Solutions for a world in motion

Drehantriebe
SA 25.1 – SA 40.1
SAEx 25.1 – SAEx 40.1
mit Stellantriebs-Steuerung
AC 01.2 -22X/-22Y
ACExC 01.2 -22X/-22Y

HINWEIS zur Verwendung!

Dieses Dokument ist nur in Verbindung mit der aktuellen, dem Gerät beiliegenden Betriebsanleitung, dem beiliegenden Handbuch 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.

Referenzunterlagen:

- Betriebsanleitung (Montage und Inbetriebnahme) zum Stellantrieb
- Handbuch (Betrieb und Einstellung) Stellantriebs-Steuerung AC 01.2/ACExC 01.2
- Handbuch (Geräteintegration) Stellantriebs-Steuerung AC(V) 01.2/AC(V)ExC 01.2
- Technische Daten zum Drehantrieb und zur Stellantriebs-Steuerung.

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

Inhaltsverzeichnis

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**ault **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

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.

Ein sicherheitsbezogenes System kann eine eigenständige Anlage zur Ausführung einer bestimmten Sicherheitsfunktion sein oder in eine andere Anlage integriert sein.

Wiederholungsprüfung

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.

MTTR (Mean Time To Restoration)

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.

MRT (Mean Repair Time)

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.

Gerätetyp (Typ A und Typ B)

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:

- 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%).

Die Stellantriebs-Steuerung muss als Gerät vom **Typ B** betrachtet werden, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- 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)

Der Proof Test Coverage beschreibt den Anteil der aufdeckbaren Ausfälle durch einen Proof-Test.

2. Anwendung und Gültigkeit

2.1. Anwendungsbereich

AUMA Stellantriebe und Stellantriebs-Steuerungen in Version 22X oder 22Y sind für die Betätigung von Industriearmaturen bestimmt und eignen sich für den Einsatz in sicherheitstechnischen Systemen nach IEC 61508 bzw. IEC 61511.

2.2. Normen

Die Stellantriebe und Stellantriebs-Steuerungen erfüllen folgende Anforderungen:

Die sicherheitstechnischen Kennzahlen der beschriebenen Geräte erfüllen die Anforderungen der IEC 61508:2010 im entsprechenden SIL bezüglich Ausfallraten und Architekturanforderungen. Dies bedeutet jedoch nicht, dass alle weiteren Anforderungen der IEC 61508 erfüllt werden.

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		**Spannungsversorgung**
Stellantrieb	**Steuerung**	**Motor**
SA 25.1 – SA 40.1	AC 01.2 in Version 22X oder 22Y	Drehstrom
SAEx 25.1 – SAEx 40.1	ACExC 01.2 in Version 22X oder 22Y	Drehstrom

Die Hardware, Software und die Konfiguration des Stellantriebs und/oder der Stellantriebs-Steuerung darf ohne schriftliche Zustimmung von AUMA nicht verändert werden. Unauthorisierte Veränderungen können die Sicherheitskennzahlen und die SIL-Fähigkeit der Produkte negativ beeinflussen.

Information

In Anwendungen mit Anforderungen zur Funktionalen Sicherheit dürfen nur AUMA Stellantriebs-Steuerungen und Stellantriebe in den Versionen SFC, SIL, 22X oder 22Y zum Einsatz kommen.
AUMA Stellantriebs-Steuerungen und Stellantriebe in Version 22X oder 22Y sind u.a. daran zu erkennen, dass auf dem Typenschild die Buchstabenfolge „22X“ oder „22Y“ zu finden ist.

Bild 1: Beispiel Typenschild mit Kennzeichnung „22X“

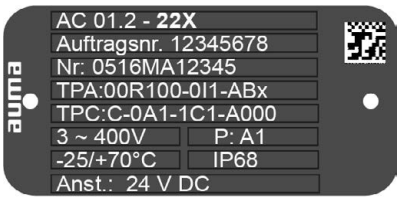


Bild 2: Beispiel Typenschild SA mit Kennzeichnung „22X“

3. Projektierung, Konfiguration und Einsatzbedingungen

3.1. Projektierung (Stellantriebsauslegung)

Für die Projektierung (Stellantriebsauslegung) der Stellantriebe 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, Schäden an der Elektronik, Erwärmung bzw. Beschädigung von Leitungen.

