

Fail-Safe-Einheit in Ausführung SIL

FQM 05.1 – FQM 12.1 /FQMEx 05.1 – FQMEx 12.1

mit nicht sicherheitsrelevanten Stellantrieben

SQ 05.2 – SQ 12.2/SQR 05.2 – SQR 12.2

SQEx 05.2 – SQEx 12.2/SQREx 05.2 – SQREx 12.2

mit Stellantriebs-Steuerung

AC 01.2/ACExC 01.2



HINWEIS zur Verwendung!

Dieses Dokument ist nur in Verbindung mit der aktuellen, dem Gerät beiliegenden Betriebsanleitung, des beiliegenden Handbuchs, der beiliegenden auftragspezifischen Herstellererklärung sowie den jeweiligen technischen und elektrischen Daten gültig. Diese sind als mitgeltende Dokumente zu verstehen.

Zweck des Dokumentes:

Dieses Dokument informiert über die notwendigen Maßnahmen, die für den Einsatz des Gerätes in sicherheitsbezogenen Systemen nach IEC 61508 bzw. IEC 61511 erforderlich sind.

Das Sicherheitshandbuch richtet sich primär an Planer, Betreiber, Servicemitarbeiter und Manager, die Sicherheitstechnische Systeme (SIS), die eine Fail-Safe-Einheit FQM / FQMEx beinhalten, erstellen, betreiben oder warten. Das Sicherheitshandbuch gibt diesen zusammen mit den mitgeltenden Dokumenten alle notwendigen Informationen um die Fail-Safe Einheit FQM / FQMEx sicher in das SIS einzubinden, zu betreiben und zu warten.

Referenzunterlagen:

- Betriebsanleitung (Montage, Bedienung, Inbetriebnahme) zum Stellantrieb.
- Betriebsanleitung (Montage, Bedienung, Inbetriebnahme) Fail-Safe-Einheit.
- Handbuch (Betrieb und Einstellung) Stellantriebs-Steuerung AC 01.2/ACExC 01.2.
- Handbuch (Geräteintegration Feldbus) Stellantriebs-Steuerung AC 01.2/ACExC 01.2.
- Technische Daten zur Fail-Safe-Einheit, zum Stellantrieb und zur Stellantriebs-Steuerung.
- Einbauerklärung und EU-Konformitätserklärung für die Fail-Safe-Einheit.
- SIL-Konformitätserklärung zur Funktionale Sicherheit (auftragsbezogen)

Referenzunterlagen sind im Internet: unter <http://www.auma.com> erhältlich.

Inhaltsverzeichnis	Seite
1. Terminologie.....	4
1.1. Abkürzungen und Begriffe	4
2. Anwendung und Gültigkeit.....	6
2.1. Anwendungsbereich	6
2.2. Normen	6
2.3. Gültige Gerätetypen	6
3. Projektierung, Konfiguration und Einsatzbedingungen.....	8
3.1. Projektierung (Antriebsauslegung)	8
3.2. Konfiguration (Einstellung)/Ausführung	9
3.3. Weitere Hinweise und Angaben zur Projektierung	10
3.4. Einsatzbedingungen (Umweltbedingungen)	10
4. Sicherheitstechnische Systeme und Sicherheitsfunktionen.....	11
4.1. Sicherheitstechnisches System mit einem Stellantrieb	11
4.2. Sicherheitsfunktionen	11
4.3. Sichere Ein- und Ausgänge	12
4.4. Redundanter Systemaufbau	12
4.5. Anwendungsbeispiele	13
4.6. Systemdarstellung	14
4.7. Diagnosefunktion durch den Betreiber	14
4.8. Interne Diagnosen der Fail-Safe-Einheit	15
5. Installation, Inbetriebnahme und Betrieb.....	16
5.1. Installation	16
5.2. Inbetriebnahme	18

5.3.	Betrieb	18
5.4.	Lebensdauer	18
5.5.	Außerbetriebsetzung	18
5.6.	Entsorgung und Recycling	19
6.	Anzeigen.....	20
7.	Meldungen.....	21
7.1.	Meldungen über das FS-Modul	21
7.2.	Zustandsmeldungen über Melderelais (digitale Ausgänge) der Stellantriebs-Steuerung	21
7.3.	Meldungen über Feldbus der Stellantriebs-Steuerung	21
8.	Prüfungen und Wartung.....	22
8.1.	Sicherheitseinrichtung überprüfen	22
8.2.	Interne Antriebsüberwachung des Gerätes mit Ansteuerung über die Stellantriebs-Steuerung	22
8.3.	Partial Valve Stroke Test (PVST) durchführen	23
8.4.	Proof-Test (Überprüfung auf sichere Funktion des Stellantriebs)	24
8.4.1.	ESD Fahrt (sicheres ÖFFNEN/SCHLIESSEN) prüfen	25
8.4.2.	ESD Fahrt (sicheres ÖFFNEN/SCHLIESSEN) mit zusätzlicher Netzauslösung prüfen	26
8.4.3.	Sichere Endlagenmeldung prüfen	27
8.5.	Wartung	28
9.	Sicherheitstechnische Kennzahlen.....	29
9.1.	Bestimmung der Kennzahlen	29
9.2.	Spezifische Kennzahlen für die Fail-Safe-Einheit in Ausführung SIL mit Stellantrieben der Baureihe SQ. 2	29
10.	Checklisten.....	33
10.1.	Inbetriebnahme-Checkliste	33
10.2.	Proof-Test-Checklisten	33
10.2.1.	Safe ESD Sicherheitsfahrt (sicheres ÖFFNEN/SCHLIESSEN)	33
10.2.2.	Überprüfen und Validierung der Sicherheitsfunktion "sichere Endlagenrückmeldung"	35
11.	SIL-Konformitätserklärung (Beispiel).....	37
	Stichwortverzeichnis.....	41
	Adressen.....	42

1. Terminologie

- Informationsquellen**
- IEC 61508-4, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen
 - IEC 61511-1, Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware

1.1. Abkürzungen und Begriffe

Für die Bewertung der Sicherheitsfunktionen werden in erster Linie die Lambda-Werte bzw. der PFD-Wert (Probability of Dangerous Failure on Demand) und der SFF-Wert (Safe Failure Fraction) benötigt. Zur Bewertung der Einzelkomponenten sind weitere Kennzahlen notwendig. In nachfolgender Tabelle werden diese kurz erläutert.

Tabelle 1: Abkürzungen Sicherheitstechnische Kennzahlen

Kennzahl	Englisch	Beschreibung
λ_S	Lambda S afe	Anzahl der sicheren Ausfälle
λ_D	Lambda D angerous	Anzahl der gefährlichen Ausfälle
λ_{DU}	Lambda D angerous U ndetected	Anzahl der unentdeckten gefährlichen Ausfälle
λ_{DD}	Lambda D angerous D etected	Anzahl der entdeckten gefährlichen Ausfälle
DC	D iagnostic C overage	Diagnosedeckungsgrad - Verhältnis der Ausfallrate der durch Diagnosetests erkannten gefährlichen Fehler zur Gesamtrate gefährlicher Fehler der Komponente oder des Teilsystems. Der Diagnosedeckungsgrad beinhaltet keine bei Wiederholungsprüfungen (proof tests) festgestellten Fehler
MTBF	M ean T ime B etween F ailures	Mittlere Zeit zwischen dem Auftreten von zwei aufeinander folgenden Fehlern
SFF	S afe F ailure F raction	Anteil sicherer sowie detektierbarer gefährlicher Ausfälle
PFD_{avg}	Average P robability of dangerous F ailure on D emand	Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
HFT	H ardware F ailure T olerance	Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen. Eine HFT = n bedeutet, dass die Funktion bei bis zu n gleichzeitig auftretenden Fehlern noch sicher ausgeführt werden kann.
T_{proof}	Proof test interval	Intervall für Wiederholungsprüfung

SIL Sicherheits-Integritätslevel (**S**afety **I**ntegrity **L**evel).

Die internationale Norm IEC 61508 definiert 4 Level (SIL 1 bis SIL 4).

Sicherheitsfunktion Funktion, die von einem SIS oder einem sicherheitsbezogenen System zur Risikominderung ausgeführt wird, mit dem Ziel, im Falle eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die Anlage/Einrichtung zu erreichen oder aufrechtzuerhalten.

Sicherheitstechnische Funktion (SIF) Funktion mit vorgegebenem Sicherheitsintegritätslevel (SIL), die zum Erreichen der funktionalen Sicherheit notwendig ist.

Sicherheitstechnisches System (SIS) Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en).

Sicherheitsbezogenes System	<p>Ein sicherheitsbezogenes System schließt alles (Hardware, Software, menschliche Faktoren) ein, das zur Ausführung von einer oder mehreren Sicherheitsfunktionen erforderlich ist. Dabei würden Ausfälle der Sicherheitsfunktion eine signifikante Zunahme des Sicherheitsrisikos für Personen und/oder Umwelt bedeuten.</p> <p>Ein sicherheitsbezogenes System kann eine eigenständige Anlage zur Ausführung einer bestimmten Sicherheitsfunktion sein oder in eine andere Anlage integriert sein.</p>
Wiederholungsprüfung	<p>Eine wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls das System in einen "Wie-Neu"-Zustand gebracht oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand herangebracht werden kann.</p>
MTTR (Mean Time To Restoration)	<p>Mittlere Zeit bis zur Wiederherstellung nach dem Auftreten eines Fehlers. Diese gibt an, wie lange die Wiederherstellung des Systems im Mittel dauert. Sie ist somit ein wichtiger Parameter für die Systemverfügbarkeit. In dieser Zeit ist auch die Zeit bis zur Entdeckung des Fehlers, das Planen der Aufgaben sowie der Betriebsmittel enthalten. Sie sollte so kurz wie möglich gehalten werden.</p>
MRT (Mean Repair Time)	<p>Die mittlere Reparaturdauer gibt die mittlere Dauer an, die zur Reparatur eines Systems benötigt wird. Die MRT ist wichtig, um die Zuverlässigkeit und Verfügbarkeit eines Systems zu bestimmen. Die MRT sollte möglichst kurz sein.</p>
Gerätetyp (Typ A und Typ B)	<p>Die Stellantriebs-Steuerung kann als Gerät vom Typ A betrachtet werden, wenn für alle Komponenten, die zur Erreichung der sicherheitstechnischen Funktion erforderlich sind, alle folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none">• Die Ausfallarten für alle beteiligten Komponenten sind gut definiert.• Das Verhalten im Fehlerfall kann vollständig vorhergesagt werden.• Es liegen ausreichend abhängige Ausfalldaten aus dem Feld vor, um nachzuweisen dass die angegebenen Ausfallraten erfüllt sind (Confidence Level min. 70%). <p>Die Stellantriebs-Steuerung muss als Gerät vom Typ B betrachtet werden, wenn eine oder mehrere der folgenden Bedingungen zutreffen:</p> <ul style="list-style-type: none">• Der Ausfall mindestens eines Elementes ist nicht gut definiert.• Das Verhalten im Fehlerfall ist nicht vollständig bekannt.• Es gibt keine zuverlässigen Fehlerangaben der Feldgeräte, um die Ausfallrate für die ermittelten und unentdeckten gefährlichen Ausfälle zu stützen.
PTC (Proof Test Coverage)	<p>Der Proof Test Coverage beschreibt den Anteil der aufdeckbaren Ausfälle durch einen Proof-Test.</p>
Fail-Safe-Stellzeit/ ESD Dauer/ Fail-Safe Fahrzeit	<p>Die Begriffe Fail-Safe-Stellzeit, ESD Dauer und Fail-Safe Fahrzeit werden in der Dokumentation zur Fail-Safe-Einheit synonym verwendet. Sie bezeichnen die Stellzeit, die benötigt wird, um bei Anforderung der ESD Funktion (Betrieb mittels Rollfeder) die Fahrt aus der entgegengesetzten Endlage in die Sicherheitsendlage durchzuführen.</p> <p>Im Gegensatz dazu bezeichnet die Stellzeit im Normalbetrieb die Zeit, die benötigt wird, die Armatur mittels des elektrischen Stellantriebs von einer Endlage in die andere zu verfahren.</p>

2. Anwendung und Gültigkeit

2.1. Anwendungsbereich

AUMA Stellantriebe und Stellantriebs-Steuerungen mit den in diesem Handbuch genannten Sicherheitsfunktionen sind für die Betätigung von Industriearmaturen bestimmt und eignen sich für den Einsatz in sicherheitstechnischen Systemen nach IEC 61508 bzw. IEC 61511.

Die Fail-Safe-Einheit ist der Teil eines Antriebs der in der Lage ist, auch ohne äußere Energiezufuhr, die an ihn angeschlossene Armatur einmalig in eine vorher festgelegte Sicherheitsposition zu verfahren und dort zu halten.

Die Hardware, Software und die Konfiguration der Fail-Safe-Einheit und des zugehörigen Stellantriebs darf ohne schriftliche Zustimmung von AUMA nicht verändert werden. Unautorisierte Veränderungen können die Sicherheitskennzahlen und die SIL-Fähigkeit der Fail-Safe-Einheit negativ beeinflussen.

Der Anwender darf die Fail-Safe-Einheit nur in sicherheitstechnischen Systemen einsetzen wenn er folgende Punkte sicher stellt:

- Die Fail-Safe-Einheit darf nur im Low Demand Mode betrieben werden.
- Alle Materialien, Umwelt- und Prozessbedingungen müssen mit den Herstellerangaben und Einschränkungen durch AUMA (siehe insbesondere das technische Datenblatt und die Betriebsanleitung) kompatibel sein.
- Alle in diesem Sicherheitshandbuch genannten Tätigkeiten müssen durchgeführt und genannte Einschränkungen beachtet werden.
- Alle in der Betriebsanleitung, den technischen Daten und der auftragspezifischen Herstellererklärung genannten Einschränkungen bezüglich des Anwendungsbereichs müssen eingehalten werden.

Bei Verwendung der Fail-Safe-Einheit in einem SIS muss die IEC 61508, die IEC 61511 oder die zutreffende Produktnorm beachtet werden.

Materialien, Umweltbedingungen und Prozessbedingungen müssen mit den Herstellerangaben und Einschränkungen durch AUMA kompatibel sein.

Alle in diesem Sicherheitshandbuch genannten Tätigkeiten müssen durchgeführt, und genannte Einschränkungen beachtet werden.

2.2. Normen

Der sicherheitsrelevante Teil der Fail-Safe-Einheit wurde gemäß IEC 61508 Ausgabe 02 entwickelt und bewertet. Sicherheitskennzahlen wurden berechnet und eine FMEDA wurde durchgeführt.

2.3. Gültige Gerätetypen

Die in diesem Handbuch enthaltenen Angaben zur Funktionalen Sicherheit sind für die hier angegebenen Gerätetypen gültig.

Tabelle 2: Übersicht über die geeigneten Gerätetypen

Typ		
Fail-Safe-Einheit	Stellantrieb	Stellantriebs-Steuerung
FQM 05.1 – FQM 12.1 in Version SIL-V1.0.00	SQ 05.2 – SQ 12.2	AC 01.2
FQMEEx 05.1 – FQMEEx 12.1 in Version SIL-V1.0.00	SQEx 05.2 – SQEx 12.2	ACExC 01.2

Die zulässigen Versionen und Konfigurationen des sicherheitsrelevanten Teils der Fail-Safe-Einheit sind in der AV 06.03.020.xx „Ausführungsbestimmungen für die FQM in SIL Ausführung“ beschrieben.

