andere, zum Beispiel mechanische Komponenten übertragen. Die Norm liegt seit 2010 in einer neuen Fassung vor.

Die Norm richtet sich als generische Grundnorm sowohl an Anlagenplaner und Anlagenbetreiber als auch an Gerätehersteller und wird ergänzt durch weitere, anwendungsspezifische Normen, zum Beispiel die IEC 61511 für die Prozessindustrie.

Konzept der Risikominderung
Ziel ist es, die Risiken von Prozessen und Anlagen durch den Einsatz von sicherheitsbezogenen Systemen zu reduzieren. Die Norm geht grundsätzlich davon aus, dass es nicht möglich ist, jegliche Risiken auszuschließen. Sie bietet jedoch Methoden zur Risikoanalyse, zur Risikominderung und zur Quantifizierung des Restrisikos.

Anforderungen an sicherheitsbezogene Systeme
Die Norm beschreibt die Anforderungen an sicherheitsbezogene Systeme bzw. an die Sicherheitsfunktionen und definiert Sicherheits-Integritätslevel (SIL). Daraus werden entsprechende SIL-Anforderungen an die eingesetzten Systemkomponenten abgeleitet.

Berücksichtigung des Lebenszyklus
Um die Ausfallrisiken zu minimieren, wird der gesamte Sicherheitslebenszyklus der Komponenten berücksichtigt, von der Spezifikation über die Realisierung bis hin zur Außerbetriebsetzung.

IEC 61511

Diese Norm beinhaltet die anwendungsspezifische Umsetzung der IEC 61508 speziell für die Prozessindustrie, insbesondere die chemische und die petrochemische Industrie. Sie definiert die Anforderungen an sicherheitsbezogene Systeme, die in prozesstechnischen Anlagen zur Risikominderung eingesetzt werden. Als Maß für die geforderte Risikoreduzierung verwendet sie ebenfalls die Sicherheits-Integritätslevel SIL 1 bis SIL 4.

Sie richtet sich in erster Linie an Anlagenplaner und Anlagenbetreiber.

IEC 62061

Diese Norm befasst sich mit der Sicherheit von Maschinen. Die Anforderungen an die funktionale Sicherheit leiten sich von der IEC 61508 ab. Die IEC 62061 verwendet die Sicherheits-Integritätslevel SIL 1 bis SIL 3.

Sie richtet sich in erster Linie an Anlagenplaner und Anlagenbetreiber.

EN ISO 13849

Die EN ISO 13849 zur Sicherheit von Maschinen beschäftigt sich mit Sicherheitsanforderungen für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen. Sie nimmt eine Klassifizierung nach Performance Level (PL) vor. Das PL stellt ein Maß für die Reduzierung des von der Maschine ausgehenden Risikos dar. Die Einteilung erfolgt von „a“ bis „e“, wobei „e“ den höchsten PL darstellt.

Funktionale Sicherheit gemäß EN ISO 13849 wird zum Beispiel in Deutschland häufig in der Wasserkraft und im Stahlwasserbau gefordert.

WIE WIRD FUNKTIONALE SICHERHEIT ERREICHT?

SICHERHEITSTECHNISCHE BEURTEILUNG

Um funktionale Sicherheit zu erreichen, müssen zunächst einmal die Risiken analysiert werden, die von einer Anlage oder einem Prozess ausgehen. Hier bieten die Normen IEC 61508 und 61511 eine anerkannte Methode zur Risikobeurteilung.

Durch eine differenzierte sicherheitstechnische Beurteilung werden diejenigen Prozesse identifiziert, von denen tatsächlich eine Gefahr ausgeht. So können Maßnahmen zur Risikoreduzierung gezielt dort eingesetzt werden, wo sie wirklich nötig sind.

Welche Prozesse sind gefährlich?

Zunächst wird untersucht, von welchen Prozessen einer Anlage Gefahren für Mensch und Umwelt ausgehen, wenn sie außer Kontrolle geraten.

Festlegung der SIL Anforderungen

Für jeden der gefahrbringenden Prozesse wird dann untersucht, wie groß Gefahr und Schadensausmaß infolge einer Fehlfunktion sein können.

Zur Beurteilung kann ein Risikograph wie unten dargestellt zu Hilfe genommen werden. Je nach Größe der Gefahr und Eintrittswahrscheinlichkeit wird festgelegt, ob ein Prozess durch eine Sicherheitsfunktion abgesichert werden muss und welchen Sicherheits-Integritätslevel (SIL) diese Sicherheitsfunktion erreichen muss.

Auswahl geeigneter Komponenten

Entsprechend des erforderlichen SIL werden die Komponenten zur Realisierung der Sicherheitsfunktion ausgewählt.

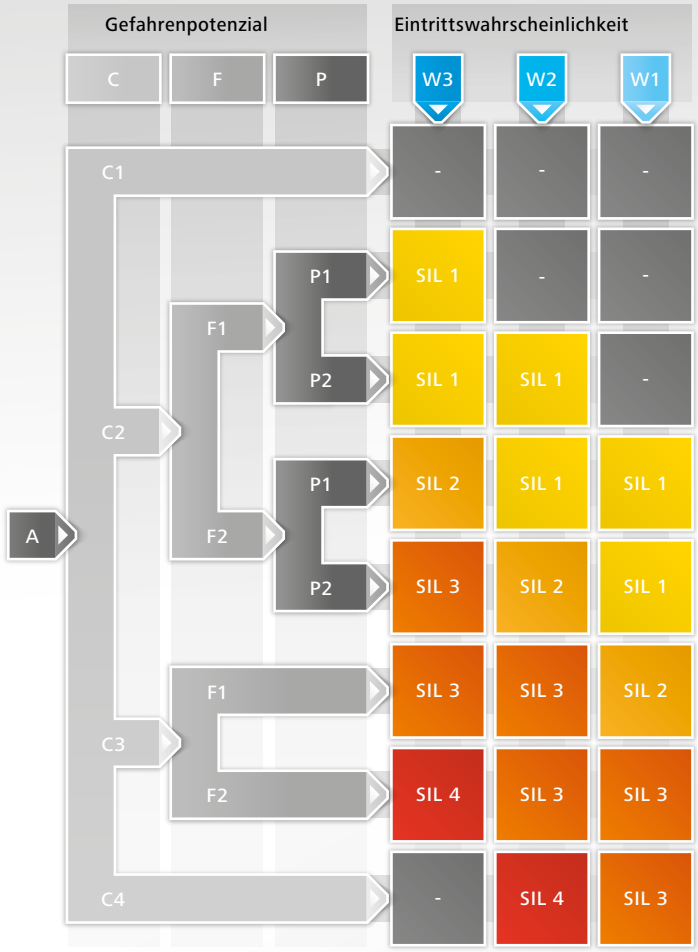
Um dies zu vereinfachen, lassen Gerätehersteller wie AUMA ihre Produkte auf ihre Eignung für die verschiedenen Sicherheits-Integritätslevel prüfen.

Vermeidung systematischer Fehler

Um Fehler zu vermeiden, die unter anderem bei Planung, Realisierung, Inbetriebnahme und Betrieb entstehen können – beispielsweise falsche Auslegung oder falsche Verkabelung –, müssen bestimmte fehlervermeidende Abläufe eingehalten und geeignete Maßnahmen ergriffen werden. Diese sind abhängig vom zu erreichenden SIL.

Überprüfung der SIL Anforderungen

Anhand von Sicherheitskennzahlen der eingesetzten Geräte sowie der dokumentierten fehlervermeidenden Maßnahmen wird für jede Sicherheitsfunktion überprüft, ob sie den geforderten SIL erreicht. Ist dies nicht der Fall, müssen zusätzliche Maßnahmen ergriffen werden.



Beispiel eines Risikographs für eine sicherheitstechnische Beurteilung nach IEC 61508/61511

A Ausgangspunkt für die Abschätzung der Risikominderung

C Schadensausmaß
C1 Leichte Verletzung einer Person oder kleinere schädliche Umwelteinflüsse
C2 Schwere irreversible Verletzungen oder Tod einer Person
C3 Tod mehrerer Personen
C4 Tod sehr vieler Personen

F Gefahrenabwendung
F1 Möglich unter bestimmten Bedingungen
F2 Kaum möglich

P Aufenthaltsdauer einer Person im gefährdeten Bereich
P1 Selten bis häufig
P2 Häufig bis dauernd

W Eintrittswahrscheinlichkeit
W3 Relativ Hoch
W2 Gering
W1 Sehr gering

SIL Geforderter Sicherheitsintegritätslevel
SIL 1 bis SIL 4 niedrigste Sicherheitsanforderung, höchste Sicherheitsanforderung

SICHERHEITSFUNKTION UND SICHERHEITSTECHNISCHES SYSTEM

WAS IST EINE SICHERHEITSFUNKTION?

Sicherheitsfunktionen (engl. Safety Instrumented Functions, SIF) sind Schutzmaßnahmen, die nur im Störfall aktiviert werden und dann verhindern, dass Personen, Umwelt und Sachwerte zu Schaden kommen. Funktionale Sicherheit wird erreicht, wenn Sicherheitsfunktionen in einer solchen Situation zuverlässig arbeiten.

Eine typische Sicherheitsfunktion ist zum Beispiel eine automatische Notabschaltung eines Prozesses.