→ Die technischen Daten der Stellantriebe sind bei der Antriebsauslegung unbedingt zu berücksichtigen.

→ Es muss genügend Reserve eingeplant werden um sicherzustellen, dass die Stellantriebe in der Lage sind, die Armatur auch im Störfall und bei Unterspannungsbedingungen zuverlässig zu schließen bzw. zu öffnen.

Projektierung bei Verwendung der Safe STOP Funktion

Information

Bei der Safe STOP Funktion wird der Motor ausgeschaltet, ggf. ergibt sich ein Nachlauf!

HINWEIS

Schäden an der Armatur durch Nachlauf möglich!

→ Für die Safe STOP Funktion muss der Nachlauf der Anordnung (Stellantrieb, Getriebe, Armatur) und die Reaktionszeit berücksichtigt werden.

→ Falls die Art der Anwendung eine Selbsthemmung des Stellantriebs erfordert, muss dies mit AUMA geklärt werden.

Projektierung bei der Verwendung der Safe ESD Funktion

Stellantriebe mit elektromechanischer Steuereinheit:

Bei der Konfiguration „SIL-Abschaltart“ = „keine Abschaltung“ (ohne Endlagenschutz) empfehlen wir:

- Um Schäden an der Armatur bei einer Sicherheitsfahrt zu vermeiden, empfehlen wir die Armatur je nach Steifigkeit, auf das 3 – 5 fache des maximalen Stellantrieb-Drehmoments auszulegen.
- Zur Vermeidung von thermischen Schäden durch zu hohe Ströme empfehlen wir eine Überwachung (Auswertung) des Motorschutzes.

Stellantriebe mit elektronischer Steuereinheit MWG:

Information

Die Endlagenmeldung (Wegschaltung) und die Drehmomentmeldung über die elektronische Steuereinheit MWG sind keine sicheren Meldungen.

- Um Schäden an der Armatur bei einer Sicherheitsfahrt zu vermeiden empfehlen wir die Armatur je nach Steifigkeit, auf das 3 – 5 fache des maximalen Stellantrieb-Drehmoments auszulegen.
- Zur Vermeidung von thermischen Schäden durch zu hohe Ströme empfehlen wir eine Überwachung (Auswertung) des Motorschutzes.

Stellantriebe mit elektronischer Steuereinheit MWG mit Wegschaltern:

Bei der Konfiguration „SIL-Abschaltart“ = „keine Abschaltung“ (ohne Endlagenschutz) empfehlen wir:

- Um Schäden an der Armatur bei einer Sicherheitsfahrt zu vermeiden, empfehlen wir die Armatur je nach Steifigkeit, auf das 3 – 5 fache des maximalen Stellantrieb-Drehmoments auszulegen.

- Zur Vermeidung von thermischen Schäden durch zu hohe Ströme empfehlen wir eine Überwachung (Auswertung) des Motorschutzes.

Information Bei der Konfiguration „SIL-Abschaltart“ = „Abschaltung in der Weg-Endlage“ findet die Abschaltung in der Endlage über die Wegschalter statt. Da jeder Schalter eine Hysterese hat, verlässt der Stellantrieb die Endlage bevor der Wegschalter wieder freigegeben wird. Folglich gibt es einen an die Sicherheitsposition angrenzenden Bereich der Stellantriebspositionen, in dem der Wegschalter bei Fahren aus der Sicherheitsposition heraus noch betätigt ist und deshalb die Safe ESD Funktion NICHT zur Verfügung steht. Auslösen der Sicherheitsfunktion führt in diesem Fall zum Stillstand des Stellantriebs. Wird der fragliche Bereich aus der Gegenrichtung erreicht, so besteht die beschriebene Einschränkung nicht. Normalerweise ist dieser Bereich klein, er kann jedoch in ungünstigen Konfigurationen (geringe Anzahl Umdrehungen pro Hub) bis über 10 % des Gesamthubs betragen.
Sollte auf Grund ungünstiger Rahmenbedingungen der oben beschriebene Effekt eine für die Sicherheitsfunktion inakzeptable Einschränkung darstellen, so empfehlen wir die Konfiguration „Abschaltung in der Drehmomentendlage“ oder „keine Abschaltung“ für die Sicherheitsfahrt zu verwenden.