Information

In Anwendungen mit Anforderungen zur Funktionalen Sicherheit dürfen nur AUMA Fail-Safe-Einheiten in Ausführung SIL zum Einsatz kommen. AUMA Fail-Safe-Einheiten in Ausführung SIL sind u.a. daran zu erkennen, dass auf dem Typenschild hinter der Zeile mit der Bezeichnung ESD: ... die Buchstabenfolge „SIL-V1.0.XX“ zu finden ist. Dabei stellt „xx“ einen Platzhalter für eine zweistellige Zahl dar.

Bild 1: Beispiel Typenschild mit Kennzeichnung „SIL“



3. Projektierung, Konfiguration und Einsatzbedingungen

3.1. Projektierung (Antriebsauslegung)

Für die Projektierung (Antriebsauslegung) der Stellantriebe mit Fail-Safe-Einheit werden in erster Linie die benötigten maximalen Drehmomente, Laufmomente und die Stellzeiten berücksichtigt.

HINWEIS

Falsche Antriebsauslegung kann zu Schäden an den Geräten im sicherheitsbezogenen System führen!

Mögliche Folgen sind z. B.: Schäden an der Armatur, Überhitzung des Motors, Verkleben der Schütze, defekte Thyristoren, Erwärmung bzw. Beschädigung von Leitungen.

- Bei der Antriebsauslegung die Technischen Daten des Stellantriebs und die der Fail-Safe-Einheit unbedingt berücksichtigen.
- Genügend Reserve einplanen, um sicherzustellen, dass der Stellantrieb mit Fail-Safe-Einheit in der Lage ist, die Armatur auch im Störfall und bei Unterspannungsbedingungen zuverlässig zu schließen bzw. zu öffnen.

Das garantierte (minimal) von der Fail-Safe-Einheit bei Durchführung einer Fail-Safe Fahrt zur Verfügung gestellte Drehmoment kann den zum jeweiligen Produkt gehörenden technischen Daten entnommen werden. Das maximal auf die Armatur ausgeübte Drehmoment ist das Doppelte dieses Betrags. Ausgenommen hiervon sind Drehmomentspitzen, die z.B. beim abrupten Abbremsen bei Einfahrt in die Endlage einer relativ steifen Armatur entstehen können. Ebenso können diese auftreten, wenn die ESD-Funktion angefordert wird und gleichzeitig die Armatur blockiert ist (z.B. sich bereits in der Fail-Safe-Endlage befindet). Die Drehmomentüberhöhung solcher Drehmomentspitzen hängt unter anderem stark von der Masse und der Steifigkeit der Armatur ab und kann den genannten Faktor 2 deutlich übersteigen.

Bei der ESD Fahrt wird die Armatur von der Feder der Fail-Safe-Einheit immer mit deren nominalem Drehmoment in die Endlage verfahren und dort gehalten. Dies gilt auch, wenn für die betriebliche Fahrt mit dem elektrischen Stellantrieb ein reduzierter Drehmoment(bereich) gewählt wurde.

Um Schäden an der Armatur bei einer Sicherheitsfahrt zu vermeiden, empfehlen wir die Armatur je nach Steifigkeit, mindestens auf das 3-fache des maximalen Drehmoments des Stellantriebs auszuliegen.

Während der Initialisierung darf kein Drehmoment gegen die Fail-Safe Richtung auf die Armatur aufgebracht werden. Deshalb ist die Fail-Safe-Einheit für Anwendungen mit Klappen ungeeignet, bei denen in der Sicherheitsposition Druck oder Drehmoment entgegen der Fail-Safe Richtung aufgebracht wird.

Die Endlagenschalter haben – wie jeder Schalter – eine gewisse Hysterese. Deshalb werden die Endlagenschalter minimal vor Erreichen des mechanischen Endanschlags betätigt und signalisieren bereits die Endposition. Ebenso signalisieren sie das Verlassen der Endposition erst minimal, nachdem die mechanische Endposition des Stellantriebs verlassen wurde. Durch eine präzise Einstellung der Endlagen/Endanschläge kann dieser Effekt jedoch minimiert werden.

Am stellantriebsseitigen Eingang des FQM darf maximal ein dem in den technischen Daten zum FQM angegebenen nominalen Drehmoment entsprechendes Drehmoment angelegt werden.

Bezüglich weiterer bei der Projektierung zu beachtender Umwelteinflüsse wie z.B. Schwingungen, Temperatur, ... müssen die Angaben in den technischen Daten und der Betriebsanleitung unbedingt beachtet werden.

Bei sicherheitskritischen Anwendungen ist eine entsprechende Manipulationssicherung vorzusehen. Je nach projektspezifischer Risikoeinschätzung kann diese z.B. eine Spezialschraube, eine Zugangsbeschränkung (z.B. Zaun) oder andere Maßnahmen sein.

3.2. Konfiguration (Einstellung)/Ausführung

Die Konfiguration (Einstellung) der sicherheitsbezogenen Funktionen wird werksintern bei der Montage der Fail-Safe-Einheit definiert und anschließend bei der Endabnahme validiert. Eine nachträgliche Änderung der Konfiguration ist beim Anlagenbetreiber nicht zulässig. Ausnahme: Einstellung der Endanschläge (siehe Betriebsanleitung) und – in gewissen Grenzen – die Einstellung der Fail-Safe Stellzeit (siehe unten).

Die Einstellung allgemeiner Funktionen erfolgt wie in der Betriebsanleitung bzw. wie im Handbuch (Betrieb und Einstellung) AUMATIC AC 01.2 beschrieben.

Die Konfiguration der sicherheitsbezogenen Funktionen steht im auftragsbezogenen technischen Datenblatt.

Die Stellzeit für die Fail-Safe Fahrt kann – in gewissen Grenzen – eingestellt werden:

- Werkseitig wird für den Punkt, ab dem die Fail-Safe Fahrt bei Einfahrt in die Endlage gebremst wird (siehe Schaltplan: Schalter 30%) eine von zwei Konfigurationen gewählt (10 % bzw. 30 %). Diese Einstellung kann nicht geändert werden.
- Im Elektroanschluss kann mittels Brücken zwischen den Anschlüssen XF 31-34 die Geschwindigkeit der Fail-Safe Fahrt in 4 Stufen beeinflusst werden. Diese Einstellung kann im Feld (vor Ort) geändert werden.

Die Tabelle <Typische Fail-Safe Stellzeiten unter Normbedingungen> gibt an, wie die typische Fail-Safe Stellzeit unter Normbedingungen (siehe Hinweis unten) von der werkseitig vorgegebenen Konfiguration des Schalters 30%, sowie der Konfiguration der Klemmen XF 31-34 abhängt. Die minimale Stellzeit unter Normbedingungen beträgt 50 % der genannten Werte, die maximale Stellzeit unter Normbedingungen beträgt 200 % der genannten Werte.

- Information**
- Die angegebenen typischen, minimalen und maximalen Fail-Safe Stellzeiten beziehen sich auf einen Schwenkwinkel von 90°.
 - Die angegebenen typischen, minimalen und maximalen Fail-Safe Stellzeiten beziehen sich auf die absolute Einstellung des Endanschlags der Fail-Safe Endlage wie werkseitig voreingestellt und ein Lastprofil gemäß EN 15714-2:2009 (Normbedingungen).
 - Die angegebenen typischen, minimalen und maximalen Fail-Safe Stellzeiten erfordern, dass während der gesamten Ausführung der Fail-Safe Funktion (Fail-Safe Fahrt) die ESD Anforderung bestehen bleibt. Wird die ESD Anforderung während der Ausführung der Fail-Safe Fahrt zurückgenommen, so fährt der Antrieb trotzdem in die Fail-Safe Endlage, möglicherweise werden die genannten Stellzeiten aber nicht eingehalten.
 - Die typische Stellzeit gilt außerdem ausschließlich bei Normaltemperatur.

Bei anderen Schwenkwinkeln, absoluten Einstellungen des Endanschlags der Fail-Safe Endlage (auch wenn der Schwenkwinkel unverändert 90° beträgt) und Lastprofilen wird sich die Stellzeit entsprechend ändern. In diesem Fall bezieht sich die Toleranz der Fail-Safe Stellzeit von –50 %/+100 % nicht auf die in Tabelle <Typische Fail-Safe Stellzeiten unter Normbedingungen> angegebenen Werte, sondern auf die durch die geänderte Konfiguration erzeugten neue typische Fail-Safe Stellzeit. Ebenso kann eine Fehlfunktion des elektrischen Stellantriebs bzw. der Stellantriebs-Steuerung die Fail-Safe Stellzeit beeinflussen (siehe hierzu Kapitel <Sicherheitsfunktionen>).

- Information**
- Wird die Stellzeit im Feld mittels der Klemmen XF 31-34 verändert, so sind nach der Veränderung mindestens folgende Prüfungen vorzunehmen:
- Proof Test gemäß Kapitel <Proof-Test>
 - Messung der Fail-Safe Stellzeit während des Proof-Tests und/oder unter realen Einsatzbedingungen.
 - Überprüfung, ob die gemessene Fail-Safe Stellzeit den in Tabelle <Typische Fail-Safe Stellzeiten unter Normbedingungen> angegebenen Werten (unter Berücksichtigung des vorherigen Information) bzw. den Anforderungen der Anwendung entspricht.

Tabelle 3:

Typische Fail-Safe Stellzeiten unter Normbedingungen (in Sekunden)								
30 %-Schalter	Konfiguration: 30 %/max. Fail-Safe Stellzeit				Konfiguration: 10 %/min. Fail-Safe Stellzeit			
	keine	XF	XF	XF	keine	XF	XF	XF
Brücke zwischen XF ... und XF ...		31-32	31-33	31-34		31-32	31-33	31-34
FQM 05.1	18	22	28	34	09	15	21	29
FQM 07.1	14	18	22	26	08	12	18	23
FQM 10.1	28	35	45	54	15	24	35	47
FQM 12.1	21	27	34	39	13	20	28	35

Konfigurationsmöglichkeiten der Sicherheitsfunktion

Tabelle 4: Konfigurationsmöglichkeiten der Sicherheitsfunktion

Konfiguration SIL-Funktion	Kurzbeschreibung	Auslösung durch	
		ESD	ESD oder Netzausfall
Safe ESD ZU	Sicheres SCHLIESSEN	ESD	ESD oder Netzausfall
Safe ESD AUF	Sicheres ÖFFNEN	ESD	ESD oder Netzausfall
Sichere Endlagenrückmeldung	Meldet, ob eine der beiden Endlagen (AUF/ZU) erreicht ist oder nicht.	–	–

3.3. Weitere Hinweise und Angaben zur Projektierung

- Die Systematische Eignung beträgt SC03
- Es sollte ein Common Cause Failure (CCF) von 10 % angenommen werden, außer es wird durch eine Analyse gezeigt, dass ein kleinerer CCF angewendet werden kann.
- Es handelt sich um ein Typ A Gerät.
- Die HFT beträgt bei Verwendung einer FS-Einheit 0.
- Erforderliche Diagnosemaßnahmen siehe Kapitel <Sicherheitstechnisches System mit einem Stellantrieb>.

3.4. Einsatzbedingungen (Umweltbedingungen)

Bei der Projektierung und beim Einsatz der Stellantriebe und der Fail-Safe-Einheit in sicherheitstechnischen Systemen ist darauf zu achten, dass die zulässigen Einsatzbedingungen, aber auch die EMV Anforderungen durch die umgebenden Geräte eingehalten werden. Die Einsatzbedingungen sind im technischen Datenblatt angegeben:

- Schutzart
- Korrosionsschutz
- Umgebungstemperatur
- Schwingungsfestigkeit (Vibration)

Wenn die tatsächlichen Umgebungstemperaturen eine höhere durchschnittliche Temperatur als +40 °C aufweisen, müssen die Lambdawerte mit einem Sicherheitsfaktor beaufschlagt werden. Siehe Kapitel <Spezifische Kennzahlen für die Fail-Safe-Einheit in Ausführung SIL mit Stellantrieben der Baureihe SQ .2>

Zur Umweltprüfung durchlief die Fail-Safe-Einheit Prüfungen gemäß folgender Normen :

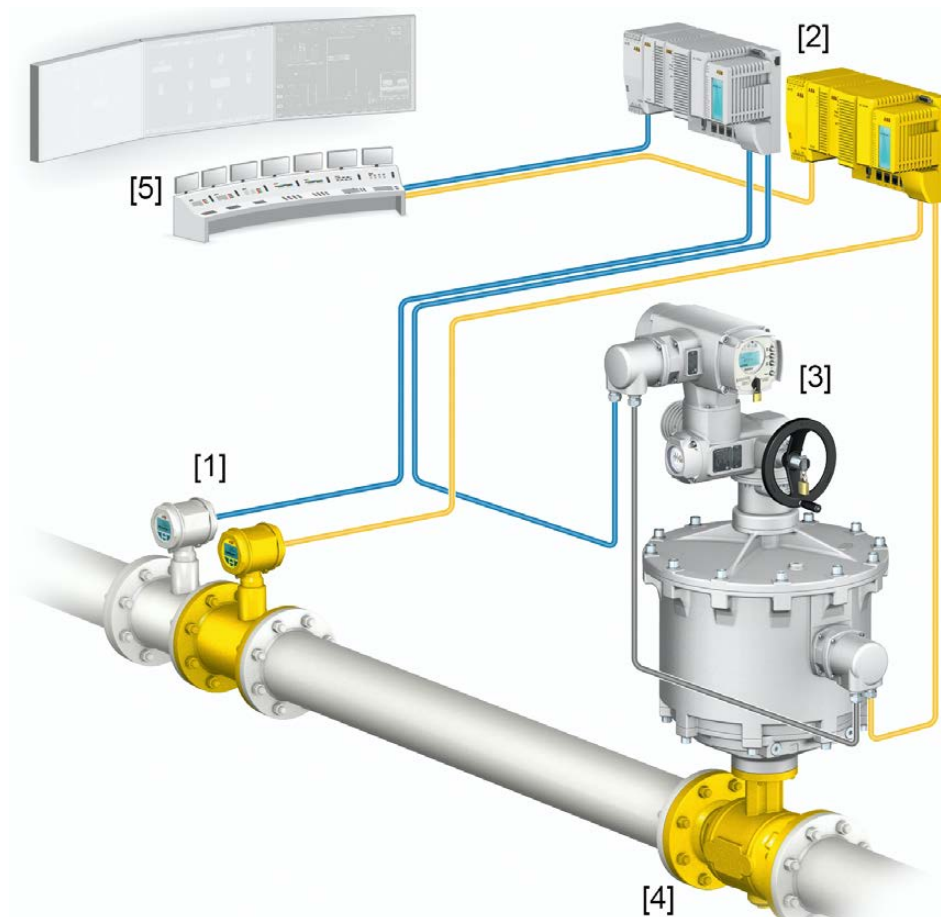
- Trockene Wärme: EN 60068-2-2
- Feuchte Wärme: EN 60068-2-30
- Kälte: EN 60068-2-1
- Schwingungsprüfung: IEC 60068-2-6
- Schutzartprüfung IP68: EN 60529
- Störfestigkeit: EN 61000-6-7
- Störaussendung: EN 61000-6-4

4. Sicherheitstechnisches Systeme und Sicherheitsfunktionen

4.1. Sicherheitstechnisches System mit einem Stellantrieb

Typischerweise besteht ein sicherheitstechnisches System mit einem Stellantrieb aus den im Bild dargestellten Komponenten.