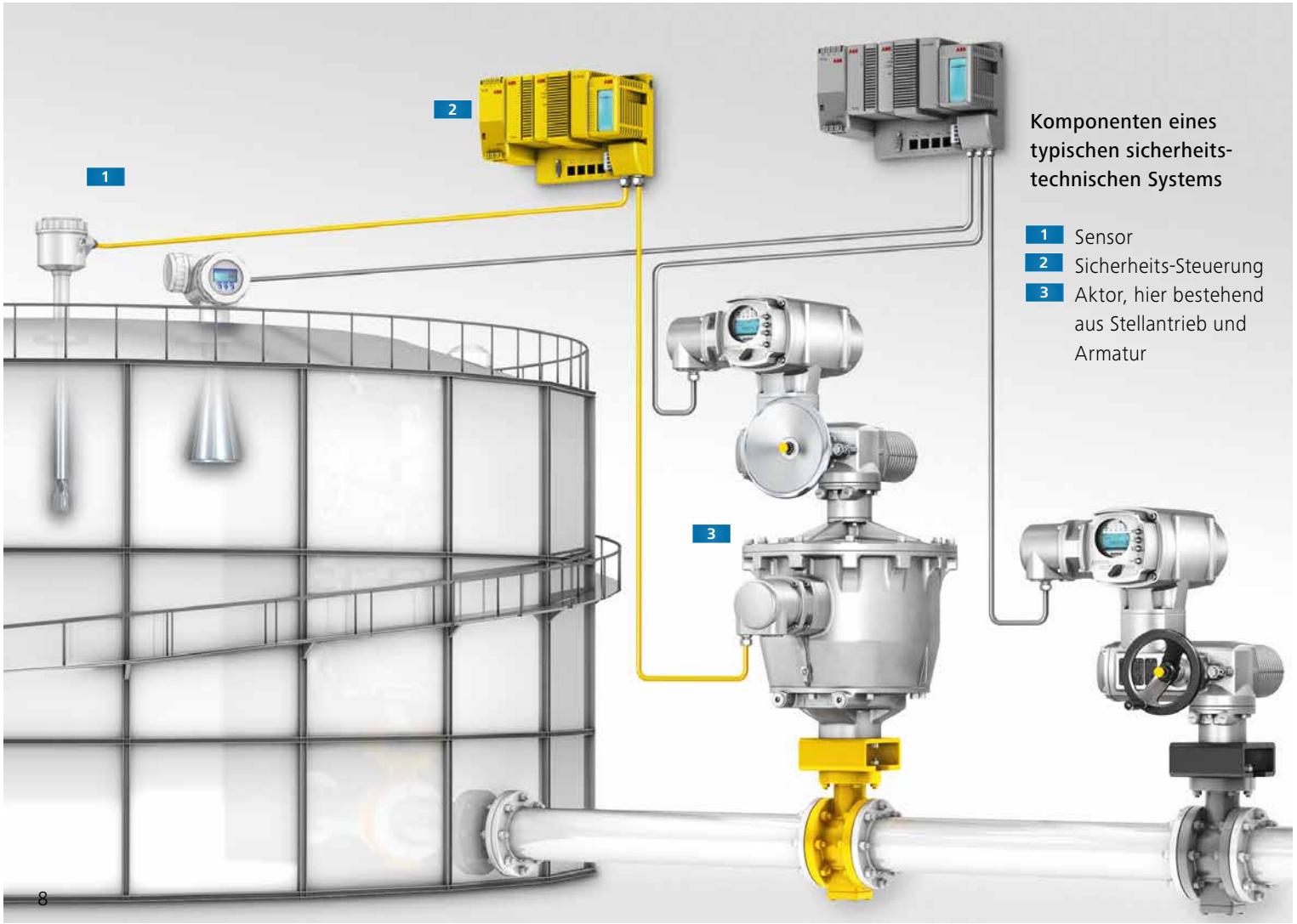
Im Armaturenbereich sind in erster Linie die folgenden Sicherheitsfunktionen von Bedeutung:

> Sicheres ÖFFNEN/Sicheres SCHLIESSEN (engl. Emergency Shutdown, ESD)
> Sicherer Stillstand/STOPP (engl. Safe Torque Off, STO)
> Sichere Endlagenrückmeldung

WAS IST EIN SICHERHEITSTECHNISCHES SYSTEM?

Eine Sicherheitsfunktion wird durch die Komponenten eines sogenannten sicherheitstechnischen Systems (engl. Safety Instrumented System, SIS) realisiert. Ein solches System besteht ganz allgemein aus den Bestandteilen Sensor, übergeordnete Sicherheits-Steuerung und Aktor. Im Armaturenbereich besteht der Aktor aus den Komponenten Stellantrieb und Armatur.

Bei der Beurteilung, ob eine Sicherheitsfunktion den geforderten SIL erreicht, müssen die systematische Eignung sowie die Sicherheitskennzahlen aller Einzelkomponenten des sicherheitstechnischen Systems berücksichtigt werden.



Komponenten eines typischen sicherheitstechnischen Systems

1 Sensor
2 Sicherheits-Steuerung
3 Aktor, hier bestehend aus Stellantrieb und Armatur

KRITERIEN FÜR DIE RISIKOREDUZIERUNG

Bei der Gefahrenbeurteilung eines Prozesses wird für jede Sicherheitsfunktion bestimmt, welchen SIL sie erfüllen muss. Die internationalen Normen IEC 61508 und IEC 61511 definieren drei Hauptkriterien, die die Sicherheitsfunktion bzw. das SIS erfüllen muss, um die geforderte Risikoreduzierung zu erfüllen:

> Systematische Eignung
> Erlaubte mittlere Ausfallwahrscheinlichkeit bei Anforderung
> Architektureinschränkungen

Diese Kriterien werden im folgenden erläutert.

SYSTEMATISCHE EIGNUNG

Die systematische Eignung (engl. systematic capability, SC) soll sicherstellen, dass eine Komponente für ein SIS mit einer bestimmten SIL-Anforderung prinzipiell geeignet ist. Die IEC 61508 definiert dazu unterschiedliche Methoden:

> Die erste Methode (Pfad 1_S in der Norm) verlangt, dass bestimmte Prozeduren während der Entwicklung, Herstellung, Wartung etc. eingehalten werden. Damit sollen systematische Fehler vermieden werden, wie zum Beispiel die falsche Dimensionierung oder Fehler im Design von Bauteilen. Diese Methode wird vor allem für neu zu entwickelnde Geräte eingesetzt.

> Die zweite Methode (Pfad 2_S) beruht auf der Auswertung von Felddaten, um eine Aussage über die Betriebsbewährung der Komponenten zu erhalten und die erforderliche Zuverlässigkeit nachzuweisen. Diese Methode wird vor allem für bereits länger existierende Gerätetypen verwendet, für die es bereits eine Vielzahl an Feldrücklaufdaten gibt.

Bei der Auswahl für ein SIS muss darauf geachtet werden, dass alle Komponenten die entsprechende systematische Eignung für den geforderten SIL des Gesamtsystems besitzen.

MITTLERE AUSFALLWAHRSCHEINLICHKEIT BEI ANFORDERUNG (PFD UND PFH)

Der PFD_{avg} Wert (Average Probability of Dangerous Failure on Demand) beschreibt die mittlere Wahrscheinlichkeit, dass die Sicherheitsfunktion bei Anforderung nicht ausgeführt werden kann. In der IEC 61508 ist für jeden der vier Sicherheits-Integritätslevel ein zulässiger Bereich für die Ausfallwahrscheinlichkeit festgelegt. SIL 1 stellt die niedrigste Sicherheitsstufe dar, SIL 4 die höchste. Je höher die Sicherheitsstufe, desto geringer darf die Wahrscheinlichkeit sein, dass die Sicherheitsfunktion bei Anforderung ausfällt.

Nicht nur die Größe des Schadensausmaßes im Störfall spielt eine Rolle, sondern auch die Häufigkeit, mit der ein Störfall erwartet und somit die entsprechende Sicherheitsfunktion angefordert wird. Die IEC 61508 unterscheidet dazu die Betriebsarten Low Demand, High Demand und Continuous Mode.

Low Demand Mode

Betriebsart mit niedriger Anforderungshäufigkeit, bei der die Sicherheitsfunktion nicht häufiger als einmal pro Jahr angefordert wird. Dies trifft typischerweise auf Sicherheitsfunktionen für die Prozessindustrie zu, die Stellantriebe einsetzen.

Betrachtet wird hierbei nur die Sicherheitsfunktion. Ein Antrieb, der sowohl für eine Sicherheitsfunktion als auch zum „normalen" Öffnen und Schließen eingesetzt wird, darf im Normalbetrieb durchaus häufiger eine Armatur öffnen und schließen. Ein Störfall in der Anlage, der das sichere Schließen der Armatur erfordert, darf jedoch nicht öfter als einmal pro Jahr erwartet werden.

Erlaubte PFD-Werte für Low Demand Mode

Sicherheits-Integritäts-level	Erlaubter PFD_{avg} Wert (Low Demand)	Theoretisch zulässige Ausfälle bei Anforderung der Sicherheitsfunktion
SIL 1	$\geq 10^{-2}$ bis $< 10^{-1}$	Ein gefährlicher Ausfall in 10 Jahren zulässig
SIL 2	$\geq 10^{-3}$ bis $< 10^{-2}$	Ein gefährlicher Ausfall in 100 Jahren zulässig
SIL 3	$\geq 10^{-4}$ bis $< 10^{-3}$	Ein gefährlicher Ausfall in 1 000 Jahren zulässig
SIL 4	$\geq 10^{-5}$ bis $< 10^{-4}$	Ein gefährlicher Ausfall in 10 000 Jahren zulässig

High Demand Mode und Continuous Mode

In der Betriebsart mit hoher Anforderungsrate (High Demand Mode) wird die Sicherheitsfunktion häufiger als einmal pro Jahr angefordert. In der Betriebsart mit kontinuierlicher Anforderung (Continuous Mode) arbeitet die Sicherheitsfunktion kontinuierlich.

Bei diesen beiden Betriebsarten wird als Maß für die Sicherheit die Ausfallwahrscheinlichkeit pro Stunde berechnet und als PFH-Wert angegeben (Probability of Failure per Hour).

Die PFD- und PFH-Werte werden zunächst für jede Komponente eines sicherheitstechnischen Systems einzeln berechnet. Ein Sicherheits-Integritätslevel beschreibt jedoch eine Eigenschaft einer gesamten Sicherheitsfunktion und nicht die einer Einzelkomponente. Daher muss aus den PFD- bzw. PFH-Werten der Einzelkomponenten der Gesamtwert für die Sicherheitsfunktion berechnet werden.

ARCHITEKTUREINSCHRÄNKUNGEN

Die Architektur eines SIS sollte so robust und fehlertolerant wie möglich sein. Grundsätzlich benennt die IEC 61508-2:2010 zwei zulässige Methoden, um das maximal erreichbare SIL auf Grund von Einschränkungen durch die Systemarchitektur (AC, architectural constraints) zu bestimmen:

> Pfad 1_H in der IEC 61508 beruht auf einer Einstufung nach einem Mindestwert für den Anteil sicherer Fehler (engl. safe failure fraction, SFF) in Kombination mit ausreichender Redundanz in der Systemarchitektur auf Basis der Hardwarefehlertoleranz (engl. hardware fault tolerance, HFT).

> Die zweite Methode, Pfad 2_H, ermöglicht eine vereinfachte Einstufung rein auf Grund der HFT. Hier sind jedoch weitere Bedingungen zu erfüllen, zum Beispiel ist auch umfangreiche Felderfahrung bei den eingesetzten Bauteilen erforderlich.

Die Anforderungen an die Architektur müssen auf Elementebene erfüllt sein. Beim Aktor (engl. final element) bestehend aus Stellantrieb und Armatur hat es sich als sinnvoll erwiesen, diesen insgesamt als ein Element zu betrachten.

Anteil Sicherer Fehler (SFF)

Der SFF-Wert (Safe Failure Fraction) beschreibt den prozentualen Anteil sicherer und erkannter gefahrbringender Ausfälle an der Gesamtfehlerzahl. Fehler sind sicher, wenn ihr Auftreten das System in einen sicheren Zustand bringt oder dort hält.

Je höher dieser Wert ist, desto geringer ist die Wahrscheinlichkeit eines gefährlichen Systemausfalls.

Hardwarefehlertoleranz (HFT)

Die HFT (Hardware Fault Tolerance) ist die Fähigkeit einer Funktionseinheit, eine geforderte Sicherheitsfunktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen.