Projektierung bei der Verwendung der „sicheren Endlagenrückmeldung“

Ausschließlich bei der Version 22Y stehen sichere Endlagenrückmeldungen zur Verfügung. Für die sichere Endlagenrückmeldung dürfen nur die direkt auf den Kundenausgang geführten mechanischen Endlagenschalter verwendet werden. Die Meldungen an den DOUT 1 – DOUT 6 Ausgängen des I/O Interfaces, die mit AOUT bezeichneten analogen Ausgänge und die Feldbusschnittstellen der AC. 2 / ACExC .2 stellen keine sicheren Rückmeldungen im Sinne der Funktionalen Sicherheit dar.

Information Bei der Sicherheitsfunktion „Sichere Endlagenrückmeldung“ ist zu beachten, dass die Signalisierung über mechanische Schalter erfolgt. Da diese Elemente eine unvermeidliche Hysterese haben, verlässt der Stellantrieb die Endlage minimal bevor die Endlagenmeldung gelöscht wird. Folglich gibt es einen an die Sicherheitsposition angrenzenden Bereich der Stellantriebspositionen, in dem bei Fahren aus der Sicherheitsposition heraus noch die Endlage gemeldet wird, der Stellantrieb diese aber bereits verlassen hat. Wird der fragliche Bereich aus der Gegenrichtung erreicht, so besteht die beschriebene Einschränkung nicht. Normalerweise ist dieser Bereich klein, er kann jedoch in ungünstigen Konfigurationen (geringe Anzahl Umdrehungen pro Hub) bis über 10 % des Gesamthubs betragen.
Sollte auf Grund ungünstiger Rahmenbedingungen der oben beschriebene Effekt eine für die Sicherheitsfunktion inakzeptable Einschränkung darstellen, so empfehlen wir für die Endlagenmeldung sowohl die Weg- als auch Drehmomentschalter auszuwerten.

Energieversorgung

Information Für die Sicherstellung der Energieversorgung ist der Anlagenbetreiber zuständig.

3.2. Konfiguration (Einstellung)/Ausführung

Die Konfiguration (Einstellung) der sicherheitsbezogenen Funktionen wird werksintern bei der Montage der Stellantriebs-Steuerung definiert und anschließend bei der Endabnahme validiert. Eine nachträgliche Änderung der Konfiguration ist beim Anlagenbetreiber nicht zulässig.

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.

Konfigurationsmöglichkeiten der Sicherheitsfunktion

Tabelle 3:

Konfigurationsmöglichkeiten der Sicherheitsfunktion	
Konfiguration SIL-Funktion	Kurzbeschreibung
Safe ESD ZU/ZU	sicheres SCHLIESSEN
Safe ESD AUF/AUF	sicheres ÖFFNEN
Safe STOP ZU/AUF	sicherer STOPP in Richtung ZU und Richtung AUF
Safe ESD ZU/ZU + Safe STOP ZU/AUF	sicheres SCHLIESSEN und sicherer STOPP in Richtung ZU und Richtung AUF
Safe ESD AUF/AUF + Safe STOP ZU/AUF	sicheres ÖFFNEN und sicherer STOPP in Richtung ZU und Richtung AUF

Bei Konfiguration einer Safe ESD Funktion und einer Safe STOPP Funktion hat bei gleichzeitiger Anforderung beider Sicherheitsfunktionen die Safe ESD Funktion immer Vorrang vor der Safe STOPP Funktion.

Konfigurationsmöglichkeiten der Abschaltart

Information

Die Abschaltart der Standard Stellantriebs-Steuerung sollte wie in den folgenden Tabellen konfiguriert sein.