Bild 2: Typisches sicherheitstechnisches System



- [1] Sensor
- [2] Steuerung (Standard- und Sicherheits-SPS)
- [3] Stellantrieb mit Stellantriebs-Steuerung und FQM
- [4] Armatur
- [5] Prozessleitsystem

Der Safety Integrity Level ist immer einem gesamten sicherheitstechnischen System, nicht einer Einzelkomponente zugeordnet.

Für eine einzelne Komponente (z.B. eine Fail-Safe-Einheit) werden sicherheitstechnische Kennzahlen ermittelt. Anhand dieser Kennzahlen können die Geräte dann einem möglichen Safety Integrity Level (SIL) zugeordnet werden. Die endgültige Einstufung des sicherheitstechnischen Systems ergibt sich allerdings erst anhand der Betrachtung und Berechnung aller Teilsysteme.

4.2. Sicherheitsfunktionen

Für das Stellantriebssystem wurden zur Berechnung der sicherheitstechnischen Kennzahlen folgende Sicherheitsfunktionen berücksichtigt:

- Safe ESD AUF/ZU: sicheres ÖFFNEN/SCHLIESSEN
 - Fail-Safe-Position: Fail-Safe-Einheit fährt in der definierten Stellzeit in die konfigurierte Fail-Safe-Position (AUF/ZU).
 - Der sichere Zustand ist erreicht, wenn der FQM die angebaute Armatur in die definierte Sicherheitsendlage (AUF/ZU) gebracht hat, bzw. diese dort hält.
 - Die Sicherheitsendlage ist erreicht, wenn der FQM den internen Endanschlag oder den Armaturendanschlag in der definierten Position (AUF/ZU) erreicht hat.
- Sichere Endlagenrückmeldung
 - Fail-Safe-Position: Die Fail-Safe-Position kann je nach Anwendung unterschiedlich sein. Daher kann keine Fail-Safe-Position definiert werden. Ein unerwartetes Wegschaltersignal kann gefährlich sein.

Die Safe ESD Funktion kann je nach Konfiguration entweder durch ein Signal (Eingang $E_{SD} = 0 \text{ V DC}$) oder durch Netzausfall ausgelöst werden.

Die verschiedenen Konfigurationsmöglichkeiten der Sicherheitsfunktionen sind im Kapitel <Konfiguration (Einstellung)/Ausführung> beschrieben.

Das Ausführen der Sicherheitsfunktion „Sicheres ÖFFNEN/SCHLIESSEN“ kann nicht unterbrochen werden.

Die Sicherheitsfunktion „Sicheres ÖFFNEN/SCHLIESSEN“ ist nur verfügbar, wenn die Meldung „FS-Ready“ vorliegt. Die Anforderung der Sicherheitsfunktion führt zum Erlöschen der Meldung „FS-Ready“. Für das Meldeverhalten der Ausgänge FS Ready NO/FS Failure NC, siehe Kapitel <Installation>.

Die Stellzeit der Fail-Safe-Einheit ist für eine Belastung gemäß EN15714-2 für einen 90° Schwenkwinkel definiert worden. Bei abweichenden Belastungen oder Veränderung des Schwenkwinkels ist diese neu zu ermitteln.

Im Falle eines Fehlers des Stellantriebs, der zu einer Bewegung entgegen der Fail-Safe Richtung führt, kann sich die Fail-Safe Stellzeit um die Laufzeit des Stellantriebs verlängern.

Die Sicherheitsfunktion „Sichere Endlagenrückmeldung“ ist unabhängig von der Meldung „FS-Ready“ vorhanden.

Die Sicherheitsfunktion „Sichere Endlagenrückmeldung“ und die Sicherheitsfunktion „Sicheres ÖFFNEN/SCHLIESSEN“ sind gleichzeitig verfügbar.

In jeder Fail-Safe Einheit ist immer nur eine der Sicherheitsfunktionen „Sicheres ÖFFNEN“ und „Sicheres SCHLIESSEN“ verfügbar.

4.3. Sichere Ein- und Ausgänge

Sicherer Eingang für sicheres ÖFFNEN/SCHLIESSEN (Safe ESD Funktion):

- ESD

Sichere Ausgänge:

- FS Failure NC (Sicherheitsfunktion bereit/nicht bereit)
- FS Ready NO (Sicherheitsfunktion bereit/nicht bereit)
- LSO 19-20=NC (Sichere Endlagenrückmeldung AUF)
LSO 19-21=NO (Sichere Endlagenrückmeldung AUF)
- LSC 22-23=NC (Sichere Endlagenrückmeldung ZU)
LSC 22-24=NO (Sichere Endlagenrückmeldung ZU)

Weitere Informationen zu den sicheren Ein- und Ausgängen siehe Kapitel <Konfiguration (Einstellung)/Ausführung> und Kapitel <Installation>.

4.4. Redundanter Systemaufbau

Neben dem bereits beschriebenen typischen sicherheitstechnischen System mit einem Stellantrieb kann zur weiteren Erhöhung der Sicherheit auch ein zweiter, redundanter Stellantrieb mit Fail-Safe-Einheit in Ausführung SIL in das sicherheitstechnische System eingebaut werden. Welche Variante gewählt werden muss ist vom Gesamtsystem abhängig. Mit den hier abgebildeten, redundanten

Systemaufbauten erreicht der Stellantrieb mit Stellantriebs-Steuerung und Fail-Safe-Einheit gemäß IEC 61508 die Sicherheitsanforderungsstufe SIL 3 für die Safe ESD Funktion.

Bild 3: Redundantes System mit Safe ESD für sicheres SCHLIESSEN



Bild 4: Redundantes System mit Safe ESD für sicheres ÖFFNEN



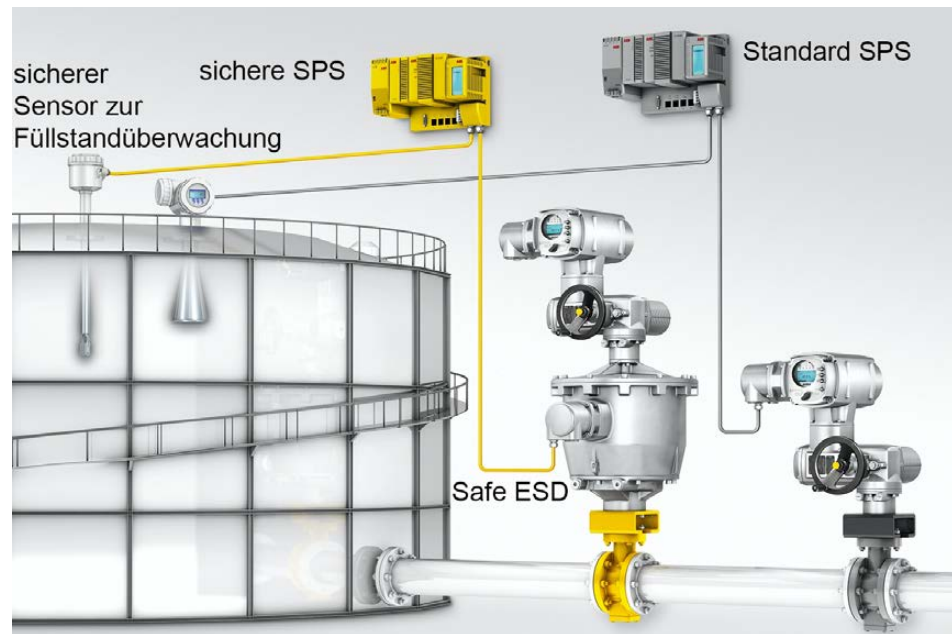
Information Ein redundantes System für sichere Endlagenrückmeldung kann nicht sinnvoll mit zwei Fail-Safe-Einheiten aufgebaut werden.

4.5. Anwendungsbeispiele

Sicheres SCHLIESSEN eines Tanklagers mit der Safe ESD Funktion

Die Standard SPS steuert das gesamte System zum Befüllen des Tanks. Wenn der Füllstand oder der Druck im Tank unzulässig hoch wird, muss von einem Fehler im System ausgegangen werden. In diesem Falle schließt die sichere SPS sofort das Ventil zum Befüllen des Tanks.

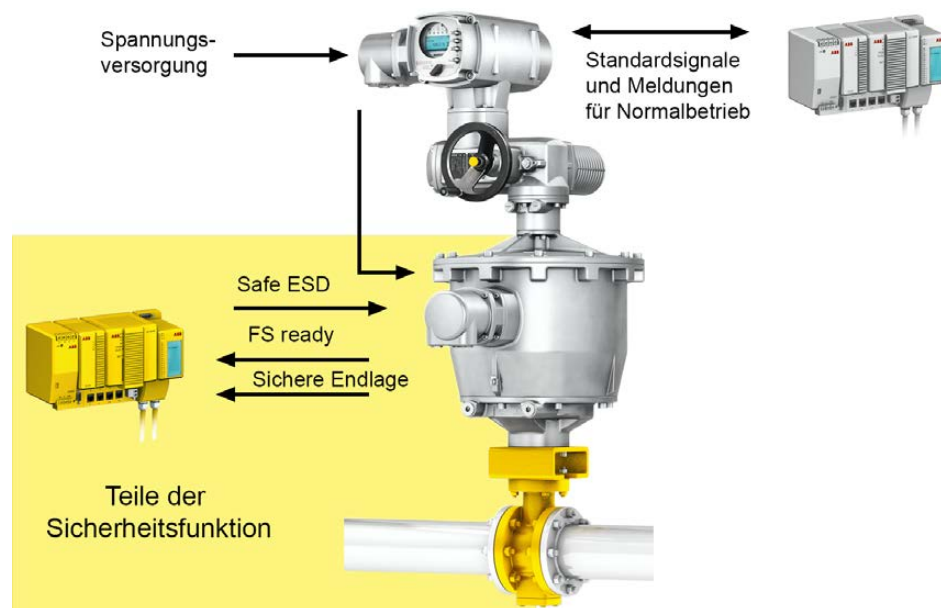
Bild 5: Anwendungsbeispiel: Überfüllschutz Tanklager



4.6. Systemdarstellung

Die folgende Darstellung stellt einen vereinfachten Aufbau einer Fail-Safe-Einheit in Ausführung SIL dar.

Bild 6: Vereinfachte Systemdarstellung



4.7. Diagnosefunktion durch den Betreiber

Zusätzlich zu den bereits in der Fail-Safe-Einheit vorhandenen internen Diagnosen sind weitere Diagnosen durch die Sicherheits-SPS erforderlich. Bei Erkennung eines Fehlers muss das System umgehend überprüft, und die Anlage ggf. in den sicheren Zustand gebracht werden.

Bei folgenden Punkten ist von einem Fehler des FQM auszugehen. Diese müssen von der Sicherheits-SPS permanent überwacht werden:

- wenn ausgehend vom normalen Betriebszustand der Fail-Safe-Einheit (Meldung „FS-Bereit“ und Eingang ESD High-Pegel) sich die Ausgänge FS Ready NO/FS Failure NC auf Meldung „FS-Fehler“ ändern.

- wenn eine betriebliche Anforderung oder Diagnosefahrt (PVST/FVST) aus einer Endlage heraus begonnen wurde und innerhalb der jeweils vorhandenen SQ-Stellzeit der Endlagenschalter nicht freigegeben wird.
 - wenn bei der automatischen Initialisierung (Start durch Anlegen Eingang ESD High-Pegel) die maximale Initialisierungszeit (2 Minuten) überschritten wird und danach immer noch ESD High-Pegel (nicht angefordert) anliegt, sowie Meldung „FS-Fehler“ (FailSafe nicht bereit) gemeldet wird.
 - wenn ESD angefordert wird (ESD Low-Pegel) und die Sicherheitsendlage nicht innerhalb der maximal definierten Fail-Safe-Stellzeit erreicht wird, (typische Stellzeit $-50\%/+100\%$).
 - ausgehend vom normalen Betriebszustand der Fail-Safe-Einheit (Meldung „FS-Bereit“ und Eingang ESD High-Pegel) die Sicherheitsfunktion „Sicheres ÖFFNEN/SCHLIESSEN“ angefordert wird (Eingang ESD Low-Pegel) und sich der Ausgang FS Ready NO nicht innerhalb der Reaktionszeit (1 Sekunde) auf Meldung „FS-Fehler“ ändert.
- Information**
- Die Reaktionszeit auf Unterbrechung der Netzversorgung bei entsprechender Konfiguration beträgt bis zu 10 Sekunden.
 - Die Meldung „FS-Fehler“ führt nicht automatisch zum Auslösen der ESD Funktion. Sie besagt, dass nicht garantiert werden kann, dass die Sicherheitsfunktion ausgeführt werden kann. Ausnahme ist, wenn die Ursache der Meldung „FS-Fehler“ der Rollfederschalter ist oder ein Fehler im Kniehebel, der dazu führt das dieser die Feder nicht mehr verriegeln kann. In diesen beiden Fällen wird zusätzlich zur Meldung „FS-Fehler“ auch die ESD Funktion ausgelöst. Auch wenn die Ausgänge FS Ready NO/FS Failure NC einen „FS-Fehler“ melden, kann unter Umständen eine Standardfahrt in die Fail-Safe Position mit Hilfe des elektrischen Stellantriebs oder eventuell auch eine ESD Fahrt mittels Anforderung der ESD Funktion am ESD Eingang der Fail-Safe Einheit noch möglich sein.
 - Wenn eine der durch den Betreiber durchgeführten Diagnosen einen Fehler der Fail-Safe-Einheit detektieren, muss das System umgehend geprüft und die Anlage ggf. in einen sicheren Zustand gebracht werden.

4.8. Interne Diagnosen der Fail-Safe-Einheit

Die Fail-Safe-Einheit besitzt folgende interne Diagnosen:

- Eine interne Temperaturüberwachung, welche bei Abweichung von der intern zulässigen Betriebstemperatur ein Auslösen der Meldung „FS-Fehler“ bewirkt.
 - Eine interne Spannungsüberwachung des Eingangs ESD, welche bei Abweichung vom intern zulässigen Pegel ein Auslösen der Meldung „FS-Fehler“ bewirkt.
 - Eine interne Überwachung der Feder und weiterer mechanischer Komponenten, welche bei Abweichung von den als zulässig definierten Spezifikationen ein Auslösen der Meldung „FS-Fehler“ bewirkt.
 - Während der Initialisierung liegt am Eingang ESD der Pegel „high“ an und die Meldung „FS-Fehler“ ist aktiv. Eine interne Diagnosefunktion der Fail-Safe-Einheit prüft, ob alle notwendigen Bedingungen für den Abschluss der Initialisierung erfüllt sind (insbesondere: Feder vollständig gespannt, Kniehebel verriegelt). Erst wenn dies der Fall ist, wird die Meldung „FS-Fehler“ durch die Meldung „FS-Bereit“ ersetzt.
- Information**
- Die Meldung „FS-Fehler“ führt nicht automatisch zum Auslösen der ESD Funktion. Sie besagt, dass nicht garantiert werden kann, dass die Sicherheitsfunktion ausgeführt werden kann. Ausnahme ist, wenn die Ursache der Meldung „FS-Fehler“ der Rollfederschalter ist oder ein Fehler im Kniehebel, der dazu führt das dieser die Feder nicht mehr verriegeln kann. In diesen beiden Fällen wird zusätzlich zur Meldung „FS-Fehler“ auch die ESD Funktion ausgelöst.