Eine Hardwarefehlertoleranz von N bedeutet, dass N + 1 Fehler zu einem Ausfall der Sicherheitsfunktion führen können. Ist die Hardwarefehlertoleranz zum Beispiel Null, kann bereits ein Fehler zu einem Ausfall der Sicherheitsfunktion führen.

Die HFT lässt sich in der Regel durch einen redundanten Systemaufbau erhöhen (siehe auch Seite 13).

Gerätetyp
Die IEC 61508 unterscheidet zwischen einfachen und komplexen Geräten.

> Einfache Geräte – Typ A
  Typ A Geräte sind „einfache" Geräte, bei denen das Ausfallverhalten der Bauteile vollständig bekannt ist. Sie enthalten z.B. Relais, Widerstände und Transistoren, jedoch keine komplexen elektronischen Bauelemente wie z.B. Mikrocontroller.
> Komplexe Geräte – Typ B
  Typ B Geräte sind „komplexe" Geräte, die elektronische Bauelemente wie Mikrocontroller, Mikroprozessoren und ASICs enthalten. Bei diesen Bauelementen und insbesondere bei softwaregesteuerten Funktionen ist es schwierig, alle Fehlermöglichkeiten vollständig zu bestimmen.

Je komplexer die Geräte desto höher die Anforderungen
Wie aus den folgenden beiden Tabellen ersichtlich wird, gelten für Typ B Geräte deutlich höhere Anforderungen als für Typ A Geräte.

SFF und HFT für Typ A Geräte (Pfad 1_H)

	HFT (Hardwarefehlertoleranz)		
SFF (Anteil Sicherer Fehler)	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % bis < 90 %	SIL 2	SIL 3	SIL 4
90 % bis < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

SFF und HFT für Typ B Geräte (Pfad 1_H)

	HFT (Hardwarefehlertoleranz)		
SFF (Anteil Sicherer Fehler)	0	1	2
< 60 %	nicht erlaubt	SIL 1	SIL 2
60 % bis < 90 %	SIL 1	SIL 2	SIL 3
90 % bis < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Die folgenden Kennzahlen werden für die Beurteilung der verschiedenen Kriterien zur Risikoreduzierung benötigt:

AUSFALLRATEN

Für die Sicherheit eines Systems ist die Analyse möglicher Fehlerquellen von entscheidender Bedeutung. Die Betrachtung der Ausfallraten Lambda bildet dabei die Grundlage der Berechnung der weiteren Sicherheitskennzahlen. Bei der Betrachtung der Ausfallraten λ wird unterschieden, welche Fehler gefährlich und welche ungefährlich sind, also keinen Einfluss auf das korrekte Ausführen der Sicherheitsfunktion haben. Zudem wird untersucht, ob Fehler diagnostiziert werden können.

Anzahl der sicheren Ausfälle pro Zeiteinheit (Lambda Safe λ_{safe})
Ein Ausfall gilt als sicher, wenn durch ihn die Sicherheitsfunktion ausgelöst und durchgeführt wird. Die Einheit Failure in Time (FIT) gibt dabei die Anzahl der Ausfälle an, die in 10^9 Stunden auftreten: 1 FIT heißt ein Ausfall pro 10^9 Stunden beziehungsweise ein Ausfall pro 114.000 Jahre.

Anzahl der entdeckten gefährlichen Ausfälle pro Zeiteinheit (Lambda Dangerous Detected, λ_{DD})
Ein Ausfall einer Komponente wird als gefährlich eingestuft, wenn dadurch möglicherweise eine Sicherheitsfunktion nicht ausgeführt werden kann. Angegeben wird die Anzahl der durch Diagnosetests erkannten gefährlichen Ausfälle pro 10^9 Stunden.

Anzahl der unentdeckten gefährlichen Ausfälle pro Zeiteinheit (Lambda Dangerous Undetected, λ_{DU})
Angegeben wird die Anzahl der nicht erkannten gefährlichen Ausfälle pro 10^9 Stunden.

Diagnosedeckungsgrad gefährlicher Fehler (Diagnostic Coverage of Dangerous Failures, DC_D)
Anteil der durch Maßnahmen zur Fehlerdiagnose erkannten Rate gefahrbringender Ausfälle λ_{DD} an der Gesamtrate der gefahrbringenden Ausfälle in Prozent.

INTERVALL FÜR WIEDERHOLUNGSPRÜFUNGEN (T_{PROOF})

Die Sicherheitsfunktion muss in regelmäßigen, vom Betreiber festgelegten Intervallen durch eine Wiederholungsprüfung (Proof Test) auf Ihre Funktionsfähigkeit getestet werden. Dies ist notwendig, um sowohl systematische als auch zufällige Fehler, die bisher nicht bemerkt wurden, zu erkennen und zu beseitigen.

Der PFD-Wert lässt sich verbessern, indem die Zeit zwischen zwei Wiederholungsprüfungen verkürzt wird.

ERMITTLUNG DER SIL-FÄHIGKEIT

Entscheidend für die Sicherheit einer Sicherheitsfunktion ist immer die SIL-Fähigkkeit des gesamten sicherheitstechnischen Systems mit allen Komponenten.

SIL-FÄHIGKEIT EINER SICHERHEITSFUNKTION

Bei der Bewertung und Einstufung der Sicherheitsfunktion sind gemäß IEC 61508 ist es entscheidend, alle drei Hauptkriterien Systematische Eignung, Ausfallwahrscheinlichkeit bei Anforderung und Architektureinschränkungen zu berücksichtigen. Dabei müssen jeweils die Werte für die einzelnen Komponenten des SIS berücksichtigt werden.

Es ist unbedingt zu beachten, dass das erreichbare SIL immer das niedrigste der bei den drei Einzelbewertungen erreichten SIL ist:

Bewertung einer Sicherheitsfunktion

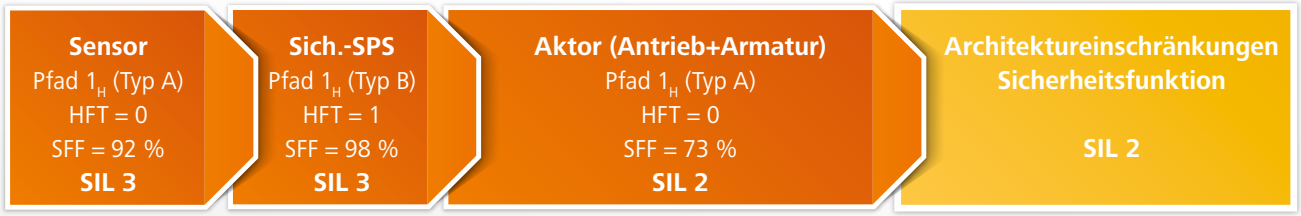
Einstufung der SIF bezogen auf	Maximal erreichbares SIL
Systematische Eignung	SIL 2 (SC = 2)
Ausfallwahrscheinlichkeit bei Anforderung	SIL 1
Architektureinschränkungen	SIL 2
Gesamtbewertung der Sicherheitsfunktion	**SIL 1**

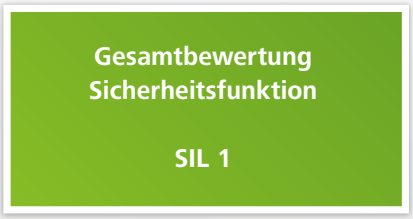
Beispiel für die Ermittlung des maximal erreichbaren SIL einer Sicherheitsfunktion (bei einkanaligem Systemaufbau)

Bewertung der Systematischen Eignung (SC) einer Sicherheitsfunktion

Berechnung des Gesamt-PFD-Wertes einer Sicherheitsfunktion

Berechnung der Architektureinschränkungen





VERBESSERUNG DER SIL-FÄHIGKEIT

Zeigt die Bewertung, dass mit den ausgewählten Hardwarekomponenten der geforderte SIL nicht erreicht wird, lässt sich die SIL-Fähigkeit durch Maßnahmen wie zusätzliche Diagnose oder Redundanz verbessern.

PARTIAL VALVE STROKE TEST (PVST)

Mit Hilfe des Partial Valve Stroke Tests wird in regelmäßigen Abständen die Funktion des Gerätes geprüft. Der Antrieb bzw. die Armatur fährt einen definierten Weg vor und wieder zurück. Damit wird geprüft, ob sich der Antrieb tatsächlich bewegt.

Der PVST ist eine anerkannte Methode, die Verfügbarkeit von Einzelkomponenten einer Sicherheitsfunktion zu erhöhen. Durch die vorbeugende Diagnose lassen sich einige sicherheitsrelevante Fehler entdecken, bevor sie die Ausführung einer Sicherheitsfunktion verhindern oder beeinträchtigen können; die Ausfallwahrscheinlichkeit im Anforderungsfall nimmt ab.

WIEDERHOLUNGSPRÜFUNG (PROOF TEST)

Hier handelt es sich um eine umfangreiche Systemüberprüfung. Wird das Intervall zwischen zwei Wiederholungsprüfungen von zum Beispiel zwei Jahren auf ein Jahr verkürzt, kann sich die SIL-Fähigkeit möglicherweise verbessern, da unerkannte Fehler schneller aufgedeckt werden können.

REDUNDANZ

Auch mit einem redundanten Systemaufbau lässt sich die Wahrscheinlichkeit erhöhen, dass eine Sicherheitsfunktion im Notfall ausgeführt werden kann. Dabei werden zwei oder mehr Geräte eines sicherheitstechnischen Systems redundant betrieben.

Je nach Sicherheitsanforderung sind verschiedene MooN („M out of N“) Konfigurationen sinnvoll. Bei einer 1oo2 („one out of two“) Konfiguration genügt zum Beispiel eines von zwei Geräten, um die Sicherheitsfunktion auszuführen. Bei einer 2oo3 („two out of three“) Konfiguration müssen zwei von drei Geräten korrekt arbeiten.

Ein redundanter Systemaufbau kann die Hardwarefehlertoleranz (HFT) und damit auch die SIL-Fähigkeit erhöhen. Für SIL 3 Anwendungen nach der IEC 61511 wird in der Regel ein redundanter Systemaufbau verwendet, zum Beispiel 1oo2.

Wie die konkrete Anordnung der Geräte aussieht, hängt jedoch auch von der geforderten Sicherheitsfunktion ab. Deshalb muss grundsätzlich anhand der Gesamtsicherheitsfunktion auf Systemebene geprüft werden, ob ein Aufbau mit mehreren Stellantrieben in der geplanten Konfiguration tatsächlich zu einer HFT > 0 führt.

Redundantes System für Sicheres ÖFFNEN

Redundantes System für Sicheres SCHLIESSEN

AUMA PRODUKTE MIT SIL-KLASSIFIZIERUNG

Für Anlagenplaner und Anlagenbetreiber ist es von zentraler Bedeutung, ausschließlich Komponenten einzusetzen, die die jeweiligen Sicherheitsanforderungen erfüllen.