Tabelle 4:

bei Stellantrieben mit elektromechanischer Steuereinheit		
Konfiguration SIL-Abschaltart	Kurzbeschreibung	Konfiguration Abschaltart Standard Stellantriebs-Steuerung
1: keine Abschaltung	Keine Abschaltung durch Weg- oder Drehmomentschalter bei einer Sicherheitsfahrt	frei wählbar
2: Abschaltung in der Drehmoment-Endlage	Sicherheitsfahrt wird durch gemeinsames Auslösen von Drehmoment- und Wegschalter gestoppt	drehmomentabhängig
3: Abschaltung in der Weg-Endlage	Sicherheitsfahrt wird durch Auslösen der Wegschalter gestoppt	wegabhängig
4: wegabhängige Abschaltung mit Überlastschutz	Sicherheitsfahrt wird durch Auslösen der Wegschalter und/oder der Drehmomentschalter (Überlastschutz) gestoppt	wegabhängig

Tabelle 5:

bei Stellantrieben mit elektronischer Steuereinheit MWG		
Konfiguration SIL-Abschaltart	Kurzbeschreibung	Konfiguration Abschaltart Standard Stellantriebs-Steuerung
1: keine Abschaltung	Keine Abschaltung durch Weg- oder Drehmomentschalter bei einer Sicherheitsfahrt	frei wählbar

Tabelle 6:

bei Stellantrieben mit elektronischer Steuereinheit MWG mit Wegschaltern		
Konfiguration SIL-Abschaltart	Kurzbeschreibung	Konfiguration Abschaltart Standard Stellantriebs-Steuerung
3: Abschaltung in der Weg-Endlage	Sicherheitsfahrt wird durch Auslösen der Wegschalter gestoppt	wegabhängig

Konfigurationsmöglichkeiten Motorschutzauswertung

Tabelle 7:

Konfigurationsmöglichkeiten Motorschutzauswertung	
Konfiguration SIL-Motorschutz	Kurzbeschreibung
aktiv	Ein Auslösen des Motorschutzes (Thermofehler) stoppt bzw. verhindert eine Sicherheitsfahrt
inaktiv	Motorschutz hat keine Auswirkung auf die Sicherheitsfahrt

Information Die Konfiguration „SIL-Motorschutz“ = „inaktiv“ wird nur auf explizite Anforderung eingestellt. Diese Ausführung erfüllt nicht die Ex-Zulassung.

Information Wenn Weg- und/oder Drehmomentschalter für die Endlagen vorhanden sind, ist deren exakte Einstellung unbedingt erforderlich um eine korrekte Funktion der „Sichere Endlagenrückmeldung“ bzw. der „ESD Funktion“ zu gewährleisten. Details zur Einstellung der entsprechenden Schalter können der Betriebsanleitung entnommen werden.

Konfiguration der Diagnosen „Reaktionsüberwachung“ und „Partial Valve Stroke Test (PVST)“

Je nach Art der vorgesehenen Diagnose müssen die Konfigurationen für die Reaktionsüberwachung mittels Blinker bzw. den Partial Valve Stroke Test überprüft und gegebenenfalls angepasst werden.

Die detaillierten Konfigurationsmöglichkeiten und Informationen zum Partial Valve Stroke Test (PVST) finden Sie im Handbuch (Betrieb und Einstellung) AUMATIC AC 01.2. Bitte beachten Sie, dass die Reaktionsüberwachung nur über die Blinkschaltung/SIL-Fehlermeldung und **nicht** über die Reaktionsüberwachung der AC .2-Firmware erfolgen darf.

3.3. Absicherung gegen unkontrollierte Bewegung (Selbsthemmung/Bremse)

Bei selbsthemmenden AUMA Stellantrieben kann davon ausgegangen werden, dass bei einer Belastung bis zum maximalen Drehmoment keine unkontrollierte Bewegung der Armatur aus dem Stillstand heraus aufgrund der Drehmomentbelastung der Armatur erfolgt. Insofern ist in diesen Fällen eine weitere Absicherung gegen unkontrollierte Bewegung nicht unbedingt erforderlich. Dies kann notwendig werden, wenn z.B. auf Grund von Vibrationen die Selbsthemmung möglicherweise nicht gewährleistet bzw. nicht hinreichend ist. Bestimmte Anwendungen können darüber hinaus trotzdem eine aktive Sicherung der Position z.B. durch eine Bremse erfordern. Außerdem gibt es anwendungsspezifische Normen, die dies fordern. Aus diesem Grund muss projektspezifisch geprüft werden, ob eine weitere Sicherung erforderlich ist. In jedem Fall ist diese bei Stellantrieben ohne Selbsthemmung erforderlich.