Auch wenn die Ausgänge FS Ready NO/FS Failure NC einen „FS-Fehler“ melden kann unter Umständen eine Standardfahrt in die Fail-Safe Position mit Hilfe des elektrischen Stellantriebs oder eventuell auch eine ESD Fahrt mittels Anforderung der ESD Funktion am ESD Eingang der Fail-Safe Einheit noch möglich sein.

5. Installation, Inbetriebnahme und Betrieb

Information Installation und Inbetriebnahme muss durch einen Montagebericht und ein Abnahmeprüfzeugnis dokumentiert werden. Die Installation und Inbetriebnahme darf nur durch ausgebildetes Fachpersonal erfolgen.

Es dürfen nur Deckel oder Schrauben am Gerät geöffnet bzw. gelöst werden, für die es in diesem Handbuch oder in der Betriebsanleitung eine Beschreibung gibt.



Verletzungsgefahr durch hohe Federspannung!

In der Fail-Safe-Einheit befinden sich Federn die unter hoher Spannung stehen. Diese Federn können sich beim nicht fachgerechten Öffnen des Gehäuses unkontrolliert entspannen.

→ FQM Gehäuse NICHT öffnen.

Für die Sicherstellung der Energieversorgung mit Über- und Unterspannungsschutz ist der Anlagenbetreiber zuständig.

5.1. Installation

Die allgemeine Installation (Montage, Elektroanschluss) muss entsprechend der zum Gerät zugehörigen Betriebsanleitung und dem beigefügten, auftragsbezogenen Schaltplan durchgeführt werden.

Leitungen müssen bei der Installation so verlegt werden, dass möglichst wenig Störungen auf Signalleitungen verursacht werden (EMV-gerechte Leitungsverlegung). Hierbei sollten insbesondere folgende Punkte beachtet werden:

- Signalleitungen sind stöempfindlich. Motorleitungen sind störbehaftet. Stöempfindliche und störbehaftete Leitungen in möglichst großem Abstand zueinander verlegen.
- Signalleitungen zur Erhöhung der Störfestigkeit möglichst dicht am Massepotential verlegen.
- Lange Leitungen möglichst vermeiden oder darauf achten, dass sie in wenig gestörten Bereichen verlegt werden.
- Lange Parallelstrecken von stöempfindlichen und störbehafteten Leitungen vermeiden.

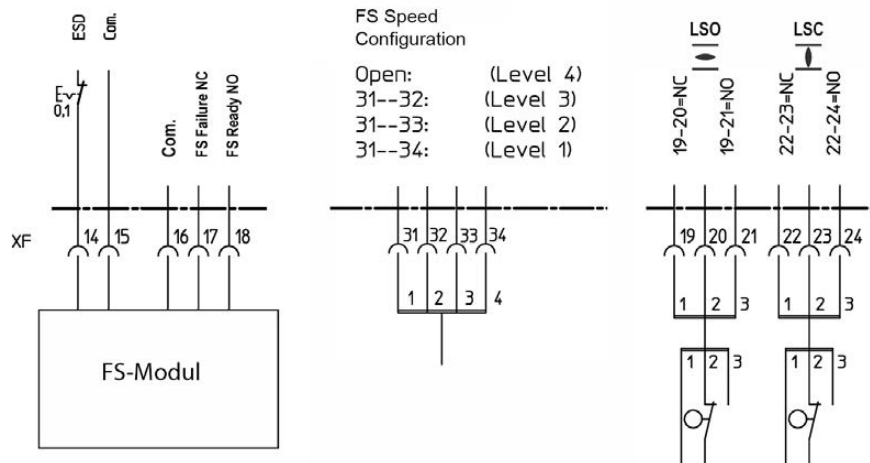
Bei Betrieb unterhalb Umgebungstemperaturen von -30 °C muss die Tieftemperaturversion verwendet werden. Das integrierte Heizsystem muss mit Spannung versorgt werden.

Die Lagerung der Fail-Safe Einheit ist bei Umgebungstemperaturen von -60 °C bis $+80\text{ °C}$ zulässig. Bei Lagerung unterhalb Umgebungstemperaturen von -40 °C muss die Tieftemperaturversion verwendet werden. Das integrierte Heizsystem muss mit Spannung versorgt werden.

Die Sicherheitsfunktionen werden über das FS-Modul, welches in der Fail-Safe-Einheit eingebaut ist, angeschlossen.

Die Ausgänge FS Failure NC und FS Ready NO müssen mit einem SIL 2 kompatiblen Eingang einer Sicherheits-SPS verbunden und ausgewertet werden.

Bild 7: Anschlüsse für Sicherheitsfunktionen über das FS-Modul



Schaltverhalten des Eingangs ESD:

- Eingangssignal = **High-Pegel** (Standard: +24 V DC)
= **Keine** Sicherheitsfahrt bei Safe ESD Funktion
- Eingangssignal = **Low-Pegel** (0 V DC bzw. Eingang offen)
= Sicherheitsfahrt bei Safe ESD Funktion

Zulässiger Spannungsbereich der Eingänge:

- High-Pegel: +24 V DC (-15 %/+20 %)
Stromaufnahme ca. 1 A, max. 1,2 A
- Low-Pegel: maximal 5 V DC

Meldeverhalten des Ausgangs FS Ready NO/FS Failure NC:

- Die Safe ESD Funktion ist bereit, es liegt kein von den Diagnosen detektierter Fehler an:
Ausgang FS Ready NO (Schließer-Kontakt) = **geschlossen**
Ausgang FS Failure NC (Öffner-Kontakt) = **offen**
- Die Safe ESD Funktion ist NICHT bereit, oder es wurde ein Fehler detektiert:
Ausgang FS Ready NO (Schließer-Kontakt) = **offen**
Ausgang FS Failure NC (Öffner-Kontakt) = **geschlossen**

Meldeverhalten der Ausgänge LS:

- Meldung **Endlage AUF erreicht** (Klemmen XF 19 – 21) oder **Endlage ZU erreicht** (Klemmen XF 22 – 24), d.h.:
Ausgang an Klemmen XF 19-21=NO bzw. XF 22-24=NO (Schließer-Kontakt) = **geschlossen**
Ausgang an Klemmen XF 19-20=NC bzw. XF 22-23=NC (Öffner-Kontakt) = **offen**

Zulässige Belastung der Ausgänge FS Ready NO und LSO/LSC:

- Spannungsbereich: 5 – 30 V
- Strombereich 2 – 100 mA

Tabelle 5: Beispiel (siehe Schaltplan zum Auftrag)

Bezeichnung Schaltplan	Signal	Kundenanschlüsse
ESD	Digitaler Eingang für Safe ESD Funktion	XF 14
Com.	Bezugspotential für Safe ESD	XF 15
FS Ready NO	Schließer-Kontakt der Meldung FS-Bereit/FS-Fehler	XF 18
FS Failure NC	Öffner-Kontakt der Meldung FS-Bereit/FS-Fehler	XF 17
FS Ready Com.	Bezugspotential für die Meldung FS-Bereit/FS-Fehler	XF 16
LSO 19-20=NC	Öffner-Kontakt der Meldung LSO (Endlage AUF)	XF 20
LSO 19-21=NO	Schließer-Kontakt der Meldung LSO (Endlage AUF)	XF 21
	Bezugspotential für die Meldung LSO	XF 19

Bezeichnung Schaltplan	Signal	Kundenanschlüsse
LSC 22-24=NO	Schließer-Kontakt der Meldung LSC (Endlage ZU)	XF 24
LSC 22-23=NC	Öffner-Kontakt der Meldung LSC (Endlage ZU)	XF 23
	Bezugspotential für die Meldung LSC	XF 22

Weitere Informationen zu FS-Fehlern und insbesondere zur Unterstützung bei der Fehlersuche siehe Kapitel <Meldungen> und die Betriebsanleitung Fail-Safe-Einheit FQM 05.1 – FQM 12.1/FQMEx 05.1 – FQMEx 12.1.

5.2. Inbetriebnahme

Für die allgemeine Inbetriebnahme muss die zum Gerät zugehörige Betriebsanleitung beachtet werden.

- Information** Eine falsche bzw. ungenaue Einstellung der Endanschläge in der Fail-Safe-Einheit oder der Wegenschaltung im Stellantrieb kann zu folgenden Fehlern führen:
- kein vollständiges Schließen der Armatur (wenn der Endanschlag des FQM zu früh erreicht wird)
 - keine Endlagenrückmeldung trotz geschlossener Armatur (da Wegschalter noch nicht betätigt)

- Information** Bei der Safe ESD Funktion ist eine Fahrt in die sichere Position bei aufgezogener Feder unabhängig von Einstellungen oder dem Betriebszustand des elektrischen Stellantriebs möglich. D.h. die Fail-Safe-Einheit kann durch Auslösen der Sicherheitsfunktion jederzeit losfahren.

Am Ende der Inbetriebnahme muss eine Überprüfung der sicheren Funktion erfolgen. Diese Überprüfung kann unter Anwendung des Proof-Test durchgeführt werden. Siehe Kapitel <Proof-Test (Überprüfung auf sichere Funktion des Stellantriebs)>.

5.3. Betrieb

Voraussetzung für einen sicheren Betrieb ist die regelmäßige Wartung und die Überprüfung des Gerätes in den vom Betreiber festzulegenden T_{proof} Intervallen. Die im Kapitel <Sicherheitstechnische Kennzahlen> angegebenen Kennzahlen gelten für einen $T_{proof} = 1$ Jahr.

Für den Betrieb muss die zum Gerät zugehörige Betriebsanleitung beachtet werden.

Bei möglichen Störungen bzw. Defekten des Sicherheitssystems muss die sichere Funktion über einen anderen Weg gewährleistet werden. Desweiteren muss ein festgestellter Fehler zusammen mit einer Fehlerbeschreibung der AUMA Riester GmbH & Co. KG gemeldet werden. Eigenständige Reparaturarbeiten des Anlagenbetreibers sind nicht zulässig.

5.4. Lebensdauer

Die Lebensdauer der Stellantriebe ist in den technischen Daten bzw. in der Betriebsanleitung beschrieben.

Die sicherheitsbezogenen Kennzahlen gelten für die in den technischen Daten festgelegten Zyklen bzw. Regelschritte und für einen Zeitraum von typischerweise bis zu 10 Jahren (das zuerst erreichte Kriterium zählt). Danach steigt die Ausfallwahrscheinlichkeit an.

Eine Verlängerung dieses Zeitraums „durch entsprechende Maßnahmen des Herstellers und Betreibers“ gemäß der nationalen Fußnote NOTE 3 zur ANMERKUNG 3 der deutschen Fassung der IEC 61508-2:2010 7.4.9.5 b) ist in vielen Fällen grundsätzlich möglich. Dies liegt in der Verantwortung des Betreibers der geeignete Maßnahmen zu ergreifen hat. In jedem Fall müssen diese Maßnahmen einen Service durch die AUMA Riester GmbH & Co. KG beinhalten.

5.5. Außerbetriebsetzung

Falls der Stellantrieb mit Sicherheitsfunktion außer Betrieb gesetzt wird, muss folgendes beachtet werden:

- Der Einfluss der Außerbetriebsetzung auf zugehörige Geräte, Einrichtungen oder andere Arbeiten muss evaluiert werden.
- Die Sicherheits- und Warnhinweise der zum Stellantrieb gehörenden Betriebsanleitung müssen eingehalten werden.
- Die Außerbetriebsetzung darf nur durch ausgebildetes Fachpersonal erfolgen.
- Die Außerbetriebsetzung muss sachgerecht dokumentiert werden.
- Die Außerbetriebsetzung darf nur in der FQM-Fail-Safe-Endlage (Feder entspannt) vorgenommen werden.



Verletzungsgefahr durch hohe Federspannung!

In der Fail-Safe-Einheit befinden sich Federn die unter hoher Spannung stehen. Diese Federn können sich beim nicht fachgerechten Öffnen des Gehäuses unkontrolliert entspannen.

→ FQM Gehäuse NICHT öffnen.

5.6. Entsorgung und Recycling

Unsere Geräte sind Produkte mit einer langen Lebensdauer. Jedoch kommt auch hier der Zeitpunkt an dem sie ersetzt werden müssen. Die Geräte sind modular aufgebaut und können dadurch gut stofflich getrennt und sortiert werden nach:

- verschiedenen Metallen
- Kunststoffe
- Fette und Öle

Generell gilt:

- Fette und Öle sind in der Regel wassergefährdende Stoffe, die nicht in die Umwelt gelangen dürfen.
- Demontiertes Material einer geregelten Entsorgung bzw. der getrennten stofflichen Verwertung zuführen.
- Nationale Entsorgungsvorschriften beachten.

6. Anzeigen

Anzeigen der Stellantriebs-Steuerung, die nur in der Ausführung mit Fail-Safe-Einheit möglich sind, sind in der Betriebsanleitung zur FQM beschrieben.

Allgemeine Anzeigen und deren Einstellung bzw. Bedienung sind in der zum Stellantrieb zugehörige Betriebsanleitung, sowie im Handbuch (Betrieb und Einstellung) der Stellantriebs-Steuerung AC 01.2/ACExC 01.2 beschrieben.

Information Anzeigen über das Display sind NICHT Teil einer Sicherheitsfunktion! Sie dürfen nicht in ein sicherheitsbezogenes System integriert werden!

Die Anzeigen unterstützen den Anwender vor Ort am Gerät, um den Status der Sicherheitsfunktionen leichter zu erkennen.

7. Meldungen

7.1. Meldungen über das FS-Modul

Das integrierte FS-Modul meldet über ein Melderelais (Ausgänge FS Ready NO bzw. FS Failure NC) einen Fail-Safe-Fehler. Nur diese Signale dürfen in einem sicherheitsbezogenen System verwendet werden.

Für das Meldeverhalten der Ausgänge FS Ready NO/FS Failure NC und der Endlagenmeldungen über die Ausgänge LS siehe Kapitel <Installation>.

Bei einem Fail-Safe-Fehler muss das System umgehend überprüft, und die Anlage ggf. in den sicheren Zustand gebracht werden.

7.2. Zustandsmeldungen über Melderelais (digitale Ausgänge) der Stellantriebs-Steuerung

Information

Die Stellantriebs-Steuerung bietet die Möglichkeit, Statusinformationen zu den sicherheitsbezogenen Funktionen über Melderelais zu melden (Ausgänge DOUT).

Zustandsmeldungen über die Ausgänge DOUT sind nicht Teil einer Sicherheitsfunktion! Sie dürfen nicht in ein sicherheitsbezogenes System integriert werden! Sie können z.B. als zusätzliche Information über die Standard SPS verwendet werden.

Die verfügbaren Signale und ihre Bedeutung sind in der Betriebsanleitung zur Fail-Safe-Einheit beschrieben.

7.3. Meldungen über Feldbus der Stellantriebs-Steuerung

Information

Bei Stellantriebs-Steuerungen in Ausführung mit Feldbus Schnittstelle werden die Statusinformationen zu den sicherheitsbezogenen Funktionen im Prozessabbild zur Verfügung gestellt.

Zustandsmeldungen über den Feldbus sind nicht Teil einer Sicherheitsfunktion! Sie dürfen nicht in ein sicherheitsbezogenes System integriert werden. Sie können z.B. als zusätzliche Information über die Standard SPS verwendet werden.

Die verfügbaren Signale und ihre Bedeutung sind in der Betriebsanleitung zur Fail-Safe-Einheit beschrieben.

8. Prüfungen und Wartung

Prüfung- und Wartungsarbeiten dürfen nur durch autorisiertes Fachpersonal durchgeführt werden, das in Funktionaler Sicherheit geschult ist.