AUMA bietet ein breites Portfolio an Produkten, die für unterschiedliche SIL-Anforderungen geeignet sind. Um unsere Kunden bei der Auswahl zu unterstützen, haben wir die Sicherheitskennzahlen und die SIL-Fähigkeit für ausgewählte AUMA Stellantriebe, Stellantriebs-Steuerungen und Getriebe ermittelt.

AUMA PRODUKTE IN AUSFÜHRUNG SIL

Die hier aufgeführten Produkte sind für höchste Sicherheitsanforderungen geeignet. Es handelt sich um Neuentwicklungen, bei denen eine vollständige Bewertung gemäß IEC 61508 durchgeführt wurde (sh. Seite 26).

STELLANTRIEBE SA UND SQ MIT INTEGRIERTER STEUERUNG AC .2 IN AUSFÜHRUNG SIL

Die integrierten Stellantriebs-Steuerungen AC .2 und ACExC .2 in Ausführung SIL enthalten ein zusätzliches SIL-Modul, das speziell für die Ausführung der Sicherheitsfunktionen entwickelt wurde. Stellantriebe mit dieser Steuerung sind SIL 2-fähig. SIL 3 lässt sich durch redundanten Systemaufbau erreichen. Die Zertifizierung wurde vom TÜV Nord durchgeführt.

Sicherheitsfunktionen:

> Sicheres ÖFFNEN/Sicheres SCHLIESSEN
> Sicherer STOPP
> Sichere Endlagenrückmeldung[1)]

Ausführliche Informationen finden Sie auf den Seiten 18 bis 21.

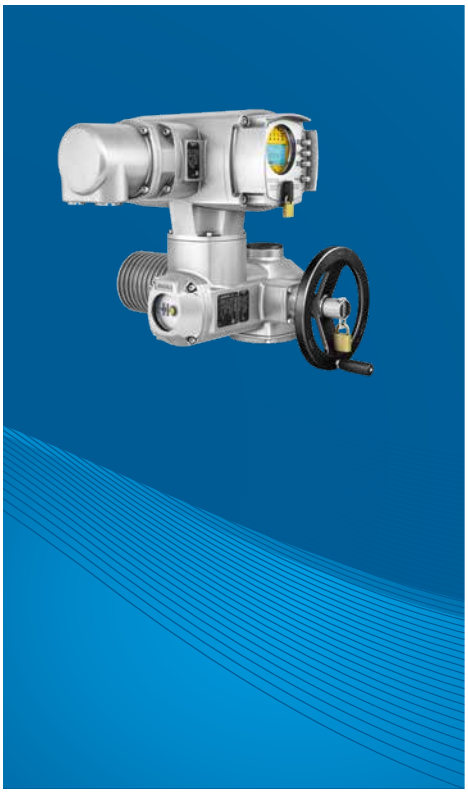
FAIL-SAFE-EINHEIT FQM IN AUSFÜHRUNG SIL

Mit der Fail-Safe-Einheit FQM bietet AUMA eine innovative und sichere Antriebslösung, um Armaturen im Notfall auch ohne elektrischen Strom zu betätigen. Sie ist für sicherheitsbezogene Anwendungen bis SIL 2 geeignet. SIL 3 lässt sich durch redundanten Systemaufbau erreichen. Die Zertifizierung wurde von exida durchgeführt.

Sicherheitsfunktionen:

> Sicheres ÖFFNEN/Sicheres SCHLIESSEN
> Sichere Endlagenrückmeldung

Ausführliche Informationen finden Sie auf den Seiten 22f.



1 Die Sichere Endlagenrückmeldung ist für diese Produkte nicht Bestandteil des Zertifikats; stattdessen ist eine Herstellererklärung erhältlich.

AUMA PRODUKTE IN AUSFÜHRUNG SFC

Mit den Stellantrieben, Steuerungen und Getrieben in Ausführung SFC (Safety Figures Calculated) stellt AUMA ein breites Produktportfolio für mittlere bis niedrige Sicherheitsanforderungen zur Verfügung. AUMA hat in Zusammenarbeit mit exida die Sicherheitskennzahlen im Rahmen einer Hardwarebeurteilung basierend auf Felderfahrung und/oder generischen Daten bestimmt. Für diese Produkte ist eine Herstellererklärung erhältlich. Die Produkte bieten eine höhere Flexibilität bezüglich Konfigurationsmöglichkeiten und Investitionskosten.

STELLANTRIEBE SA UND SQ OHNE INTEGRIERTE STEUERUNG IN AUSFÜHRUNG SFC

Die Stellantriebe SA und SQ für sich genommen, ohne integrierte Steuerung, sind in den betrachteten Sicherheitsfunktionen bis zu SIL 2-fähig.

Sicherheitsfunktionen:

> Sicheres Fahren in Richtung AUF/ZU
> Sicherer Stillstand
> Sichere Endlagenrückmeldung

Bei diesen Ausführungen müssen die steuerungstechnischen Funktionen vom Kunden zur Verfügung gestellt werden.

STELLANTRIEBE SA UND SQ MIT INTEGRIERTER STEUERUNG AM UND AC .2 IN AUSFÜHRUNG SFC

Die Stellantriebe mit integrierter Steuerung AM .1 und AC .2 in Ausführung SFC sind in den betrachteten Ausführungen bis zu SIL 2-fähig.

Sicherheitsfunktionen:

> Sichere Endlagenrückmeldung

GETRIEBE GK UND GS .3 IN AUSFÜHRUNG SFC

Für die AUMA Getriebe GK und GS .3 wurden ebenfalls die Sicherheitskennzahlen bestimmt. Die betrachteten Getriebe sind bis zu SIL 2-fähig.

Sicherheitsfunktionen:

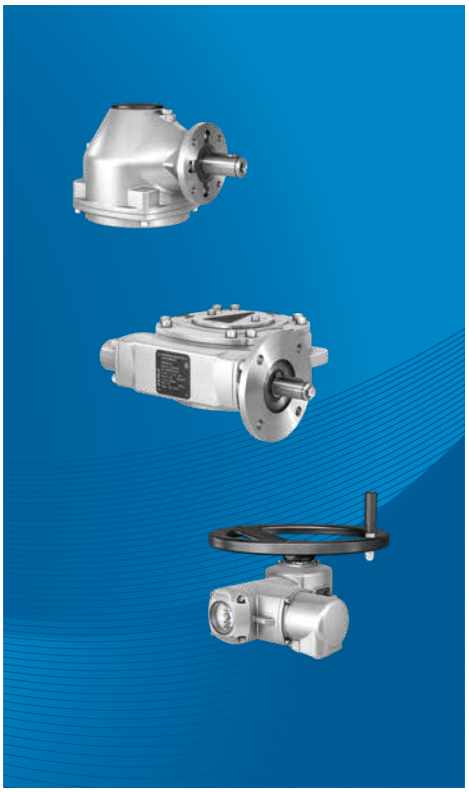
> Sicheres Fahren in Richtung AUF/ZU

WEGSCHALTUNG WSH IN AUSFÜHRUNG SFC

Handgetriebe mit elektromechanischer Steuereinheit WSH sind SIL 1-fähig.

Sicherheitsfunktionen:

> Sichere Endlagenrückmeldung



BEURTEILTE SICHERHEITSFUNKTIONEN

Die Sicherheitskennzahlen und damit auch die SIL-Fähigkeit sind abhängig von der Sicherheitsfunktion, die das Gerät im Notfall ausführt, um die Anlage in einen sicheren Zustand zu bringen.

AUMA Stellantriebe sind für die folgenden Sicherheitsfunktionen geeignet:

Sicheres ÖFFNEN/Sicheres SCHLIESSEN
(engl. Emergency Shutdown, ESD)
Hier fährt der Antrieb bei Anforderung der Sicherheitsfunktion in Richtung Endlage AUF oder Endlage ZU.

Diese Sicherheitsfunktionen werden in der Regel mit einem Partial Valve Stroke Test (PVST) als zusätzliche Diagnosemaßnahme kombiniert.

Sicherer Stillstand/Sicherer STOPP
(engl. Safe Torque Off, STO)
Der Motor des Antriebs wird bei Anforderung der Sicherheitsfunktion stromfrei geschaltet. Ein unerwünschtes Anfahren des Motors aus dem Stillstand wird verhindert.

Sicheres Fahren in Richtung AUF/ZU
Diese Sicherheitsfunktion wird von Stellantrieben ohne integrierte Steuerung und von Getrieben ausgeführt. Der Stellantrieb fährt bei Anforderung in die entsprechende Richtung. Über die Armaturenposition wird hier keine Aussage getroffen.

Sichere Endlagenrückmeldung
Bei dieser Sicherheitsfunktion wird der Stellantrieb als „Sensor“ im SIS eingesetzt. Er gibt über die elektromechanische Steuereinheit eine sichere Meldung aus, sobald eine der Endlagen AUF oder ZU oder das Abschaltdrehmoment erreicht ist.

ANWENDUNGSBEISPIELE FÜR SICHERHEITSFUNKTIONEN

Sicheres SCHLIESSEN
am Beispiel einer Überfüllsicherung für Öltanks
In Tanklagern sind häufig die normalen Systeme zum Befüllen der Tanks durch zusätzliche Sicherheitssysteme abgesichert, die ein Überlaufen verhindern sollen. Eine Sicherheits-SPS überwacht kontinuierlich über separate Sensoren den Füllstand im Tank. Wird ein Grenzwert überschritten, übermittelt die Sicherheits-SPS ein Emergency Shutdown Signal an den Stellantrieb des SIS und die Armatur wird geschlossen.

Sichere Endlagenrückmeldung und Sicherer STOPP
am Beispiel einer Schleuse
Am Beispiel einer Schleuse lassen sich verschiedene Sicherheitsfunktionen veranschaulichen:

Zum Beispiel sollte sichergestellt sein, dass die Schleusentore auf der einen Seite vollständig geschlossen sind, bevor die andere Seite geöffnet wird. Dies kann über einen Stellantrieb mit sicherer Endlagenrückmeldung in Kombination mit einer Sicherer STOPP Funktion als Verriegelungsfunktion realisiert werden. Die Verriegelungsfunktion stellt sicher, dass eine Bewegung des Schleusentors nur dann erfolgen kann, wenn das Signal „Sicherer STOPP“ nicht anliegt.

Befindet sich ein Schiff zwischen den geöffneten Schleusentoren, kann mit der Sicherheitsfunktion Sicherer STOPP das Schließen der Schleuse zuverlässig angehalten werden.

ÜBERSICHT AUMA PRODUKTE MIT SIL-KLASSIFIZIERUNG

Für alle SIL-klassifizierten AUMA Produkte können Sie die Herstellererklärungen bzw. Prüfberichte direkt bei AUMA anfordern.