Tabelle 8: Übersicht Selbsthemmung bei AUMA Stellantrieben (zum Zeitpunkt der Drucklegung)

Typ	Abtriebsdrehzahl		Selbsthemmung
	50 Hz	60 Hz	
SA 25.1 – SA 30.1 SAEx 25.1 – SAEx 30.1	≤ 90 1/min.	≤ 108 1/min.	selbsthemmend
	≥ 125 1/min.	≥ 150 1/min.	NICHT selbsthemmend
SA 35.1 SAEx 35.1	≤ 22 1/min.	≤ 26 1/min.	selbsthemmend
	≥ 32 1/min.	≥ 38 1/min.	NICHT selbsthemmend
SA 40.1 SAEx 40.1	≤ 22 1/min.	≤ 26 1/min.	selbsthemmend
	≥ 32 1/min.	≥ 38 1/min.	NICHT selbsthemmend

Werden nicht hinreichend selbsthemmende Stellantriebe in Kombination mit der SIL-Abschaltart „Abschaltung in Drehmoment-Endlage“ für die Sicherheitsfunktion verwendet, so kann folgender Effekt entstehen: Der Stellantrieb fährt bei ESD in die Endlage und schaltet auf Grund von Erreichen der Wegposition und des Abschaltdrehmoments ab. Danach entspannt sich der Getriebezug und das Drehmoment sinkt unter den eingestellten Grenzwert. Der Stellantrieb erkennt dies – korrekterweise – als Verlassen der ESD-Bedingungen und schaltet den Stellantrieb

wieder ein. Dieser baut zusätzlichen Drehmoment auf bis die Abschaltbedingung wieder erreicht ist, usw. Es kommt zu einem „Pumpen“ des Stellantriebs.

Um diesen Effekt zu vermeiden, empfehlen wir entweder Stellantriebe oder andere Elemente mit hinreichender Selbsthemmung im Getriebezug zu verwenden oder – falls prozess- und sicherheitstechnisch möglich – „Abschaltung in der Weg-Endlage“ für die Sicherheitsfunktion zu wählen.

3.4. Betriebsart (low/high demand mode)

Die Sicherheitsfunktionen der von AUMA gelieferten Stellantriebe sind für die Betriebsart mit niedriger Anforderungsrate (low demand mode) ausgelegt und dürfen nur in dieser Betriebsart verwendet werden. Falls zusätzlich zur Sicherheitsfunktion über den gleichen Stellantrieb auch eine nicht-sicherheitstechnische Funktion der Betriebs- und Überwachungseinrichtung ausgeführt wird, so muss beachtet werden, dass auch bei Berücksichtigung der Summe aus nicht-sicherheitstechnischer Funktion, notwendigen Tests und Sicherheitsfunktion die für den jeweiligen Stellantrieb definierte maximal zulässige Anzahl an Schaltspielen[1)] sowie die maximal zulässige Anzahl der Anläufe[2)] während des Einsatzes des Stellantriebs in einem sicherheitstechnischen System nicht überschritten werden darf.

3.5. Weitere Hinweise und Angaben zur Projektierung

Die HFT ist 0.

Eventuell im Stellantrieb verbaute Stellungsgeber MWG, RWG, EWG dürfen nicht in ein sicherheitstechnisches System eingebunden werden.

Die Sicherheitsfunktionen des Stellantriebs können als Typ A Gerät angesehen werden.

Die Stellzeit für den vollen Hub muss größer 4 Sekunden betragen. ACHTUNG: Eine Veränderung des nominellen Hubs verändert auch die Stellzeit.

Die Sicherheitsfunktion(en) und Ihre Rückmeldungen dürfen ausschließlich über die digitalen Ein- und Ausgänge des SIL-Moduls bzw. die direkt auf den Kundenanschluss geführten Endlagenschalter erfolgen.

Die Meldung über den Ausgang `SIL-Fehler` muss kontinuierlich ausgewertet werden. Meldet dieser einen Fehler ist von einer nicht-Verfügbarkeit der Sicherheitsfunktion auszugehen. Die Sicherheitsfunktion ist dann umgehend zu prüfen. Möglicherweise sind weitere Sicherungsmaßnahmen zu ergreifen bis die Sicherheitsfunktion wieder fehlerfrei funktioniert.