Die Prüfungs- und Wartungsmittel müssen kalibriert sein.

Die Fail-Safe-Einheit ist innerhalb der im Kapitel <Lebensdauer> genannten Lebensdauer von 10 Jahren bzw. der dort genannten maximalen Anzahl an Zyklen oder Regelschritten wartungsfrei. Es müssen jedoch die notwendigen Prüfungen (insbesondere Proof-Test und Online-Diagnosen) in den festgelegten Intervallen und in Einklang mit den in diesem Sicherheitshandbuch beschriebenen Vorgehensweisen und zeitlichen Abständen durchgeführt werden.

Information Die Durchführung einer Prüfung/Wartung muss durch einen Prüf-/Wartungsbericht dokumentiert werden.

Der Einfluss der Prüfung/Wartung auf zugehörige Geräte, Einrichtungen oder andere Arbeiten muss evaluiert werden.

8.1. Sicherheitseinrichtung überprüfen

Sämtliche Schutzfunktionen in einer Sicherheitseinrichtung müssen in angemessenen Intervallen auf ihre Funktionsfähigkeit und Sicherheit überprüft werden. Die Intervalle für die Überprüfung der Sicherheitseinrichtung muss der Betreiber festlegen.

Um systematische Fehler zu vermeiden, muss der Anlagenbetreiber eine Sicherheitsplanung für den gesamten Sicherheitslebenszyklus des SIS vornehmen. Darin sollten z.B. die Politiken und Strategien zum Erreichen der Sicherheit und die verschiedenen Tätigkeiten während des Sicherheitslebenszykluses genannt sein.

8.2. Interne Antriebsüberwachung des Gerätes mit Ansteuerung über die Stellantriebs-Steuerung

Das Gerät, bestehend aus Stellantrieb mit Stellantriebs-Steuerung und Fail-Safe-Einheit, verfügt über eine interne Antriebsüberwachung. Durch das Fahren im Normalbetrieb über den Stellantrieb, aus einer Endlage heraus¹⁾, wird die interne Antriebsüberwachung automatisch ausgeführt. Die interne Antriebsüberwachung diagnostiziert einen Großteil der sicherheitsbezogenen Komponenten der Fail-Safe-Einheit und würde in einem Fehlerfall einen Fehler über das Melderlais des FS-Moduls (Ausgänge FS Ready NO und FS Failure NC) signalisieren.

Um die in Kapitel <Sicherheitstechnische Kennzahlen> genannten, beispielhaften Sicherheitskennzahlen, insbesondere PFD, der Sicherheitsfunktion Safe ESD zu gewährleisten, muss das Gerät mindestens einmal pro Monat über die Stellantriebs-Steuerung angesteuert und zusätzlich das Melderlais des FS-Moduls (Ausgänge FS Ready NO und FS Failure NC) ausgewertet werden. Von der Sicherheits-SPS muss überprüft werden, ob der Endlagenschalter erwartungsgemäß die Abfolge "Endlage -> keine Endlage -> Endlage" signalisiert. Kann nicht gewährleistet werden, dass das Gerät mindestens einmal pro Monat über die Stellantriebs-Steuerung angesteuert wird, muss statt dessen ein <Partial Valve Stroke Test (PVST)> durchgeführt werden.

Das Ansteuerungssignal und die damit verbundene Fahrt des Stellantriebs muss so lang anstehen dass gewährleistet ist, dass der Endlagenschalter das Verlassen der Endlage signalisiert.

Da die Diagnosefunktion nicht rein intern im FQM erfolgt, sondern von der Sicherheits-SPS angestoßen und/oder ausgewertet werden muss, sind auch andere Diagnose-Testintervalle als 1x pro Monat möglich. Dies hat jedoch zur Folge, dass sich die sicherheitstechnischen Kennzahlen, insbesondere die PFD ändern wird. Ferner ist bei der Wahl des Diagnose-Testintervalls durch den Betreiber zu bedenken, dass die Testfrequenz mindestens dem 10-fachen der Anforderungsrate entsprechen sollte und dass - für die Sicherheitsfunktion ESD - das Testintervall niemals unter 22 Tage betragen kann (siehe nächster Absatz).

Um übermäßigen Verschleiß zu vermeiden, sind die internen Diagnosen der mechanischen Elemente so aufgebaut, dass sie auch bei häufigeren betrieblichen Fahrten maximal alle 22 Tage durchgeführt werden. Um ein Testintervall z.B. von einem Monat zu gewährleisten, muss der Betreiber sicherstellen, dass 22 Tage bis

1) (Ausgang LiSC bzw. LSO öffnet)

1 Monat nach der letzten Diagnosefahrt eine betriebliche Fahrt oder ein PVST aus einer Endlage heraus erfolgt.

Ein FVST (Full Valve Stroke Test) oder eine betriebliche Fahrt kann den PVST ersetzen, vorausgesetzt die Fahrt wird an die Sicherheits-SPS gemeldet und die Sicherheits-SPS wird in eine entsprechende Erwartungshaltung gebracht.

Wenn eine sichere Endlagenrückmeldung für beide Endlagen gefordert wird, muss der PVST aus beiden Endlagen heraus gestartet werden. Ein FVST kann alternativ für diese Prüfung verwendet werden.

8.3. Partial Valve Stroke Test (PVST) durchführen

Der Ablauf des PVST ist für beide Sicherheitsfunktionen identisch.

Der PVST kann auf zwei verschiedene Arten durchgeführt werden.

1. **Durchführung PVST unter Verwendung der Standardfunktionen der AC .2:**
Der Stellantrieb wird im Normalbetrieb über die Standard-SPS und die AC .2 angesteuert. Für den PVST wird die Fahrabfolge „Endlage -> keine Endlage -> Endlage“ durchgeführt. Während der Fahrt überwacht die Sicherheits-SPS folgende Zustände bzw. Ereignisse:
 - Befindet sich der Stellantrieb zu Beginn des PVST in einer der beiden Endlagen?. Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
 - Beginnt der PVST, bzw. wird die Sicherheits-SPS über den Start des PVST durch die Standard-SPS oder die AC .2 informiert?
 - Bewegt sich der Stellantrieb innerhalb der eingestellten PVST Fahrzeit aus der Endlage heraus? Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
 - Befindet sich der Stellantrieb am Ende wieder in der ursprünglichen Endlage? Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
 - Wird während der PVST Fahrzeit ein Fehler über das Melderelais (FS-Modul: FS Ready NO/FS Failure NC) gemeldet?

2. **Durchführung des PVST unter Verwendung der PVST-Funktion der AC .2:**
Ist die AC .2 mit einem PVST-Eingang konfiguriert, so kann auch dieser unter bestimmten Umständen für die Diagnose des sicherheitsrelevanten Teils der Steuerung verwendet werden.

Voraussetzungen und notwendige Einstellungen:

- Ein digitaler Eingang (von den anderen Eingängen galvanisch getrennt) der Stellantriebs-Steuerung ist auf folgenden Wert konfiguriert: **PVST ausführen** (949)
- Die Sicherheits-SPS steuert den PVST-Eingang direkt an oder erhält ebenfalls das Steuersignal, wenn der PVST-Eingang angesteuert wird.
- Der PVST erfolgt unter folgender Einstellung der Betriebsart: Parameter **PVST Betriebsart M0889 = Endlagenprüfung**
- Der PVST darf nur aus einer der beiden Endlagen heraus erfolgen.
- Der Parameter **PVST Fahrzeit M0890** muss so eingestellt werden, dass die Endlage sicher verlassen wird.

Während die AC .2-Stellantriebs-Steuerung den PVST durchführt, überwacht die Sicherheits-SPS folgende Zustände bzw. Ereignisse:

- Befindet sich der Stellantrieb zu Beginn des PVST in einer der beiden Endlagen? Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
- Beginnt der PVST, bzw. wird die Sicherheits-SPS über den Start des PVST durch die Standard-SPS oder die AC .2 informiert?
- Bewegt sich der Stellantrieb innerhalb der eingestellten PVST Fahrzeit aus der Endlage heraus? Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
- Befindet sich der Stellantrieb am Ende wieder in der ursprünglichen Endlage? Die Kontrolle erfolgt über die sichere Endlagenrückmeldung der FQM.
- Wird während der PVST Fahrzeit ein Fehler über das Melderelais (FS-Modul: FS Ready NO/FS Failure NC) gemeldet?

Für beide Durchführungsarten gilt: **Der PVST war erfolgreich, wenn Folgendes erfüllt ist:**

- Der Stellantrieb war zu Beginn des PVST in einer Endlage.
- Der Stellantrieb hat sich während des PVST aus dieser Endlage heraus bewegt.
- Der Stellantrieb befindet sich am Ende des PVST in der gleichen Endlage wie vor dem PVST.
- Das FS-Modul hat **keinen** Fehler über das Melderelais (FS Ready NO/FS Failure NC) gemeldet.

Wir empfehlen auch die Meldungen **PVST Fehler** (953) und **PVST Abbruch** (954) der Stellantriebs-Steuerung auszuwerten. Dies muss nicht notwendigerweise durch die Sicherheits-SPS erfolgen.

Sollte dies nicht der Fall sein, muss das Gerät nach den in Kapitel <Proof-Test> genannten Schritten überprüft werden.

8.4. Proof-Test (Überprüfung auf sichere Funktion des Stellantriebs)

Mit dem Proof-Test werden die sicherheitsbezogenen Funktionen des Stellantriebs und der Stellantriebs-Steuerung geprüft.

Der Proof-Test soll gefährliche Fehler aufdecken, die sonst bis zum Auslösen einer Sicherheitsfunktion unentdeckt bleiben und dann zu einer Gefahr werden könnten.

Information Während der Durchführung des Proof-Tests steht die Sicherheitsfunktion kurzzeitig nicht zur Verfügung.

Vor Beginn der unten beschriebenen Proof-Test Prozedur/Prozeduren müssen folgende Vorprüfungen durchgeführt werden:

- Sichtprüfung auf übermäßige Korrosion und mögliche Schäden.

- Prüfen und ggf. Nachziehen aller Schrauben der Verbindung zwischen der Fail-Safe Einheit FQM und dem Schwenkantrieb SQ. Anzugsmoment: FQM 5.1/7.1: 24 Nm, FQM 10.1/12.1: 82 Nm

Der Proof-Test beinhaltet je nach Ausführung und Konfiguration folgende Prüfungen:

1. Safe ESD Sicherheitsfahrt (sicheres ÖFFNEN/SCHLIESSEN) prüfen.
2. Fail-Safe-Fehlermeldung prüfen.
3. Safe ESD Reaktion auf „sichere Endlagenrückmeldung“ prüfen (Auswertung Endlagenschalter).

Zur Prüfung der Sicherheitsfunktion wird der sicherheitsbezogene Signaleingang entsprechend beschaltet. Der Stellantrieb muss in der Folge die Sicherheitsfunktion ausführen. Die genaue Durchführung der genannten Proof-Test-Schritte ist in den folgenden Unterkapiteln beschrieben.

Intervalle:

Ein Proof-Test-Intervall beschreibt die Zeit zwischen zwei Proof-Tests. Die Funktionsfähigkeit muss in angemessenen Intervallen überprüft werden. Die Intervalle muss der Betreiber festlegen. Die Sicherheitskennzahlen sind abhängig von dem gewählten Proof-Test-Intervall (siehe Kapitel <Sicherheitstechnische Kennzahlen>).

In jedem Fall müssen nach der Inbetriebnahme und nach jeder Wartung oder Reparatur nach Änderung der Fail-Safe Stellzeit, sowie bei den in der Sicherheitsbetrachtung festgelegten T_{proof} Intervallen die sicherheitsbezogenen Funktionen überprüft werden.

Ergibt sich ein Fehler während des Proof-Tests muss die sichere Funktion auf einem anderen Weg gewährleistet und die AUMA Riester GmbH & Co. KG kontaktiert werden.

Welcher Proof-Test durchgeführt werden muss, ist abhängig von der Ausführung und Konfiguration des Produktes. Es müssen nur die zutreffenden Tests durchgeführt werden.

Information Bevor mit einer Prüfung begonnen wird, empfehlen wir den entsprechenden Prüfablauf einmal komplett durchzulesen.

8.4.1. ESD Fahrt (sicheres ÖFFNEN/SCHLIESSEN) prüfen

- Konfiguration** Diese Prüfung gilt für alle Ausführungen mit Safe ESD Funktion.
- Prüfverfahren** Es muss eine Sicherheitsfahrt in Richtung der konfigurierten Fail-Safe-Position ausgelöst werden.
- Prüfablauf**
1. Stellantrieb in Endlage AUF (Safe ESD in Richtung ZU), bzw. in Endlage ZU (Safe ESD in Richtung AUF) fahren.
Information: Fahrbefehle (in Richtung AUF oder ZU) können für den Test sowohl von Fern (über die Leittechnik) als auch direkt vor Ort an der Stellantriebs-Steuerung (über die Drucktaster der Ortssteuerstelle) ausgeführt werden.
- ➔ Es darf **keine** Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“).

2. Sicherheitsfahrt auslösen:
 - Dazu Eingangssignal $\overline{\text{ESD}}$ auf 0 V (Low) setzen.
 - Bei Verlassen der Endlage Stellzeitmessung starten.
 - ➔ Der FQM Endlagenschalter zeigt durch Signaländerung das Verlassen der Endlage an.
 - ➔ Es muss eine Fail-Safe-Fehlermeldung erfolgen (Meldung "FS-Fehler").
 - Bei Erreichen der Fail-Safe-Endlage Stellzeitmessung stoppen.
 - ➔ Der FQM Endlagenschalter zeigt durch Signaländerung das Erreichen der Endlage an.
 - ➔ Die Stellzeit der FQM muss der Angabe auf dem Typenschild für 90° Schwenkwinkel entsprechen, oder der ermittelten Zeit bei der Inbetriebnahme. Die zulässige Toleranz der Stellzeit beträgt $-50 \%/+100 \%$.
 - Prüfen ob die Armatur vollständig geschlossen ist.
3. Nach der Prüfung Eingangssignal $\overline{\text{ESD}}$ auf +24 V DC (High) setzen.
 - ➔ Der FQM startet die automatische Initialisierung (Feder wird gespannt).
 - ➔ Bei erfolgreicher Initialisierung erfolgt nach Abschluss der Initialisierung die Meldung „FS-Bereit“. Die Initialisierungszeit muss dazu < 2 Minuten sein.

8.4.2. ESD Fahrt (sicheres ÖFFNEN/SCHLIESSEN) mit zusätzlicher Netzauslösung prüfen

Konfiguration	Diese Prüfung gilt zusätzlich für alle Ausführungen mit zusätzlicher Netzauslösung der Sicherheitsfunktion.
Prüfverfahren	Es muss eine weitere Sicherheitsfahrt in Richtung der konfigurierte Fail-Safe-Position über die Netzspannung ausgelöst werden.
Prüfablauf	<ol style="list-style-type: none"> 1. Stellantrieb in Endlage AUF (Safe ESD in Richtung ZU), bzw. in Endlage ZU (Safe ESD in Richtung AUF) fahren. Information: Fahrbefehle (in Richtung AUF oder ZU) können für den Test sowohl von Fern (über die Leittechnik) als auch direkt vor Ort an der Stellantriebs-Steuerung (über die Drucktaster der Ortssteuerstelle) ausgeführt werden. <ul style="list-style-type: none"> ➔ Es darf keine Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“). 2. Sicherheitsfahrt auslösen: <ul style="list-style-type: none"> → Dazu Spannungsversorgung der FQM unterbrechen. Information: Die Reaktionszeit auf eine Unterbrechung beträgt bis zu 10 Sekunden. → Bei Verlassen der Endlage Stellzeitmessung starten. ➔ Der FQM Endlagenschalter zeigt durch Signaländerung das Verlassen der Endlage an. ➔ Es muss eine Fail-Safe-Fehlermeldung erfolgen (Meldung "FS-Fehler"). → Bei Erreichen der Fail-Safe-Endlage Stellzeitmessung stoppen. ➔ Der FQM Endlagenschalter zeigt durch Signaländerung das Erreichen der Endlage an. ➔ Die Stellzeit der FQM muss der Angabe auf dem Typenschild für 90° Schwenkwinkel entsprechen, oder der ermittelten Zeit bei der Inbetriebnahme. Die zulässige Toleranz der Stellzeit beträgt $-50 \%/+100 \%$. → Prüfen ob die Armatur vollständig geschlossen ist.