Antrieb / Getriebe	Stellantriebs-Steuerung	Aus-führung	Sicherheitsfunktion	Maximal mögliche Sicherheitsanforderung		
				bei HFT[1]	gemäß IEC 61508	gemäß ISO 13849
FQM 05.1 SIL – FQM 12.1 SIL mit SQ 05.2 – SQ 12.2 FQMEx 05.1 SIL – FQMEx 12.1 SIL mit SQEx 05.2 – SQEx 12.2	AC 01.2 (Standard) ACExC 01.2 (Standard)	SIL	Sicheres ÖFFNEN/SCHLIESSEN (ESD) (ohne externe Stromversorgung)	HFT = 0 HFT = 1	SIL 2 (mit PVST) SIL 3 (mit PVST)	
			Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d/e (mit 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	Sicheres ÖFFNEN/SCHLIESSEN (ESD)	HFT = 0 HFT = 1	SIL 2 (mit PVST) SIL 3 (mit PVST)	
			Sicherer STOPP	HFT = 0 HFT = 1	SIL 2 SIL 3	
			Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)[3]	PL c (mit PVST)[3] PL d/e (mit PVST)[2] [3]
	ohne Steuerung	SFC	Sicheres Fahren in Richtung AUF/ZU	HFT = 0	SIL 2 (mit PVST)	
			Sicherer Stillstand	HFT = 0	SIL 2	
			Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d/e (mit PVST)[2]
	AM 01.1/02.1 AMExC 01.1 AMExB 01.1	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d/e (mit PVST)[2]
	AC 01.2 (Standard) ACExC 01.2 (Standard)	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d/e (mit 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	Sicheres ÖFFNEN/SCHLIESSEN (ESD)	HFT = 0 HFT = 1	SIL 2 (mit PVST) SIL 3 (mit PVST)	
			Sicherer STOPP	HFT = 0 HFT = 1	SIL 2 SIL 3	
			Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (SIL 1 für SQ 14.2)(mit PVST)[3]	PL c (mit PVST)[3] PL d/e (mit PVST)[2] [3]
	ohne Steuerung	SFC	Sicheres Fahren in Richtung AUF/ZU	HFT = 0	SIL 2 (mit PVST)	
			Sicherer Stillstand	HFT = 0	SIL 2	
			Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (SIL 1 für SQ 14.2) (mit PVST)	PL c (mit PVST) PL d/e (mit PVST)[2]
	AM 01.1/02.1 AMExC 01.1	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (SIL 1 für SQ 14.2) (mit PVST)	PL c (mit PVST) PL d/e (mit PVST)[2]
	AC 01.2 (Standard) ACExC 01.2 (Standard)	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (SIL 1 für SQ 14.2) (mit PVST)	PL c (mit PVST) PL d/e (mit 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	ohne Steuerung	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d (mit PVST)[2]
	AM 01.1/02.1 AMExC 01.1 AMExB 01.1	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d (mit PVST)[2]
	AC 01.2 (Standard) ACExC 01.2 (Standard)	SFC	Sichere Endlagenrückmeldung	HFT = 0 HFT = 1	SIL 2 (mit PVST)	PL c (mit PVST) PL d (mit PVST)[2]
GK 10.2 – GK 40.2	nicht relevant	SFC	Sicheres Fahren in Richtung AUF/ZU	HFT = 0	SIL 2 (mit PVST)	
GS 50.3 – 250.3	nicht relevant	SFC	Sicheres Fahren in Richtung AUF/ZU	HFT = 0	SIL 2 (mit PVST)	
WSH 10.2 – WSH 16.2 WSHEx 10.2 – WSHEx 16.2	nicht relevant	SFC	Sichere Endlagenrückmeldung	HFT = 0	SIL 1	PL c

1 Hardwarefehlertoleranz.
HFT = 0 wird beispielsweise durch ein einkanaliges System „1oo1" („one out of one") erreicht.
HFT = 1 kann beispielsweise durch ein redundantes System „1oo2" („one out of two") erreicht werden. Es muss jedoch grundsätzlich auf Systemebene geprüft werden, ob durch Verwendung mehrerer Antriebe tatsächlich eine HFT > 0 erreicht wird.

2 Unter Berücksichtigung weiterer Anforderungen, insbesondere Redundanz und Überwachung auf Systemebene (welcher PL erreicht wird, muss auf Systemebene beurteilt werden)

3 Herstellererklärung in Zusammenarbeit mit exida, nicht Bestandteil des Zertifikats

INTEGRIERTE STELLANTRIEBS-STEUERUNG AC .2 IN AUSFÜHRUNG SIL

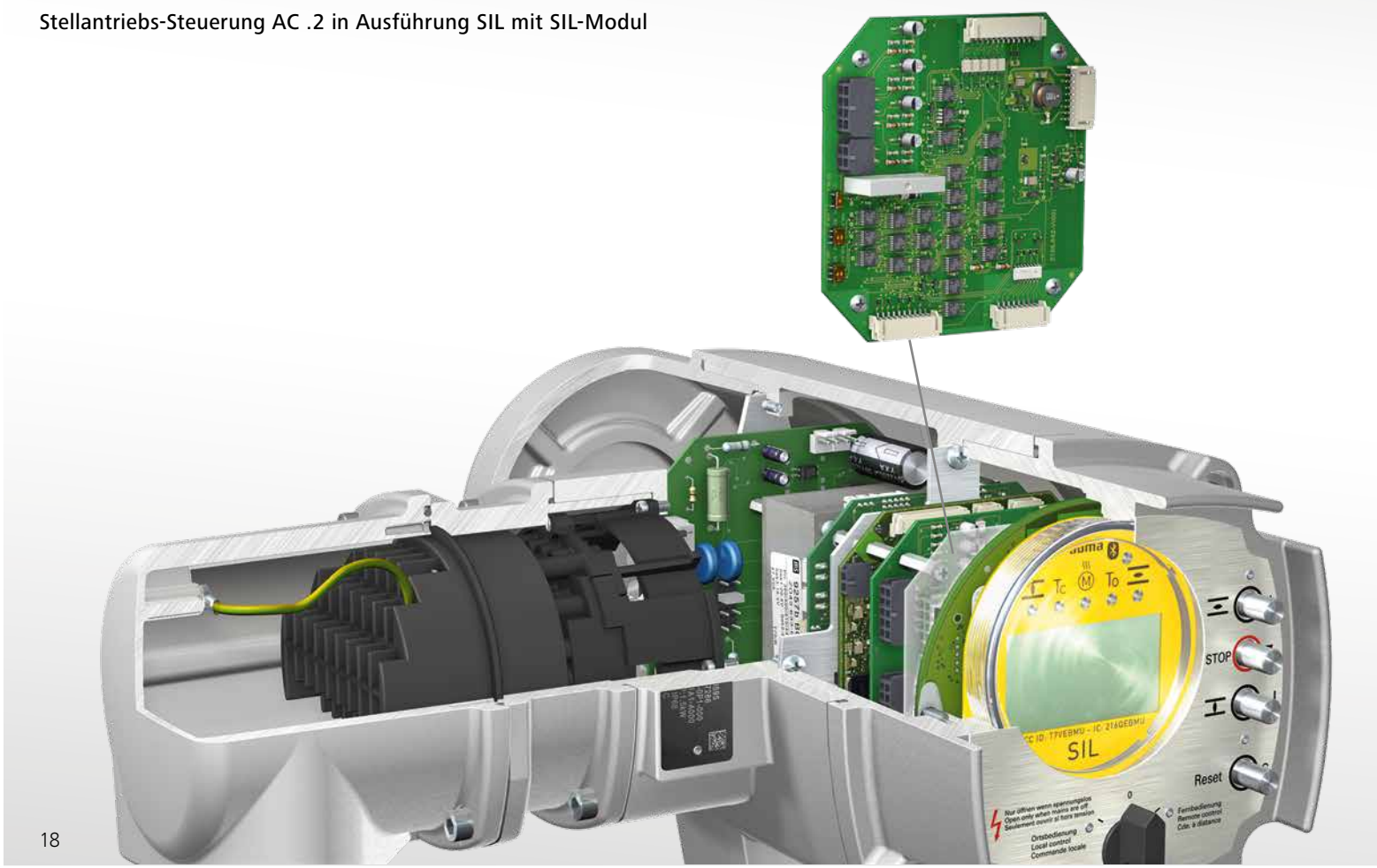
Mit der integrierten Stellantriebs-Steuerung AC .2 in Ausführung SIL bietet AUMA eine moderne Steuerung für sicherheitsbezogene Systeme bis SIL 3. Sicherheitsfunktionen werden ausschließlich über das sichere SIL-Modul ausgeführt. Im Normalbetrieb steht der volle Funktionsumfang der AC .2 zur Verfügung.

TÜV ZERTIFIKAT FÜR SIL 2/SIL 3 ANWENDUNGEN

Wer die integrierte Stellantriebs-Steuerung AC .2 kennt, schätzt ihre Vielfalt an Funktionen und Einstellmöglichkeiten. Mit ihren frei konfigurierbaren parallelen und Feldbusschnittstellen lässt sie sich problemlos in moderne Leitsysteme einbinden. Die AC .2 ist die ideale Steuerung für komplexe Steuer- und Regelfunktionen. Zusätzliche Diagnosefunktionen wie Betriebsdatenerfassung und Überwachung von Lebensdauerfaktoren erhöhen zudem Sicherheit und Verfügbarkeit des Antriebs.

Dank des von AUMA entwickelten SIL-Moduls sind diese Funktionen auch für SIL 2- und SIL 3-Anwendungen nutzbar. Stellantriebe SA und SQ mit AC .2 in Ausführung SIL sind durch den TÜV Nord zertifiziert und für sicherheitsbezogene Systeme bis SIL 3 zugelassen (SC = 3, SIL 3 in redundanter Ausführung 1oo2/HFT = 1).

Stellantriebs-Steuerung AC .2 in Ausführung SIL mit SIL-Modul



DAS SIL-MODUL

Beim SIL-Modul handelt es sich um eine zusätzliche Platine, die für die Ausführung von Sicherheitsfunktionen zuständig ist. Diese Platine wird zusätzlich zur Standardlogik in den integrierten Stellantriebs-Steuerungen AC .2 und ACExC .2 eingesetzt.

Auf dem SIL-Modul werden nur vergleichsweise einfache Bauelemente wie Transistoren, Widerstände und Kondensatoren eingesetzt, deren Ausfallarten vollständig bekannt sind. Deshalb gilt die AC .2 in Ausführung SIL als einfaches Typ A Gerät. Die ermittelten Sicherheitskennzahlen erlauben den Einsatz in SIL 2- und, in redundanter Ausführung (1oo2), in SIL 3-Anwendungen (SC = 3).

VORRANG FÜR DIE SICHERHEITSFUNKTION

Kommt es zu einem Notfall und wird eine Sicherheitsfunktion angefordert, während Funktionen über die Standardlogik ausgeführt werden, so wird die Standardlogik der AC .2 durch eine Bypass-Schaltung umgangen und die Sicherheitsfunktion über das SIL-Modul ausgeführt. Die Sicherheitsfunktionen haben damit immer Vorrang vor dem Normalbetrieb.