3.6. Einsatzbedingungen (Umweltbedingungen)

Bei der Projektierung und beim Einsatz der Stellantriebe 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. Bei einer Durchschnittstemperatur von +60 °C beträgt dieser Faktor 2,5.

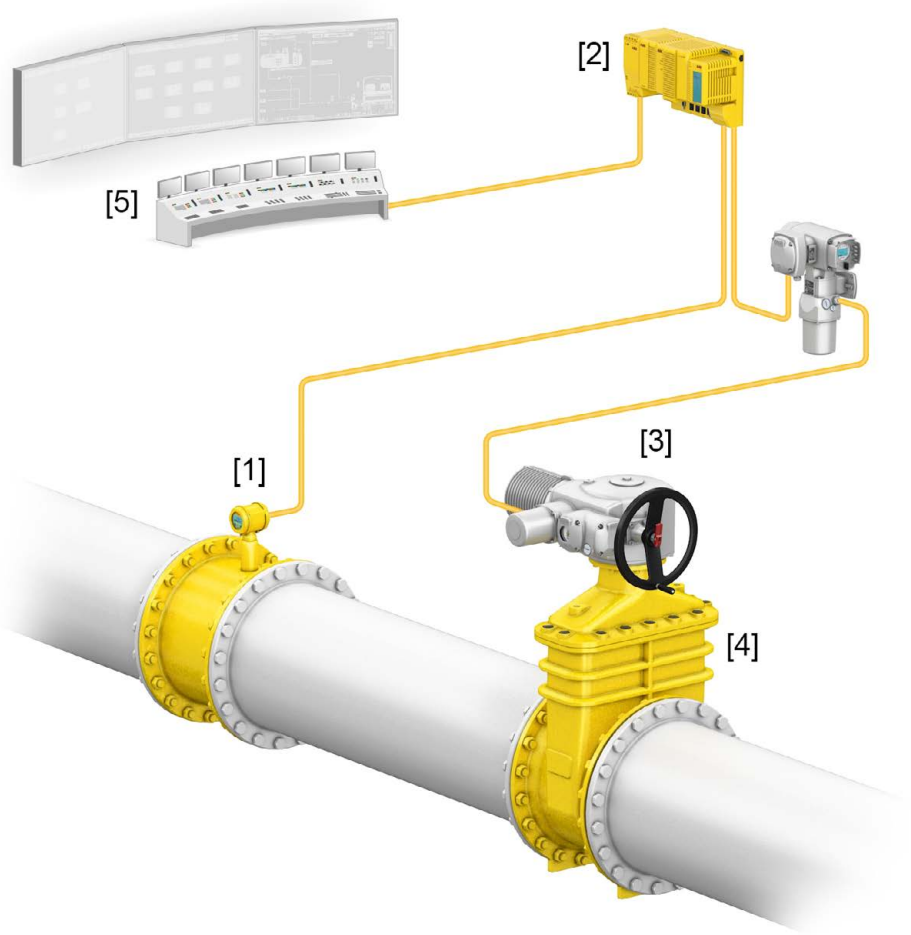
1) Definition von “Schaltspiele” gemäß DIN EN 15714-2:2010
2) Definition von “Anläufe” gemäß DIN EN 15714-2:2010

4. Sicherheitstechnisches System und Sicherheitsfunktionen

4.1. Sicherheitstechnisches System mit einem Stellantrieb

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

Bild 3: Typisches sicherheitstechnisches System



[1] Sensor
[2] Steuerung (Sicherheits-SPS)
[3] Stellantrieb (mit Stellantriebs-Steuerung auf Wandhalter)
[4] Armatur
[5] Prozessleitsystem

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

Für eine einzelne Komponente (z.B. einem Stellantrieb) 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 Funktion (**E**mergency **S**hut **D**own): sicheres ÖFFNEN/SCHLIESSEN
  - Durch redundante Signale Safe ESDa und Safe ESDb (Standard: Low Akiv) fährt der Stellantrieb unabhängig von der Wahlschalterstellung in die konfigurierte Richtung (AUF/ZU).