3. Nach der Prüfung Spannungsversorgung der FQM wieder anlegen.
 - ➔ Der FQM startet die automatische Initialisierung (Feder wird gespannt).
 - ➔ Bei erfolgreicher Initialisierung erfolgt nach Abschluss der Initialisierung die Meldung „FS-Bereit“. Die Initialisierungszeit muss dazu < 2 Minuten sein.

8.4.3. Sichere Endlagenmeldung prüfen

- | | |
|----------------------|---|
| Konfiguration | Diese Prüfung gilt für die Konfigurationen "SIL-Funktion" = " Sichere Endlagenrückmeldung ". |
| Prüfverfahren | Die Endlage muss unmittelbar gemeldet werden, wenn der Stellantrieb die Endlage erreicht. |
| Prüfablauf | <ol style="list-style-type: none">1. FQM über Stellantrieb in Zwischenstellung fahren.<ul style="list-style-type: none">→ Endlagenschalter des FQM prüfen:<ul style="list-style-type: none">➔ Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen- Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen➔ Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen- Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen➔ Es darf keine Fail-Safe-Fehlermeldung erfolgen (Meldung „FS-Bereit“).2. Fahrbefehl in Richtung ZU starten.<ul style="list-style-type: none">→ Warten bis FQM Endlagenschalter auslöst bzw. Endlage ZU erreicht ist.→ Reaktion des Stellantriebs prüfen:<ul style="list-style-type: none">→ Fahrt wurde bei Erreichen des Endlagenschalters ZU gestoppt?➔ Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen- Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen➔ Meldung Endlage ZU erreicht (Ausgangssignal aktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSC 22-23=NC (Öffner-Kontakt) = offen- Ausgang LSC 22-24=NO (Schließer-Kontakt) = geschlossen➔ Es darf keine Fail-Safe-Fehlermeldung (Meldung „FS-Bereit“) erfolgen.3. Fahrbefehl in Richtung AUF starten. Dabei Stellzeit für den Fahrweg von ZU nach AUF messen.<ul style="list-style-type: none">→ Warten bis FQM Endlagenschalter auslöst bzw. Endlage AUF erreicht ist.→ Reaktion des Stellantriebs prüfen:<ol style="list-style-type: none">3.1 Fahrt wurde bei Erreichen des Endlagenschalters AUF gestoppt?<ul style="list-style-type: none">➔ Meldung Endlage AUF erreicht (Ausgangssignal aktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSO 19-20=NC (Öffner-Kontakt) = offen- Ausgang LSO 19-21=NO (Schließer-Kontakt) = geschlossen➔ Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.:<ul style="list-style-type: none">- Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen- Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen➔ Es darf keine Fail-Safe-Fehlermeldung erfolgen (Meldung „FS-Bereit“).3.2 Die gemessene Stellzeit für die Fahrt von Endlage ZU nach Endlage AUF entsprach der Einstellung des Stellantriebs SQ? |

4. FQM über Stellantrieb in Zwischenstellung fahren.
 - Endlagenschalter des FQM prüfen:
 - ➔ Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.:
 - Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen
 - Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen
 - ➔ Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.:
 - Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen
 - Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen
 - ➔ Es darf **keine** Fail-Safe-Fehlermeldung erfolgen (Meldung „FS-Bereit“).

8.5. Wartung

Wartungs- und Servicearbeiten dürfen nur durch autorisiertes Fachpersonal durchgeführt werden, das in Funktionaler Sicherheit geschult ist.

Nach Wartungs- und Servicearbeiten ist zusätzlich zur Funktionsprüfung eine Validierung der Sicherheitsfunktion, die mindestens alle unter den Kapiteln <Sicherheitseinrichtung überprüfen> und <Proof-Test (Überprüfung auf sichere Funktion des Antriebs)> beschriebenen Prüfungen enthält, unbedingt erforderlich.

Falls bei der Wartung ein Fehler festgestellt wird, muss dieser an die AUMA Riester GmbH & Co. KG gemeldet werden.

9. Sicherheitstechnische Kennzahlen

9.1. Bestimmung der Kennzahlen

- Bei der Berechnung der sicherheitstechnischen Kennzahlen wurden die genannten Sicherheitsfunktionen zu Grunde gelegt. Die Bewertung der Hardware erfolgte auf Basis einer Failure Modes, Effects and Diagnostic Analysis (FMEDA). Eine FMEDA ist ein Schritt zur Bewertung der Funktionalen Sicherheit eines Gerätes gemäß IEC 61508. Auf Basis der FMEDA werden die Ausfallraten und der Anteil ungefährlicher Ausfälle des Gerätes bestimmt.
- Die Ausfallquoten für mechanische Teile wurden aus der exida Datenbank für mechanische Teile abgeleitet. Die elektronischen Ausfallraten sind die Basisausfallraten aus der SIEMENS- Norm SN 29500.
- Gemäß Tabelle 2 der IEC 61508-1, liegt der durchschnittliche PFD Wert für Systeme, welche für Low Demand Mode ausgelegt sind, bei:
 - SIL 2 Sicherheitsfunktionen: $\geq 10^{-3}$ bis $< 10^{-2}$
 - SIL 3 Sicherheitsfunktionen: $\geq 10^{-4}$ bis $< 10^{-3}$Da Stellantriebe aber nur einen Teil der gesamten Sicherheitsfunktion darstellen, sollte der PFD des Stellantriebs samt Getriebe nicht mehr als ca. 40 % des zulässigen Gesamtwertes (PFD_{avg}) einer Sicherheitsfunktion betragen. Dies ergibt folgenden Wert:
 - PFD Stellantrieb + Getriebe für SIL 2 Anwendungen: $\leq 4,0E-03$
- Die Fail-Safe-Einheit ist als Typ A Komponente mit einer Hardwarefehler toleranz von 0 eingestuft. Für das Typ A Teilsystem soll die SFF zwischen 60 % und < 90 % gemäß Tabelle 2 der IEC 61508-2 für SIL 2 (Teilsysteme mit einer Hardwarefehler toleranz von 0) sein.

9.2. Spezifische Kennzahlen für die Fail-Safe-Einheit in Ausführung SIL mit Stellantrieben der Baureihe SQ. 2

Die sicherheitstechnischen Kennzahlen, insbesondere die PFD, sind von diversen, vom Betreiber festzulegenden Maßnahmen und Intervallen abhängig (z.B. T_{Proof} , MRT, ...). Da die Diagnosefunktion nicht rein intern im FQM erfolgt, sondern von der Sicherheits-SPS angestoßen und/oder ausgewertet werden muss, kann auch das Diagnostestintervall in gewissen Grenzen vom Betreiber festgelegt werden. Dabei ist jedoch folgendes zu beachten:

- die Testfrequenz sollte mindestens dem 10-fachen der Anforderungsrate entsprechen
- das Testintervall kann für die Sicherheitsfunktion ESD niemals unter 22 Tage betragen
- das festgelegte Testintervall muss angemessen in der PFD-Berechnung berücksichtigt werden

Die nachfolgenden Kennzahlentabellen zeigen beispielhaft die sicherheitstechnischen Kennzahlen für die verschiedenen Ausführungen unter den weiter unten genannten beispielhaften Annahmen zu T_d und T_{proof} . Die vollständigen Datensätze der sicherheitstechnischen, beispielhaften Kennzahlen aller Varianten sind im exida Prüfbericht zu finden. Über die relevanten Kennzahlen unter den gemachten Angaben gibt die jeweilige auftragspezifische Herstellererklärung Auskunft.

Bei der Ermittlung der PFD-Werte muss beachtet werden, dass der vorgeschriebene Proof-Test keine vollständige Wiederherstellung des Systems ergibt. Daher werden zur Berechnung folgende Daten verwendet:

- $PTC = 95\%$ (Proof-Test Aufdeckungsgrad [%])
(PTC bei Durchführung des in diesem Handbuch beschriebenen Proof-Tests)
- $T_{Proof} = 1$ Jahr bzw. wie angegeben (Proof-Test Intervall [h])
- $T_{Mission} = 10$ Jahre (Anforderungsintervall = Lebensdauer [h])
- $MRT = 72$ Stunden (Mittlere Reparaturdauer [h])
- $T_{d_ESD} = 730$ Stunden
(Diagnostestintervall der Antriebsüberwachung (für die Sicherheitsfunktion Safe ESD [h]))

- MTTR = 802 Stunden

Für die Berechnung der PFD_{avg} Werte kann folgende Formel verwendet werden:

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

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

$$MTTR = Td_ESD + MRT$$

Darüber hinaus wurden folgende Annahmen gemacht:

- Die Ausfallraten sind konstant, Verschleißmechanismen sind nicht enthalten.
- Nur ein einzelner Komponentenfehler führt zu einem Ausfall des gesamten Geräts.
- Die Ausbreitung von Fehlern ist nicht von Bedeutung.
- Alle Komponenten die nicht Teil der Sicherheitsfunktion sind und welche die Sicherheitsfunktion nicht beeinflussen können, sind ausgeschlossen.
- Das System wird gemäß den Anweisungen des Herstellers (Sicherheitshandbuch) installiert.
- Fehler, die durch Wartungsfunktionen oder fehlerhafte Bedienung verursacht werden, sind standortspezifisch und sind daher nicht enthalten.
- Die Materialien sind mit den Prozessbedingungen kompatibel.
- Alle Geräte werden in der Betriebsart Low Demand betrieben.
- Für die ESD Funktion wird der Stellantrieb mindestens dem festgelegten Diagnosetestintervall entsprechend betätigt, um die interne Diagnose zu übernehmen.
- Die Häufigkeit der Diagnosefahrten (PVST/FVST) ist abhängig von dem im SIS geforderten Einsatz (Proof-Test-Intervall) und den anzuwendende Normen.
- Die Häufigkeit der Diagnosefahrten ist intern durch den FQM auf minimal 22 Tage beschränkt um Verschleiß vorzubeugen. Häufigere Fahrten können problemlos erfolgen, die interne Diagnose wird durch den FQM aber nicht ausgeführt.
- Nur die beschriebenen Varianten und Funktionen der Fail-Safe-Einheit FQM werden für Sicherheitsanwendungen verwendet.
- Interne und externe Diagnosemöglichkeiten sind im Sicherheitshandbuch angegeben.
- Für die Sicherheitsfunktionen wird ein PVST als Diagnosemaßnahme durchgeführt.
- Ein Handbetrieb ist nicht Teil der Sicherheitsfunktion und wurde daher nicht berücksichtigt.
- Die aufgelisteten elektronischen Fehlerraten gelten für typische Betriebs-Spannungsbedingungen in industrieller Feldumgebung mit Temperaturgrenzen innerhalb der Herstellerbewertung und mittlerer Temperatur von 40 °C (35 °C Umgebungstemperatur plus interne Selbsterhitzung), über einen langen Zeitraum. Für eine höhere Durchschnittstemperatur sollten die Fehlerraten mit einem erfahrungsbasierten Faktor von 1,5 für 50 °C, 2,5 für 60 °C und 5 für 80 °C multipliziert werden.
- Die Systemgrenze für die Fehlerbetrachtungen bezüglich des FQM ist die Kupplung zur Armatur.
Bei der sicheren Endlagenmeldung handelt es sich somit um die Rückmeldung, dass die Kupplung die entsprechende Position eingenommen hat. Es können jedoch keine Aussagen über mögliche Ausfälle der Armatur gemacht werden.

Zur Berechnung der Kennzahlen wurden folgende Tools verwendet:

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

Sicherheitsfunktion ESD mit PVST

Tabelle 6: Sicherheitstechnische Kennzahlen und Ausfallraten nach IEC 61508-2: 2010

Fehlerkategorie	Kennzahlen ¹⁾
λ_{SD}	0
λ_{SU}	273 FIT
λ_{DD}	672 FIT
λ_{DU}	513 FIT
Gesamte Fehlerrate (Sicherheitsfunktion)	1 458 FIT
SFF ²⁾	64 %
DC	56 %
PTC	95 %
SIL AC ³⁾	SIL2 (HFT = 0), SIL3 (HFT = 1)
MTBF (Jahre)	51
$PFD(T_{Proof}) = 1 \text{ Jahr}$	3,83E-03
$PFD(T_{Proof}) = 3 \text{ Jahre}$	8,1E-03
$PFD(T_{Proof}) = 5 \text{ Jahre}$	1,24E-02

- 1) Die Analyse wurde unter der Annahme durchgeführt, dass Fehler durch einen PVST mit Überwachung des Endlagenschalters über eine Sicherheits-SPS erkannt werden können.
- 2) Um die gesamte SFF (Safe Failure Fraction) zu bestimmen, muss das komplette finale Subsystem ausgewertet werden. Die aufgeführte Kennzahl dient ausschließlich als Referenz.
- 3) SIL AC (Architekturbeschränkungen) bedeutet, dass die berechneten Werte innerhalb des Bereichs für Hardwarearchitektur-Einschränkungen für den entsprechenden SIL liegen.

Sicherheitsfunktion sichere Endlage mit PVST

Tabelle 7: Sicherheitstechnische Kennzahlen und Ausfallraten nach IEC 61508-2: 2010/IEC 62061

Fehlerkategorie	Kennzahlen ¹⁾
λ_{SD}	0
λ_{SU}	0
λ_{DD}	62 FIT
λ_{DU}	39 FIT
Gesamte Fehlerrate (Sicherheitsfunktion)	101 FIT
SFF ²⁾	61 %
DC	61 %
PTC	95 %
SIL AC / SILCL	SIL2
$PFD(T_{Proof}) = 1 \text{ Jahr}$	3,0E-04
$PFD(T_{Proof}) = 3 \text{ Jahre}$	6,23E-04
$PFD(T_{Proof}) = 5 \text{ Jahre}$	9,47E-04

- 1) Die Analyse wurde unter der Annahme durchgeführt, dass Fehler durch einen PVST mit Überwachung des Endlagenschalters über eine Sicherheits-SPS erkannt werden können.
- 2) Um die gesamte SFF (Safe Failure Fraction) zu bestimmen, muss das komplette finale Subsystem ausgewertet werden. Die aufgeführte Kennzahl dient ausschließlich als Referenz.

Tabelle 8: Sicherheitstechnische Kennzahlen nach ISO 13849-1

Fehlerkategorie	Fehlerraten
MTTF _d (Jahre)	1 130 (high)
DC	61 % (low)
Kategorie (CAT)	CAT 1 oder CAT 2
Performance Level (berechnet)	3,89E-08 1/h
Performance Level (erreicht) ¹⁾	PL = c

- 1) Das komplette sicherheitstechnische, elektrische, elektronische und programmierbare elektronische Steuerungssystem (SRECS) für Maschinen muss bewertet werden, um den insgesamt erreichten Performance Level zu bestimmen. Der Performance Level ist nur als Referenz aufgeführt. Wichtig ist der berechnete Performance Level.