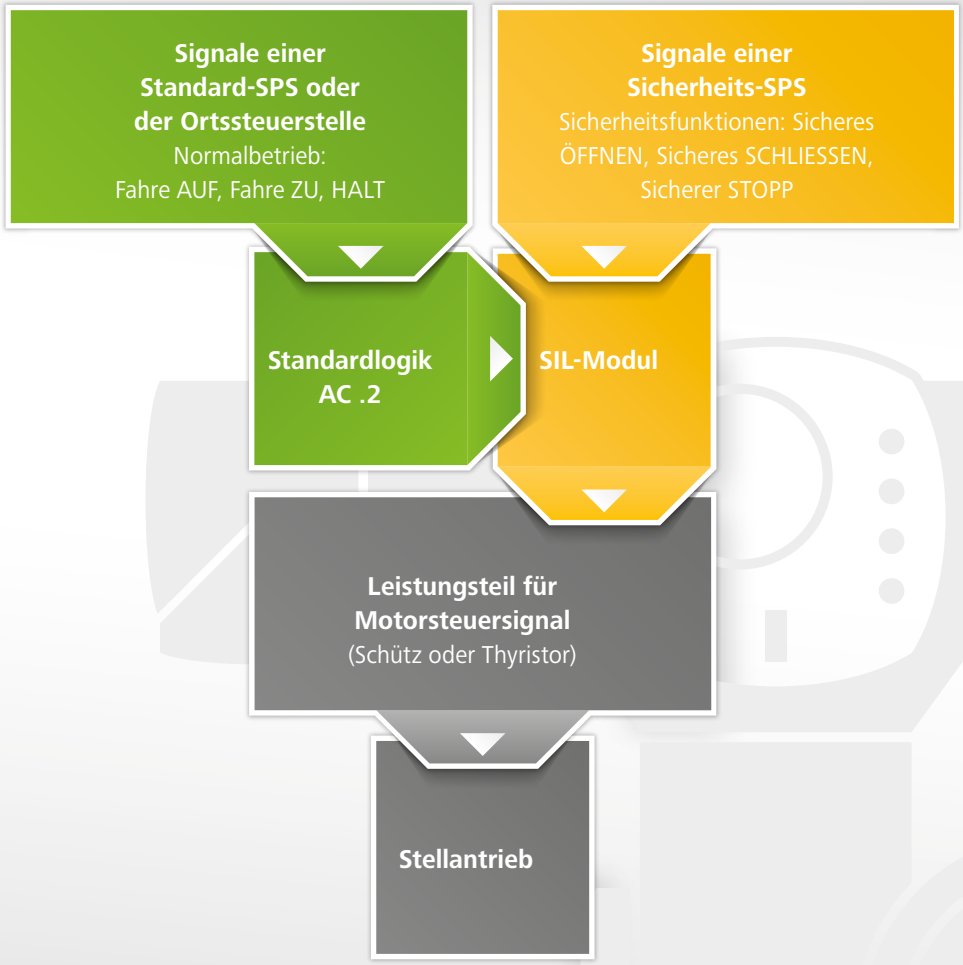
TYPISCHER SYSTEMAUFBAU

Stellantriebe mit integrierter Steuerung AC .2 in Ausführung SIL bieten verschiedene Möglichkeiten beim Systemaufbau:

Physikalisch getrenntes SIS
Im Normalfall wird ein SIS vollständig physikalisch getrennt von der normalen Prozesssteuerung aufgebaut. Dies bedeutet, dass ein Stellantrieb mit AC .2 in Ausführung SIL ausschließlich für die Ausführung der Sicherheitsfunktion vorgesehen wird. Ein zweiter Stellantrieb in Standardausführung übernimmt die Armaturenbetätigung im Normalbetrieb.

Kombination von SIS und Normalbetrieb
Grundsätzlich kann ein Stellantrieb mit integrierter Steuerung AC .2 in Ausführung SIL sowohl für die Ausführung der Sicherheitsfunktion als auch für die Prozesssteuerung im Normalbetrieb verwendet werden: Die AC .2 wird dann über zwei übergeordnete Steuerungen (SPS) angesteuert, eine Standard-SPS und eine Sicherheits-SPS, also eine SIL-zugelassene SPS.

Für diesen Einsatzfall definiert die IEC 61511 jedoch zusätzliche Bedingungen, die bei Konzeption und Integration beachtet werden müssen.



Vorrang für die Sicherheitsfunktion
Der Signalweg in der AC .2 in Ausführung SIL verläuft auch im Normalbetrieb, d.h. bei einem Fahrbefehl oder einem anderen Signal von einer Standard-SPS oder von der Ortssteuerstelle, immer über das SIL-Modul. Wird eine Sicherheitsfunktion über eine Sicherheits-SPS angefordert, sorgt das SIL-Modul dafür, dass diese unverzüglich und prioritär ausgeführt wird.

KONFIGURATIONSMÖGLICHKEITEN

Die AC .2 in Ausführung SIL zeichnet sich durch eine Vielfalt an Konfigurationsmöglichkeiten aus. Im Werk wird bereits entsprechend der Kundenwünsche voreingestellt, welche Sicherheitsfunktion ausgeführt und wann eine Abschaltung der Fahrt erfolgen soll. Diese Einstellung erfolgt über DIP-Schalter auf dem SIL-Modul.

Sicherheitsfunktionen
Die folgenden Sicherheitsfunktionen können mit Hilfe der AC .2 in Ausführung SIL realisiert werden:

> Sicheres ÖFFNEN/SCHLIESSEN
(Safe ESD, Emergency Shut Down)
Der Stellantrieb fährt in die konfigurierte Endlage AUF bzw. ZU. Für zusätzliche Sicherheit ist der Signaleingang redundant ausgeführt.

> Sicherer STOPP (Safe STOP)
Bei dieser Sicherheitsfunktion wird ein Fahrbefehl der Standard-SPS in Richtung AUF oder ZU nur dann ausgeführt, wenn ein zusätzliches Freigabesignal des SIL-Moduls anliegt.
Falls das Freigabesignal fehlt, wird eine Fahrt in Richtung AUF bzw. ZU gestoppt oder erst gar nicht gestartet.

> Sicheres ÖFFNEN/SCHLIESSEN kombiniert mit Sicherem STOPP
In diesem Fall besitzt die Funktion Sicheres ÖFFNEN/Sicheres SCHLIESSEN die höhere Priorität.

Zusätzlich ist über den Stellantrieb die sichere Endlagenrückmeldung möglich.

Abschaltkriterien
Wie für den Normalbetrieb kann auch für die Sicherheitsfunktionen festgelegt werden, in welchen Fällen der Antrieb abschaltet. Während im Normalbetrieb die Abschaltkriterien den Schutz von Armatur und Antrieb gewährleisten, kann es im Anforderungsfall einer Sicherheitsfunktion jedoch vorrangig sein, die Armatur unbedingt zu öffnen bzw. zu schließen. Ein Schaden am Antrieb oder an der Armatur wird dann gegebenenfalls in Kauf genommen.

Insgesamt stehen für Sicherheitsfunktionen die folgenden Abschaltkriterien zur Verfügung:

> Wegabhängige Abschaltung mit Überlastschutz
Sobald der eingestellte Schaltpunkt in der Endlage AUF oder ZU erreicht wird, schaltet die Steuerung den Antrieb ab. Tritt während der Fahrt ein überhöhtes Drehmoment auf, zum Beispiel durch einen in der Armatur eingeklemmten Gegenstand, wird der Antrieb zum Schutz der Armatur abgeschaltet, bevor die Endlage erreicht wird.

> Abschaltung in der Weg-Endlage
Der Stellantrieb stoppt erst, wenn die Endlage AUF oder ZU erreicht ist, unabhängig vom ausgeübten Drehmoment.

> Abschaltung in der Drehmoment-Endlage
Der Stellantrieb stoppt erst bei Erreichen der Weg-Endlage und des eingestellten Endlagendrehmoments.

> Keine Abschaltung
Hier werden Drehmoment- und Wegschalter überbrückt, um die Armatur unbedingt zu öffnen bzw. zu schließen. Um ein Verbrennen des Motors zu verhindern, empfehlen wir in diesem Fall, die AC .2 in Ausführung SIL mit Thermoschutzfunktion zu verwenden.

LAUFÜBERWACHUNG DES ANTRIEBS

Über eine elektromechanische Laufüberwachung des Antriebs kann mit Hilfe des SIL-Moduls die Zuverlässigkeit des Systems überprüft werden. Wird ein Fahrbefehl ausgegeben und der Antrieb fährt nach einer vordefinierten Zeit nicht an, dann aktiviert das SIL-Modul die SIL-Sammelfehlermeldung.

Diese Laufüberwachung ist auch im Normalbetrieb aktiv.

SICHERE EIN- UND AUSGÄNGE

Das SIL-Modul stellt drei sichere Eingänge und zwei sichere Ausgänge zur Verfügung:

> 1 redundant ausgeführter Eingang für Sicheres ÖFFNEN/ Sicheres SCHLIESSEN (es kann entweder Öffnen oder Schließen konfiguriert werden)
> 1 Eingang für Sicheren STOPP bzw. Freigabe in Richtung AUF
> 1 Eingang für Sicheren STOPP bzw. Freigabe in Richtung ZU
> 1 Ausgang zur Meldung eines SIL-Sammelfehlers
> 1 Ausgang zur Meldung „System bereit“

UNTERSTÜTZENDES DISPLAY

Informationen über den Status des SIL-Moduls, wie zum Beispiel das Ausführen einer Sicherheitsfunktion oder das Anstehen der SIL-Sammelfehlermeldung, werden mit entsprechenden Symbolen und Texten auf dem Display der AC .2 angezeigt.

FAIL-SAFE-EINHEIT FQM IN AUSFÜHRUNG SIL

Häufig wird gefordert, dass eine Sicherheitsfunktion auch bei Stromausfall ausgeführt werden kann.

Mit der Fail-Safe-Einheit FQM bietet AUMA eine innovative und sichere Antriebslösung, um Armaturen im Notfall auch ohne elektrischen Strom zu öffnen oder zu schließen.

EXIDA-ZERTIFIKAT FÜR SIL 2/SIL 3 ANWENDUNGEN

Die Fail-Safe-Einheit FQM in Ausführung SIL wurde von exida zertifiziert und ist für sicherheitsbezogene Anwendungen bis SIL 2 bei einkanaligem Systemaufbau auf bis SIL 3 bei redundantem Systemaufbau einsetzbar.

Die Fail-Safe-Einheit FQM wird immer in Kombination mit einem Schwenkantrieb SQ und einer Stellantriebs-Steuerung AC .2 eingesetzt. Die Fail-Safe-Einheit ist auch in explosionsgeschützter und in feuerfester Ausführung erhältlich.