10. Checklisten

10.1. Inbetriebnahme-Checkliste

Tabelle 9: Inbetriebnahme-Checkliste

1. Fail-Safe-Einheit, Stellantrieb und Stellantriebs-Steuerung korrekt verdrahtet?	<input type="checkbox"/> ✓
2. Weg- und Drehmomentschaltung im Stellantrieb eingestellt?	<input type="checkbox"/> ✓
3. Endlagen der Fail-Safe-Einheit korrekt eingestellt?	<input type="checkbox"/> ✓
4. Sichere Funktion (je nach Konfiguration) anhand der Proof-Test-Checklisten geprüft?	<input type="checkbox"/> ✓
5. Inbetriebnahme der Grundeinstellungen (Stellantriebs-Steuerung) entsprechend der Betriebsanleitung durchgeführt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
☒ ✓ = ausgeführt	

10.2. Proof-Test-Checklisten


Wird der Proof-Test anhand der Proof-Test-Checklisten durchgeführt, müssen die zugehörigen HINWEISE aus dem Kapitel <Prüfungen und Wartung> berücksichtigt werden. Die Reihenfolge der Prüfschritte muss eingehalten werden.

10.2.1. Safe ESD Sicherheitsfahrt (sicheres ÖFFNEN/SCHLIESSEN)

Proof-Test-Checkliste für Ausführung bzw. Konfiguration:

- Safe ESD Funktion "sicheres SCHLIESSEN" (Safe ESD in Richtung ZU)
- Safe ESD Funktion "sicheres ÖFFNEN" (Safe ESD in Richtung AUF)

Tabelle 10: Proof-Test-Checkliste

Konfiguration sicheres SCHLIESSEN (ESD in Richtung Fail-Safe-Position ZU)		Konfiguration sicheres ÖFFNEN (ESD in Richtung Fail-Safe-Position AUF)	
1. Stellantrieb steht in Endlage AUF?	<input type="checkbox"/> ✓	1. Stellantrieb steht in Endlage ZU?	<input type="checkbox"/> ✓
2. Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“)	<input type="checkbox"/> ✓	2. Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“)	<input type="checkbox"/> ✓
3. Eingangssignal ESD auf 0 V (Low) gesetzt? (Stellzeitmessung durchführen)	<input type="checkbox"/> ✓	3. Eingangssignal ESD auf 0 V (Low) gesetzt? (Stellzeitmessung durchführen)	<input type="checkbox"/> ✓
↳ Reaktion der Fail-Safe-Einheit prüfen: FQM fährt in Richtung ZU? (Start der Stellzeitmes- sung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Reaktion der Fail-Safe-Einheit prüfen: FQM fährt in Richtung AUF? (Start der Stellzeitmes- sung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
FQM erreicht Endlage ZU? (Ende der Stellzeitmes- sung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	FQM erreicht Endlage AUF? (Ende der Stellzeitmes- sung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Stellzeit der FQM entspricht der Angabe auf dem Ty- penschild für 90° Schwenkwinkel bzw. der konfigurier- ten Stellzeit? Stellzeit [-50 %/+ 100 %]	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Stellzeit der FQM entspricht der Angabe auf dem Ty- penschild für 90° Schwenkwinkel bzw. der konfigurier- ten Stellzeit? Stellzeit [-50 %/+ 100 %]	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = zu (Meldung „FS-Fehler“)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = zu (Meldung „FS-Fehler“)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Eingangssignal ESD auf +24 V DC (High) gesetzt? Beginn der Zeitmessung.	<input type="checkbox"/> ✓	4. Eingangssignal ESD auf +24 V DC (High) gesetzt? Beginn der Zeitmessung.	<input type="checkbox"/> ✓

Konfiguration sicheres SCHLIESSEN (ESD in Richtung Fail-Safe-Position ZU)		Konfiguration sicheres ÖFFNEN (ESD in Richtung Fail-Safe-Position AUF)	
Der FQM startet die automatische Initialisierung (Feder wird gespannt)	<input checked="" type="checkbox"/>	Der FQM startet die automatische Initialisierung (Feder wird gespannt)	<input checked="" type="checkbox"/>
↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung ändert sich nach Abschluss der Initialisierung auf: Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“) Ende der Zeitmessung, 2 Minuten wurden nicht überschritten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung ändert sich nach Abschluss der Initialisierung auf: Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“) Ende der Zeitmessung, 2 Minuten wurden nicht überschritten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
<input checked="" type="checkbox"/> ✓ = ausgeführt <input checked="" type="checkbox"/> Ja = Bedingung erfüllt <input checked="" type="checkbox"/> Nein = Bedingung nicht erfüllt Falls eine Frage Ja/Nein mit Nein beantwortet wird, muss das sicherheitstechnische System überprüft werden.			

Zusätzliche Proof-Test-Checkliste für Ausführung bzw. Konfiguration:

- Safe ESD Funktion "sicheres SCHLIESSEN" (Safe ESD in Richtung ZU) mit zusätzlicher Auslösung bei Netzausfall
- Safe ESD Funktion "sicheres ÖFFNEN" (Safe ESD in Richtung AUF) mit zusätzlicher Auslösung bei Netzausfall
- unabhängig von der Abschaltart

Tabelle 11: Zusätzliche Proof-Test-Checkliste


Konfiguration sicheres SCHLIESSEN mit zusätzlicher Auslösung bei Netzausfall (ESD in Richtung Fail-Safe-Position ZU)		Konfiguration sicheres ÖFFNEN mit zusätzlicher Auslösung bei Netzausfall (ESD in Richtung Fail-Safe-Position AUF)	
1. Stellantrieb steht in Endlagen AUF?	<input checked="" type="checkbox"/>	1. Stellantrieb steht in Endlagen ZU?	<input checked="" type="checkbox"/>
2. Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“)	<input checked="" type="checkbox"/>	2. Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“)	<input checked="" type="checkbox"/>
3. Spannungsversorgung (Netz) der FQM unterbrochen? (Stellzeitmessung durchführen)	<input checked="" type="checkbox"/>	3. Spannungsversorgung (Netz) der FQM unterbrochen? (Stellzeitmessung durchführen)	<input checked="" type="checkbox"/>
↳ Reaktion der Fail-Safe-Einheit prüfen: FQM fährt in Richtung ZU? (Start der Stellzeitmessung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Reaktion der Fail-Safe-Einheit prüfen: FQM fährt in Richtung AUF? (Start der Stellzeitmessung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
FQM erreicht Endlage ZU? (Ende der Stellzeitmessung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	FQM erreicht Endlage AUF? (Ende der Stellzeitmessung)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Stellzeit der FQM entspricht der Angabe auf dem Typenschild für 90° Schwenkwinkel bzw. der konfigurierten Stellzeit? Stellzeit [-50 %/+ 100 %]	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Stellzeit der FQM entspricht der Angabe auf dem Typenschild für 90° Schwenkwinkel bzw. der konfigurierten Stellzeit? Stellzeit [-50 %/+ 100 %]	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = zu (Meldung „FS-Fehler“)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung? Ausgang FS Failure NC (Öffner-Kontakt) = zu (Meldung „FS-Fehler“)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Spannungsversorgung (Netz) der FQM wieder hergestellt? Beginn der Zeitmessung.	<input checked="" type="checkbox"/>	4. Spannungsversorgung (Netz) der FQM wieder hergestellt? Beginn der Zeitmessung.	<input checked="" type="checkbox"/>
Der FQM startet die automatische Initialisierung (Feder wird gespannt)	<input checked="" type="checkbox"/>	Der FQM startet die automatische Initialisierung (Feder wird gespannt)	<input checked="" type="checkbox"/>
↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung ändert sich nach Abschluss der Initialisierung auf: Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“) Ende der Zeitmessung, 2 Minuten wurden nicht überschritten.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	↳ Meldeverhalten FS-Modul prüfen: Fail-Safe-Fehlermeldung ändert sich nach Abschluss der Initialisierung auf: Ausgang FS Failure NC (Öffner-Kontakt) = offen (Meldung „FS-Bereit“) Ende der Zeitmessung, 2 Minuten wurden nicht überschritten.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein


10.2.2. Überprüfen und Validierung der Sicherheitsfunktion "sichere Endlagenrückmeldung"

Proof-Test-Checkliste für Ausführung bzw. Konfiguration einer der folgenden Sicherheitsfunktionen:

- Sicherheitsfunktion "sichere Endlagenrückmeldung"
- Gilt auch für die Kombination mit Safe ESD in Richtung AUF/ZU.

Tabelle 12: Proof-Test-Checkliste

Konfiguration Fail-Safe-Position AUF und ZU (Sicherheitsposition AUF und ZU)	
1. Stellantrieb steht in Mittelstellung bzw. in ausreichender Entfernung zu den Endlagen?	<input type="checkbox"/> ✓
↳ Endlagenschalter des FQM prüfen: • Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.: Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen • Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.: Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen ↳ Es darf keine Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“).	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
2. Fahrbefehl in Richtung ZU ausgeführt?	<input type="checkbox"/> ✓
↳ Reaktion des Stellantriebs prüfen: Fahrt wurde ausgelöst?	<input type="checkbox"/> ✓
3. Warten bis FQM Endlagenschalter auslöst. ↳ Reaktion des Stellantriebs prüfen: Fahrt wurde bei Erreichen des Endlagenschalters ZU gestoppt? • Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.: Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen • Meldung Endlage ZU erreicht (Ausgangssignal aktiv), d.h.: Ausgang LSC 22-23=NC (Öffner-Kontakt) = offen Ausgang LSC 22-24=NO (Schließer-Kontakt) = geschlossen ↳ Es darf keine Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“).	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
4. Fahrbefehl in Richtung AUF ausgeführt?	<input type="checkbox"/> ✓
↳ Reaktion des Stellantriebs prüfen: Fahrt wurde ausgelöst? Beginn der Stellzeitmessung.	<input type="checkbox"/> ✓
5. Warten bis FQM Endlagenschalter auslöst. ↳ Reaktion des Stellantriebs prüfen: Fahrt wurde bei Erreichen des Endlagenschalters AUF gestoppt? Ende der Stellzeitmessung. • Meldung Endlage AUF erreicht (Ausgangssignal aktiv), d.h.: Ausgang LSO 19-20=NC (Öffner-Kontakt) = offen Ausgang LSO 19-21=NO (Schließer-Kontakt) = geschlossen • Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.: Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen ↳ Es darf keine Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“).	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Stellzeit für Fahrt aus Endlage ZU in Richtung Endlage AUF entspricht der Konfiguration des Stellantriebs.	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
6. FQM über Stellantrieb in Zwischenstellung fahren. Stellantrieb steht in Mittelstellung bzw. in ausreichender Entfernung zu den Endlagen?	<input type="checkbox"/> ✓

Konfiguration Fail-Safe-Position AUF und ZU (Sicherheitsposition AUF und ZU)	
<ul style="list-style-type: none"> ↳ Endlagenschalter des FQM prüfen: <ul style="list-style-type: none"> • Meldung Endlage AUF nicht erreicht (Ausgangssignal inaktiv), d.h.: <ul style="list-style-type: none"> Ausgang LSO 19-20=NC (Öffner-Kontakt) = geschlossen Ausgang LSO 19-21=NO (Schließer-Kontakt) = offen • Meldung Endlage ZU nicht erreicht (Ausgangssignal inaktiv), d.h.: <ul style="list-style-type: none"> Ausgang LSC 22-23=NC (Öffner-Kontakt) = geschlossen Ausgang LSC 22-24=NO (Schließer-Kontakt) = offen ↳ Es darf keine Fail-Safe-Fehlermeldung vorliegen (Meldung „FS-Bereit“). 	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> ✓ = ausgeführt <input checked="" type="checkbox"/> Ja = Bedingung erfüllt <input checked="" type="checkbox"/> Nein = Bedingung nicht erfüllt Falls eine Frage Ja/Nein mit Nein beantwortet wird, muss das sicherheitstechnische System überprüft werden.	

11. SIL-Konformitätserklärung (Beispiel)

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



SIL Declaration of Conformity / SIL Declaration of Incorporation

Functional Safety according to IEC 61508

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

AUMA order no.

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

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

The above mentioned version achieves the following Hardware Safety Integrity:

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

For further details, please refer to supplement overleaf.


i.A. Michael Noll
Functional Safety Management Representative

i.A. Jörg Isenberg
Product Management

Date

Date

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

 Solutions for a world in motion	Supplement SIL Declaration of Conformity/ SIL Declaration of Incorporation Functional Safety according to IEC 61508	2019-07-24
--	---	------------

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

General	
Device designation and permissible types	See page 1
Safety function(s)	Fail Safe OPEN/CLOSE (ESD) with PVST
Device type according to IEC 61508-2	<input checked="" type="checkbox"/> Type A <input type="checkbox"/> Type B
Operating mode	<input checked="" type="checkbox"/> Low Demand Mode <input type="checkbox"/> High Demand or Continuous Mode
Type of evaluation	<input checked="" type="checkbox"/> Evaluation by FMEDA according to IEC 61508-2
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG / AUMA 14/07-095 R013

Hardware Integrity			
Hardware integrity for "Fail Safe OPEN/CLOSE" (ESD) with PVST	Single channel use with PVST FQM 05.1 – FQM 12.1 (HFT = 0)	<input type="checkbox"/> SIL1 capable	<input checked="" type="checkbox"/> SIL2 capable <input type="checkbox"/> SIL3 capable

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

Restrictions	
<ul style="list-style-type: none"> - Imperatively comply with any information given in the safety manual. - The safety figures for the "Fail Safe OPEN/CLOSE" (ESD) function are only valid if the end position switches directly wired to the customer connection are used for end position evaluation. - Frequent diagnostic via Partial Valve Stroke Test (PVST) out of end position controlled by the Safety PLC is necessary. The frequency has to be defined by the end user in accordance with the applicable standards, the restrictions given in the safety manual and the defined Proof Test interval. - For the PVST only evaluation of the switches directly connected from the FQM to the customer connector is permissible. - Evaluation of the collective fault signal output contact of the FQM (FS ready/failure signal) is necessary. - The failure rates are valid for the useful life of the individual components of the "Fail Safe OPEN/CLOSE" (ESD) with PVST function of the Fail Safe Unit. <p>The SIL / PL has to be evaluated for the complete (sub-)system. The numbers listed are for reference only.</p>	

⁽¹⁾ FIT = Failure In Time, Number of failures per 10⁹ h

⁽²⁾ PFD_{avg} = Probability of a failure on demand (average)

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



SIL Declaration of Conformity / SIL Declaration of Incorporation

Functional Safety according to IEC 61508

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

AUMA order no.

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

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

The above mentioned version achieves the following Hardware Safety Integrity:

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

For further details, please refer to supplement overleaf.


i.A. Michael Noll
Functional Safety Management Representative

i.A. Jörg Isenberg
Product Management

Date

Date

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

 Solutions for a world in motion	Supplement SIL Declaration of Conformity/ SIL Declaration of Incorporation Functional Safety according to IEC 61508	2019-07-24
--	---	------------

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

General	
Device designation and permissible types	See page 1
Safety function(s)	Safe End Position Feedback with PVST
Device type according to IEC 61508-2	<input checked="" type="checkbox"/> Type A <input type="checkbox"/> Type B
Operating mode	<input checked="" type="checkbox"/> Low Demand Mode <input type="checkbox"/> High Demand or Continuous Mode
Type of evaluation	<input checked="" type="checkbox"/> Evaluation by FMEDA according to IEC 61508-2
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG / AUMA 14/07-095 R013

Hardware Integrity				
Hardware integrity for Safe End Position Feedback with PVST	Single channel use with PVST FQM 05.1 – FQM 12.1 (HFT = 0)	<input type="checkbox"/> SIL1 capable	<input checked="" type="checkbox"/> SIL2 capable	<input type="checkbox"/> SIL3 capable

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

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

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

Restrictions	
<ul style="list-style-type: none"> - Imperatively comply with any information given in the safety manual. - The safety figures for the Safe End Position Feedback with PVST are only valid if the end position switches directly wired to the customer connection are used for end position evaluation. - Frequent diagnostic via Partial Valve Stroke Test (PVST) out of end position controlled by the Safety PLC is necessary. The frequency has to be defined by the end user in accordance with the applicable standards, the restrictions given in the safety manual and the defined Proof Test interval. - For the PVST only evaluation of the switches directly connected from the FQM to the customer connector is permissible. - Evaluation of the collective fault signal output contact of the FQM (FS ready/failure signal) is necessary. - The failure rates are valid for the useful life of the individual components of the Safe End Position Feedback with PVST of the Fail Safe Unit. - The SIL / PL has to be evaluated for the complete (sub-)system. The numbers listed are for reference only. 	

⁽¹⁾ FIT = Failure In Time, Number of failures per10⁹ h

⁽²⁾ PFD_{avg} = Probability of a failure on demand (average)

⁽³⁾ Depending on the application and possible external diagnostics a higher DC and therefore also a higher category and a higher Performance level might be possible to achieve.

Stichwortverzeichnis

A

Anteil ungefährlicher Ausfälle (SFF)	4, 29
Antriebsauslegung	8
Antriebsüberwachung intern	22
Anwendungsbeispiele	13
Anwendungsbereich	6
Anzeigen	20
Ausfallwahrscheinlichkeit	4
Außerbetriebsetzung	18

B

Betrieb	18
---------	----

C

Checklisten	33, 33
-------------	--------

D

DC	4
Diagnosedeckungsgrad	4
Digitale Ausgänge	21

E

Einsatzbedingungen	10
Einstellung	9
Entsorgung	19

F

Feldbus (Meldungen)	21
---------------------	----

G

Gerätetypen	6
-------------	---

H

HFT	4
-----	---

I

Inbetriebnahme	18
Inbetriebnahme-Checkliste	33
Installation	16
Intervall für Wiederholungsprüfung	4

K

Kennzahlen	29
Konfiguration	9
Konformitätserklärung	37

L

Lambda-Werte	4, 29
Lebensdauer	18
Low Demand Mode	29

M

Meldungen	21
Mittlere Ausfallwahrscheinlichkeit (MTBF)	4
MRT (Mean Repair Time)	5
MTBF	4
MTTR (Mean Time To Restoration)	5

N

Normen	6
--------	---

P

Partial Valve Stroke Test (PVST)	23
PFD	4
PFD Stellantrieb	29
Projektierung	8
Proof-Test	24
Proof-Test-Checklisten	33
Prüfungen	22

R

Recycling	19
-----------	----

S

SFF	4
Sicherheitsbezogenes System	5
Sicherheitsfunktion	4
Sicherheitsfunktionen	11
Sicherheitstechnische Funktion (SIF)	4
Sicherheitstechnisches System	11
Sicherheitstechnisches System (SIS)	4
SIL	4

T

T proof	4
---------	---

U

Umweltbedingungen	10
-------------------	----

W

Wartung	28
Wiederholungsprüfung	5, 24

Z

Zertifikat	37
Zustandsmeldungen	21

Europa**AUMA Riester GmbH & Co. KG**

Werk Müllheim
DE 79373 Müllheim
 Tel +49 7631 809 - 0
 info@auma.com
 www.auma.com

Werk Ostfildern-Nellingen
DE 73747 Ostfildern
 Tel +49 711 34803 - 0
 riester@auma.com

Service-Center Bayern
DE 85386 Eching
 Tel +49 81 65 9017- 0
 Service.SCB@auma.com

Service-Center Köln
DE 50858 Köln
 Tel +49 2234 2037 - 900
 Service@sck.auma.com

Service-Center Magdeburg
DE 39167 Niederndodeleben
 Tel +49 39204 759 - 0
 Service@scm.auma.com

AUMA-Armaturentriebe Ges.m.b.H.
AT 2512 Tribuswinkel
 Tel +43 2252 82540
 office@auma.at
 www.auma.at

AUMA BENELUX B.V. B. A.
BE 8800 Roeselare
 Tel +32 51 24 24 80
 office@auma.be
 www.auma.nl

ProStream Group Ltd.
BG 1632 Sofia
 Tel +359 2 9179-337
 valtchev@prostream.bg
 www.prostream.bg

OOO "Dunkan-Privod"
BY 220004 Minsk
 Tel +375 29 6945574
 belarus@auma.ru
 www.zatvor.by

AUMA (Schweiz) AG
CH 8965 Berikon
 Tel +41 566 400945
 RettichP.ch@auma.com

AUMA Servopohony spol. s.r.o.
CZ 250 01 Brandýs n.L.-St.Boleslav
 Tel +420 326 396 993
 auma-s@auma.cz
 www.auma.cz

IBEROPLAN S.A.
ES 28027 Madrid
 Tel +34 91 3717130
 iberoplan@iberoplan.com

AUMA Finland Oy
FI 02230 Espoo
 Tel +358 9 5840 22
 auma@auma.fi
 www.auma.fi

AUMA France S.A.R.L.
FR 95157 Taverny Cedex
 Tel +33 1 39327272
 info@auma.fr
 www.auma.fr

AUMA ACTUATORS Ltd.
GB Clevedon, North Somerset BS21 6TH
 Tel +44 1275 871141
 mail@auma.co.uk
 www.auma.co.uk

D. G. Bellos & Co. O.E.
GR 13673 Acharnai, Athens
 Tel +30 210 2409485
 info@dgbellos.gr

APIS CENTAR d. o. o.
HR 10437 Bestovje
 Tel +385 1 6531 485
 auma@apis-centar.com
 www.apis-centar.com

Fabo Kereskedelmi és Szolgáltató Kft.
HU 8800 Nagykanizsa
 Tel +36 93/324-666
 auma@fabo.hu
 www.fabo.hu

Falkinn HF
IS 108 Reykjavik
 Tel +00354 540 7000
 os@falkinn.is
 www.falkinn.is

AUMA ITALIANA S.r.l. a socio unico
IT 20023 Cerro Maggiore (MI)
 Tel +39 0331 51351
 info@auma.it
 www.auma.it

AUMA BENELUX B.V.
LU Leiden (NL)
 Tel +31 71 581 40 40
 office@auma.nl

NB Engineering Services
MT ZBR 08 Zabbar
 Tel + 356 2169 2647
 nikibel@onvol.net

AUMA BENELUX B.V.
NL 2314 XT Leiden
 Tel +31 71 581 40 40
 office@auma.nl
 www.auma.nl

SIGUM A. S.
NO 1338 Sandvika
 Tel +47 67572600
 post@sifag.no

AUMA Polska Sp. z o.o.
PL 41-219 Sosnowiec
 Tel +48 32 783 52 00
 biuro@auma.com.pl
 www.auma.com.pl

AUMA-LUSA Representative Office, Lda.
PT 2730-033 Barcarena
 Tel +351 211 307 100
 geral@aumalusa.pt

SAUTECH
RO 011783 Bucuresti
 Tel +40 372 303982
 office@sautech.ro

OOO PRIWODY AUMA
RU 141402 Khimki, Moscow region
 Tel +7 495 221 64 28
 aumarussia@auma.ru
 www.auma.ru

OOO PRIWODY AUMA
RU 125362 Moscow
 Tel +7 495 787 78 21
 aumarussia@auma.ru
 www.auma.ru

AUMA Scandinavia AB
SE 20039 Malmö
 Tel +46 40 311550
 info.scandinavia@auma.com
 www.auma.se

ELSO-b, s.r.o.
SK 94901 Nitra
 Tel +421 905/336-926
 office@elsob.sk
 www.elsob.sk

Auma Endüstri Kontrol Sistemleri Limited
 Sirketi
TR 06810 Ankara
 Tel +90 312 217 32 88
 info@auma.com.tr

AUMA Technology Automations Ltd
UA 02099 Kiev
 Tel +38 044 586-53-03
 auma-tech@amatech.com.ua

Afrika

Solution Technique Contrôle Commande
DZ Bir Mourad Rais, Algiers
 Tel +213 21 56 42 09/18
 stcco@wissal.dz

A.T.E.C.
EG Cairo
 Tel +20 2 23599680 - 23590861
 contactus@atec-eg.com

SAMIREG
MA 203000 Casablanca
 Tel +212 5 22 40 09 65
 samireg@menara.ma

MANZ INCORPORATED LTD.
NG Port Harcourt
 Tel +234-84-462741
 mail@manzincorporated.com
 www.manzincorporated.com

AUMA South Africa (Pty) Ltd.
ZA 1560 Springs
 Tel +27 11 3632880
 aumasa@mweb.co.za

Amerika

AUMA Argentina Rep.Office
AR Buenos Aires
 Tel +54 11 4737 9026
 contacto@aumaargentina.com.ar

AUMA Automação do Brazil Ltda.
BR Sao Paulo
 Tel +55 11 4612-3477
 contato@auma-br.com

TROY-ONTOR Inc.
CA L4N 8X1 Barrie, Ontario
 Tel +1 705 721-8246
 troy-ontor@troy-ontor.ca

AUMA Chile Representative Office
CL 7870163 Santiago
 Tel +56 2 2821 4108
 claudio.bizama@auma.com

B & C Biosciences Ltda.
CO Bogotá D.C.
 Tel +57 1 349 0475
 proyectos@bycenlinea.com
 www.bycenlinea.com

AUMA Región Andina & Centroamérica
EC Quito
 Tel +593 2 245 4614
 auma@auma-ac.com
 www.auma.com

Corsusa International S.A.C.
PE Miraflores - Lima
 Tel +511444-1200 / 0044 / 2321
 corsusa@corsusa.com
 www.corsusa.com

Control Technologies Limited
TT Marabella, Trinidad, W.I.
 Tel + 1 868 658 1744/5011
 www.ctltech.com

AUMA ACTUATORS INC.
US PA 15317 Canonsburg
 Tel +1 724-743-2862
 mailbox@auma-usa.com
 www.auma-usa.com

Suplibarca
VE Maracaibo, Estado, Zulia
 Tel +58 261 7 555 667
 suplibarca@intercable.net.ve

Asien

AUMA Actuators UAE Support Office
AE 287 Abu Dhabi
 Tel +971 26338688
 Nagaraj.Shetty@auma.com

AUMA Actuators Middle East
BH 152 68 Salmabad
 Tel +97 3 17896585
 salesme@auma.com

Mikuni (B) Sdn. Bhd.
BN KA1189 Kuala Belait
 Tel + 673 3331269 / 3331272
 mikuni@brunet.bn

AUMA Actuators (China) Co., Ltd.
CN 215499 Taicang
 Tel +86 512 3302 6900
 mailbox@auma-china.com
 www.auma-china.com

PERFECT CONTROLS Ltd.
HK Tsuen Wan, Kowloon
 Tel +852 2493 7726
 joeip@perfectcontrols.com.hk

PT. Carakamas Inti Alam
ID 11460 Jakarta
 Tel +62 215607952-55
 auma-jkt@indo.net.id

AUMA INDIA PRIVATE LIMITED.
IN 560 058 Bangalore
 Tel +91 80 2839 4656
 info@auma.co.in
 www.auma.co.in

ITG - Iranians Torque Generator
IR 13998-34411 Teheran
 +982144545654
 info@itg-co.ir

Trans-Jordan Electro Mechanical Supplies
JO 11133 Amman
 Tel +962 - 6 - 5332020
 Info@transjordan.net

AUMA JAPAN Co., Ltd.
JP 211-0016 Kawasaki-shi, Kanagawa
 Tel +81-(0)44-863-8371
 mailbox@auma.co.jp
 www.auma.co.jp

DW Controls Co., Ltd.
KR 153-702 Gasan-dong, GeumChun-Gu,, Seoul
 Tel +82 2 2624 3400
 sales@dwcontrols.net
 www.dwcontrols.net

Al-Arfaj Engineering Co WLL
KW 22004 Salmiyah
 Tel +965-24817448
 info@arfajengg.com
 www.arfajengg.com

TOO "Armaturny Center"
KZ 060005 Atyrau
 Tel +7 7122 454 602
 armacentre@bk.ru

Network Engineering
LB 4501 7401 JBEIL, Beirut
 Tel +961 9 944080
 nabil.ibrahim@networkenglb.com
 www.networkenglb.com

AUMA Malaysia Office
MY 70300 Seremban, Negeri Sembilan
 Tel +606 633 1988
 sales@auma.com.my

Mustafa Sultan Science & Industry Co LLC
OM Ruwi
 Tel +968 24 636036
 r-negi@mustafasultan.com

FLOWTORK TECHNOLOGIES CORPORATION
PH 1550 Mandaluyong City
 Tel +63 2 532 4058
 flowtork@pltdsl.net

M & C Group of Companies
PK 54000 Cavalry Ground, Lahore Cantt
 Tel +92 42 3665 0542, +92 42 3668 0118
 sales@mcass.com.pk
 www.mcass.com.pk

Petrogulf W.L.L.
QA Doha
 Tel +974 44350151
 pgulf@qatar.net.qa

AUMA Saudi Arabia Support Office
SA 31952 Al Khobar
 Tel + 966 5 5359 6025
 Vinod.Fernandes@auma.com

AUMA ACTUATORS (Singapore) Pte Ltd.
SG 569551 Singapore
 Tel +65 6 4818750
 sales@auma.com.sg
 www.auma.com.sg

NETWORK ENGINEERING
SY Homs
 +963 31 231 571
 eyad3@scs-net.org

Sunny Valves and Intertrade Corp. Ltd.
TH 10120 Yannawa, Bangkok
 Tel +66 2 2400656
 mainbox@sunnyvalves.co.th
 www.sunnyvalves.co.th

Top Advance Enterprises Ltd.
TW Jhonghe City, Taipei Hsien (235)
 Tel +886 2 2225 1718
 support@auma-taiwan.com.tw
 www.auma-taiwan.com.tw

AUMA Vietnam Hanoi RO
VN Hanoi
 +84 4 37822115
 chiennguyen@auma.com.vn

Australien

BARRON GJM Pty. Ltd.
AU NSW 1570 Artarmon
 Tel +61 2 8437 4300
 info@barron.com.au
 www.barron.com.au



Solutions for a world in motion

AUMA Riester GmbH & Co. KG

Werk Müllheim

Postfach 1362

DE 79373 Muellheim

Tel +49 7631 809 - 0

Fax +49 7631 809 - 1250

info@auma.com

www.auma.com

Werk Ostfildern-Nellingen

Postfach 1151

DE 73747 Ostfildern

Tel +49 711 34803 - 0

Fax +49 711 34803 - 3034

riester@auma.com

Service-Center Köln

DE 50858 Köln

Tel +49 2234 2037 - 900

Fax +49 2234 2037 - 9099

Service@sck.auma.com