Vielseitig in der Anwendung

AUMA Stellantriebe mit Fail-Safe-Einheit FQM eignen sich zur Automatisierung von Klappen und Hähnen mit Schwenkwinkeln von 90° (±10°). Sie werden in den verschiedensten Branchen eingesetzt: In Wasserhochbehältern zum Beispiel verhindern sie ein Leerlaufen bei Rohrbruch. In Kühlsystemen schützen sie bei Ausfall des normalen Kühlsystems vor Überhitzung. Dampfkesselapplikationen in Kraftwerken und Brandschutzmaßnahmen in Tunneln sind weitere Beispiele.

Anwendungen in der Öl- und Gasindustrie

In der petrochemischen Industrie sind die Anforderungen besonders hoch. Hier sorgen explosionsgeschützte und feuerfeste Ausführungen der Fail-Safe-Einheit für die geforderte Sicherheit. Typische Anwendungen sind Überfüllschutz in Tanklagern, Auslaufschutz in Tanks und Pipelines und der Einsatz in Gasregelstationen.

MECHANISCHE LÖSUNG FÜR HÖCHSTE SICHERHEIT

Die innovative Technik bietet zahlreiche Vorteile: Das im Notfall nötige Drehmoment wird rein mechanisch über die in einer Rollfeder gespeicherte Energie bereitgestellt. Elektrische Energie wird für die Fail-Safe-Fahrt nicht benötigt.

Der Rollfedermotor sorgt bei der Fail-Safe-Fahrt für ein gleichmäßig hohes Drehmoment über den gesamten Stellweg. Die Rollfeder ist bei Normalbetrieb entkoppelt und muss nicht mitbewegt werden. Entsprechend klein kann der Antrieb dimensioniert werden.

Ein weiterer Vorteil ist die regelbare Stellgeschwindigkeit: Kurz vor Erreichen der Endlage wird sie reduziert, so dass die Armatur langsam und sanft in die Endlage gefahren wird. Dies schont die Armatur und verhindert Druckspitzen in der Rohrleitung.

SICHERHEITSFUNKTIONEN

Die folgenden Sicherheitsfunktionen können mit Hilfe der Fail-Safe-Einheit FQM in Ausführung SIL realisiert werden:

> Sicheres ÖFFNEN/Sicheres SCHLIESSEN (Safe ESD, Emergency Shut Down)
Die Fail-Safe-Einheit FQM fährt in die konfigurierte Endlage AUF bzw. ZU. Diese Sicherheitsfunktion erreicht bei einkanaligem Systemaufbau SIL 2 (SC = 3, 1oo1/HFT = 0) und bei redundantem Systemaufbau SIL 3 (SC = 3, 1oo2/HFT = 1).

> Sichere Endlagenrückmeldung
Über SIL-bewertete Endlagenschalter in der Fail-Safe-Einheit FQM ist eine sichere Endlagenrückmeldung gemäß SIL 2 bei einkanaligem Systemaufbau möglich. Diese kann auch ausgelesen werden, wenn die Stromversorgung des Stellantriebs unterbrochen ist.

AUSLÖSEN DER FAIL-SAFE-FAHRT

Die folgenden Auslösekriterien für eine Fail-Safe-Fahrt sind bei einer Fail-Safe-Einheit in Ausführung SIL möglich:

> Emergency Shutdown (ESD) Signal einer Sicherheits-SPS

> Spannungsausfall ODER ESD Signal einer Sicherheits-SPS

Die Fail-Safe-Fahrt wird direkt im FQM ausgelöst. Dies ist unabhängig von der Stellantriebs-Steuerung AC. Die Rollfeder wird bei der Fail-Safe-Fahrt freigegeben und überträgt über ein Planetengetriebe das entstehende Drehmoment auf die Armatur.

Anwendungsbeispiel: Überfüllsicherung mit Fail-Safe-Einheit FQMEx in Ausführung SIL
Soll sichergestellt sein, dass eine Überfüllsicherung für Öltanks auch bei einem Stromausfall funktioniert, kann das SIS mit Fail-Safe-Einheit FQMEx realisiert werden.

In der Regel sind SIS und System für den Normalbetrieb separat aufgebaut (Bild rechts oben). Eine Standard-SPS steuert mithilfe eines Füllstandssensors und eines Stellantriebs in Standardausführung mit zugehöriger Armatur das gesamte System zum Befüllen des Tanks. Die Armatur des SIS ist im Normalbetrieb geöffnet. Die Sicherheits-SPS überwacht kontinuierlich über separate Sensoren den Füllstand im Tank. Wird ein vorher festgelegter Grenzwert überschritten, geht die Sicherheits-SPS von einem Fehler aus. Sie übermittelt ein Emergency Shutdown Signal direkt an die Fail-Safe-Einheit FQM. Dies löst eine Fail-Safe-Fahrt aus und die Armatur des SIS wird geschlossen.

Grundsätzlich können SIS und System für den Normalbetrieb auch kombiniert werden (Bild rechts unten). Es muss jedoch in jedem Einzelfall geprüft werden, ob die von der IEC 61511 geforderten Bedingungen an ein solches kombiniertes System vollständig erfüllt sind.

Um eine fundierte und nachvollziehbare Aussage über die Eignung von AUMA Produkten für sicherheitstechnische Anwendungen machen zu können, wurde ihre SIL-Fähigkeit ermittelt. Die Norm IEC 61508 sieht dazu zwei verschiedene Verfahren vor: die Hardwarebeurteilung und die vollständige Bewertung.

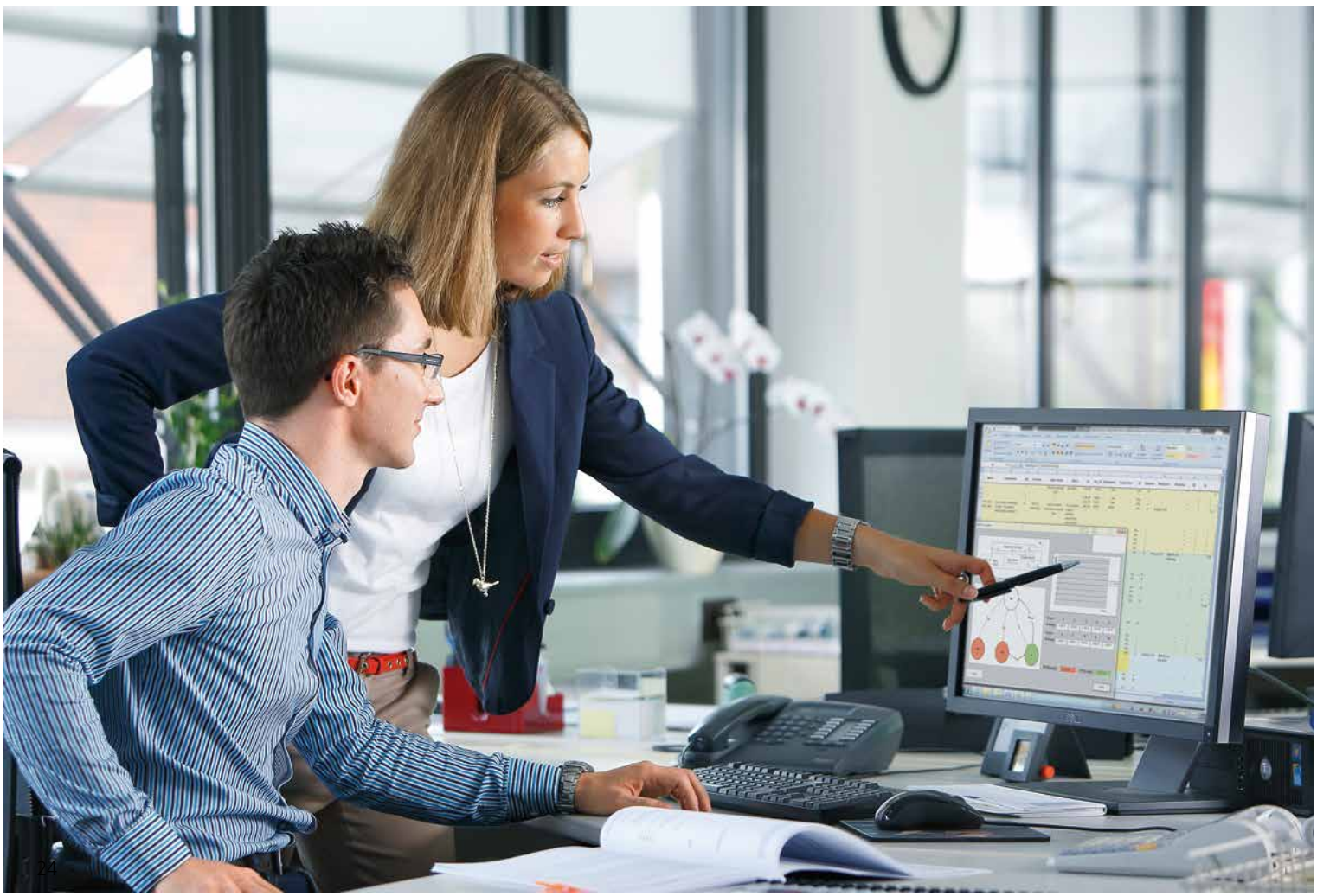
Hardwarebeurteilung

Bereits bestehende Produkte hat AUMA anhand einer Hardwarebeurteilung aufgrund von Felderfahrung bewerten lassen. Dazu zählen zum Beispiel die Stellantriebe SA und SQ sowie die Getriebe GK. Nähere Informationen finden Sie auf Seite 25.

Vollständige Bewertung

Die Neuentwicklungen Stellantriebs-Steuerung AC .2 in Ausführung SIL und Fail-Safe-Einheit FQM in Ausführung SIL dagegen sind vollständig bewertet worden. Dabei wurden die relevanten fehlervermeidenden Maßnahmen gemäß IEC 61508 in allen relevanten Phasen des Produktlebenszyklus angewendet, von der Spezifikation bis hin zur Außerbetriebsetzung des Produkts. Nähere Informationen finden Sie auf Seite 26.

ERMITTLUNG DER SIL-FÄHIGKEIT FÜR AUMA PRODUKTE



Zur Bewertung bereits bestehender Komponenten sieht die Norm IEC 61508 eine Eignungsaussage auf der Basis einer Hardwarebeurteilung eines Gerätes vor.

Für die einzelnen Komponenten werden Sicherheitskennzahlen ermittelt, anhand derer die SIL-Einstufung vorgenommen werden kann.

Generische Daten

Generische Daten sind statistisch ermittelte Ausfallraten für einzelne Bauelemente, die in speziellen Datenbanken, sogenannten „Reliability data books“, gelistet sind. Für die Beurteilung der elektronischen Bauelemente, die in AUMA Produkten verwendet werden, wurden beispielsweise generische Daten von exida und aus der Siemens Norm SN 29500 verwendet.

Feldrücklaufdaten

Für mechanische Komponenten sind nur wenige generische Daten verfügbar. Hier werden über Feldrücklaufdaten, zum Beispiel Fehlerrückmeldungen während der Garantiezeit, und über Versuchsergebnisse Rückschlüsse auf die Zuverlässigkeit der entsprechenden Bauteile gezogen.

FMEDA

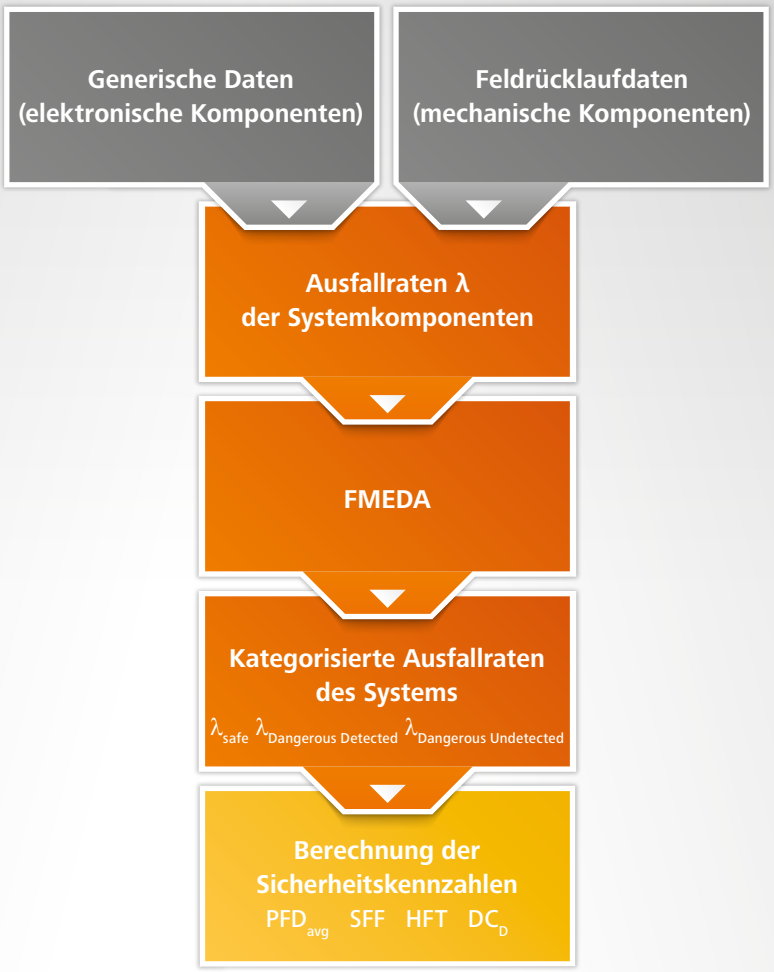
Die FMEDA (Failure Mode Effects and Diagnostic Analysis, Ausfallarten-, Auswirkungs- und Diagnoseabdeckungsanalyse) ist eine nach der IEC 61508 anerkannte Methode, um Sicherheitskennzahlen zu berechnen.

Diese Analyse erfolgt in definierten Schritten, die dokumentiert und jederzeit nachvollziehbar sind.

Mit Hilfe der FMEDA werden mögliche Fehlerszenarien und die jeweiligen Eintrittswahrscheinlichkeiten untersucht. Zudem wird analysiert, ob die möglichen Fehler für die Sicherheitsfunktion gefährlich sind oder nicht und ob sie diagnostiziert und damit erkannt werden können.

Aus den so ermittelten Ausfallraten werden Ausfallwahrscheinlichkeiten (PFD_{avg}-Werte) und weitere Sicherheitskennzahlen wie Safe Failure Fraction (SFF) und Diagnosedeckungsgrad (DC_D) berechnet.

Ermittlung der Sicherheitskennzahlen



Bei der Stellantriebs-Steuerung AC .2 in Ausführung SIL und bei der Fail-Safe-Einheit FQM in Ausführung SIL handelt es sich um Neuentwicklungen, für die eine vollständige Bewertung nach IEC 61508 durchgeführt wurde.

Die Zertifizierung wurde bei der AC 01.2 in Ausführung SIL vom TÜV Nord und beim FQM in Ausführung SIL von exida durchgeführt.

Was wurde geprüft?
Gegenüber der reinen Hardwarebeurteilung bereits bestehender Produkte werden bei der vollständigen Bewertung zusätzlich zum Beispiel die Entwicklungs- und Produktionsabläufe geprüft und zertifiziert, um systematische Fehler möglichst zu vermeiden.

Systematische Fehler sind in der Regel Fehler, die z.B. bei der Spezifikation, Entwicklung, Fertigung, Inbetriebnahme, Betrieb oder Wartung auftreten. Sie sind prinzipiell vermeidbar.

Functional Safety Management System
AUMA nutzt zur Vermeidung von systematischen Fehlern ein Functional Safety Management (FSM) System. Ein solches FSM System kann als Erweiterung eines Qualitätsmanagementsystems betrachtet werden. Durch die darin beschriebenen Regelungen und Definitionen werden mögliche Fehlerquellen möglichst weitgehend vermieden. Außerdem werden Maßnahmen ergriffen, um möglichst alle verbliebenen systematischen Fehlerquellen rechtzeitig zu entdecken und zu beseitigen, bevor eine gefährliche Situation entsteht.

Ermittlung der Sicherheitskennzahlen
Die trotz aller Maßnahmen verbleibenden zufälligen Fehler werden quantitativ erfasst, um das verbleibende Restrisiko beurteilen zu können. Dazu werden die Sicherheitskennzahlen wie zum Beispiel die Ausfallwahrscheinlichkeit der Produkte ermittelt und dem Endanwender zur Verfügung gestellt.

Dieser Vorgang läuft bei AUMA nach der gleichen Vorgehensweise ab wie bei der reinen Hardwarebeurteilung (siehe Seite 25).

ERMITTLUNG DER SIL-FÄHIGKEIT FÜR AUMA PRODUKTE

TÜV NORD

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

Zertifikat

Nr. 1435.IM.155027/19 V1.0

Die TÜV NORD Systems GmbH & Co. KG bestätigt hiermit

AUMA Riester GmbH & Co. KG
Aumastraße 1
79379 Müllheim

dass das

elektrische Stellantriebssystem mit den Stellantrieben 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 und SQ(R)05.2- SQ(R)14.2/ SQ(R)Ex05.2- SQ(R)Ex14.2 mit Stellantriebs-Steuerungen AC01.2/ACExC01.2 in Ausführung SIL

mit den Sicherheitsfunktionen „Emergency Shut Down (ESD)" und „Safe Stop" die Anforderungen der nachfolgenden Norm erfüllt.

- DIN EN 61508-1/-2: 2011, einsetzbar bis SIL 2 (HFT = 0) und SIL 3 (HFT ≥ 1)
- IEC 61508-1/-2: 2010, einsetzbar bis SIL 2 (HFT = 0) und SIL 3 (HFT ≥ 1)

Zertifizierungsprogramm Leitbechnik (SEB-ZE-SEECERT-VA-320-20, Rev. 5.1 / 04.19)

Grundlage der Zertifizierung ist der Bericht 1435.IM.155027/19TB in der jeweils gültigen Fassung.

Dieses Zertifikat berechtigt zur Nutzung des nebenstehenden Prüfzeichens.

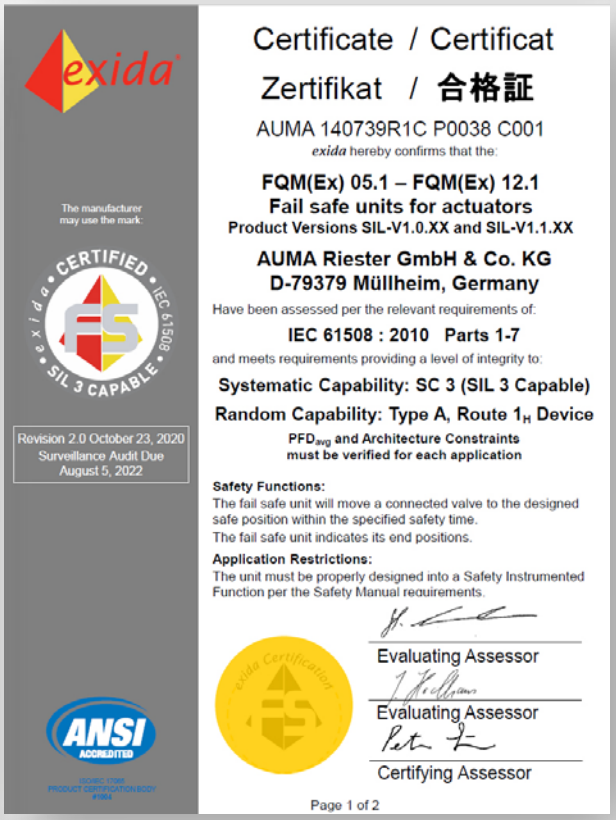
Gültig bis: 2024-12-17
Aktenzeichen: 8117657310

Hamburg, 2019-12-17

Bianca Pfuff

TÜV NORD Safety Approved Elektrisches Stellantriebssystem DIN EN 61508-1-2: 2011 IEC 61508-1/-2: 2010 einsetzbar bis SIL 3 1435.IM.155027/19

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



exida

The manufacturer may use the mark:

exida 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

FRAGEN SIE UNSERE EXPERTEN

Die Auswahl der richtigen Komponenten zur Realisierung eines sicherheitstechnischen Systems ist immer wieder eine Herausforderung. Mit der bloßen Berechnung der Ausfallwahrscheinlichkeit ist es nicht getan. Viele Rahmenbedingungen müssen in jedem Einzelfall untersucht und bewertet werden.

Unsere Experten verfügen über langjährige Erfahrung beim Einsatz von elektrischen Stellantrieben in sicherheitstechnischen Systemen. Gerne unterstützen wir Sie bei Fragen zur Auslegung Ihres SIS oder bei der Auswahl des passenden Stellantriebs.

Sprechen Sie uns an. Wir freuen uns auf das Gespräch mit Ihnen.

NUTZEN SIE UNSERE DOKUMENTATION

AUMA stellt detailliertes und umfangreiches Material zum Thema Funktionale Sicherheit zur Verfügung.

Die folgenden Dokumente können Sie bei AUMA anfordern:

> Herstellererklärungen
> Sicherheitskennzahlen
> Sicherheitshandbücher mit Checklisten

Die folgenden Dokumente zu SIL-klassifizierten Stellantrieben, Stellantriebs-Steuerungen und Getrieben finden Sie direkt auf www.auma.com:

> Handbücher und Betriebsanleitungen
> Technische Daten
> Produktzertifikate

SO UNTERSTÜTZT AUMA

auma®
Solutions for a world in motion

AUMA Riester GmbH & Co. KG
Aumastraße 1
79379 Müllheim
Deutschland
Tel +49 7631 809-0
Fax +49 7631 809-1250
info@auma.com

AUMA Tochtergesellschaften und Vertretungen sind in über 70 Ländern für Sie da. Detaillierte Kontaktinformationen finden Sie auf unserer Website.
www.auma.com