- Safe STOP Funktion: sicherer STOPP
  - Ein Fahrbefehl der Standard Stellantriebs-Steuerung (in Richtung AUF oder ZU) wird nur dann ausgeführt, wenn ein zusätzliches Freigabsignal für den Fahrbefehl anliegt.
  - Falls das Freigabesignal fehlt, wird eine Fahrt in Richtung AUF bzw. ZU gestoppt (Motor wird abgeschaltet).
  - Die Safe STOP Funktion wirkt auf alle Fahrbefehle der Standard Stellantriebs-Steuerung unabhängig von deren Befehlsquelle (z.B. Fern oder Ort).
- Safe ESD Funktion kombiniert mit Safe STOP Funktion
  - Die Safe ESD Funktion besitzt höhere Priorität, d.h. bei gleichzeitiger Aktivierung beider Funktionen fährt der Stellantrieb in die konfigurierte Richtung (AUF/ZU).
- Nur Version 22Y: „Sichere Endlagenrückmeldung“
  - Es ist eine direkt auf den Stellantrieb verdrahtete Endlagenmeldung vorhanden. Die Sicherheitsfunktion ist die korrekte Meldung, dass der Stellantrieb sich in der fraglichen Endlage des Stellantriebs befindet oder nicht.[3)] Nur die Meldung über diesen Meldeweg ist sicherheitsrelevant. Eine Endlagenmeldung über die Relais des I/O Interface, über einen Stellungsgeber (RWG, MWG, Potentiometer, ...) oder über eine Feldbusschnittstelle stellt keine Sichere Endlagenmeldung dar.

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

4.3. Sichere Ein- und Ausgänge

Sichere Eingänge für sicheres ÖFFNEN/SCHLIESSEN (Safe ESD Funktion):

- `Safe ESDa`
- `Safe ESDb`

Sichere Eingänge für sicheren Stopp (Safe STOP Funktion):

- `Safe STOP AUF`
- `Safe STOP ZU`

Sichere Ausgänge (Anzeige, dass die Sicherheitsfunktion möglicherweise nicht ausgeführt werden kann:

- `SIL Fehler`
- `SIL Bereit`

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 Stellantriebs-Steuerung in Version 22X oder 22Y in das sicherheitstechnische System eingebaut werden. Welche Variante gewählt werden muss ist vom Gesamtsystem abhängig.

Information

Abhängig von der Sicherheitsfunktion und von der auf der Anlage vorgesehenen sicherheitstechnischen Aufgabe dieser Sicherheitsfunktion ist in jedem einzelnen Anwendungsfall zu prüfen, ob und ggf. in welcher Konfiguration durch die Verwendung mehrerer Stellantriebe tatsächlich eine HFT>0 erzielt wird. Dies gilt insbesondere – aber nicht nur – für die Sicherheitsfunktion Safe STOP.

Ein mögliches Beispiel für sicheres SCHLIESSEN bzw. sicheres ÖFFNEN ist in Bild 3 und 4 gezeigt. Ein weiteres Beispiel, bei dem durch mehrere Stellantriebe **keine** Redundanz erzielt werden kann, ist eine Safe STOP Funktion, die dazu dient, die Bewegung mechanischer Anlagenteile sicher auszuschließen, wenn in einer

3) Bitte beachten, dass die sicherheitstechnischen Kennzahlen nur die Komponenten des Stellantriebs beinhalten. Weitere ggf. zu betrachtende Komponenten (z.B. Integrität von externen Steuerungen, Getrieben, Armaturenschaft, andere Komponenten der Armatur, …) sind in den von AUMA angegebenen Kennzahlen dieses Produktes nicht berücksichtigt.

Notsituation z.B. die Feuerwehr den fraglichen Anlagenteil betreten muss. Die Verwendung von 2 Stellantrieben führt hier in aller Regel nicht zu einem 1oo2, sondern zu einem 2oo2 System im Sinne der zu erzielenden Sicherheitswirkung. Somit wird die HFT in diesem Fall nicht erhöht.

Bild 4: Redundantes System mit Safe ESD für sicheres SCHLIESSEN

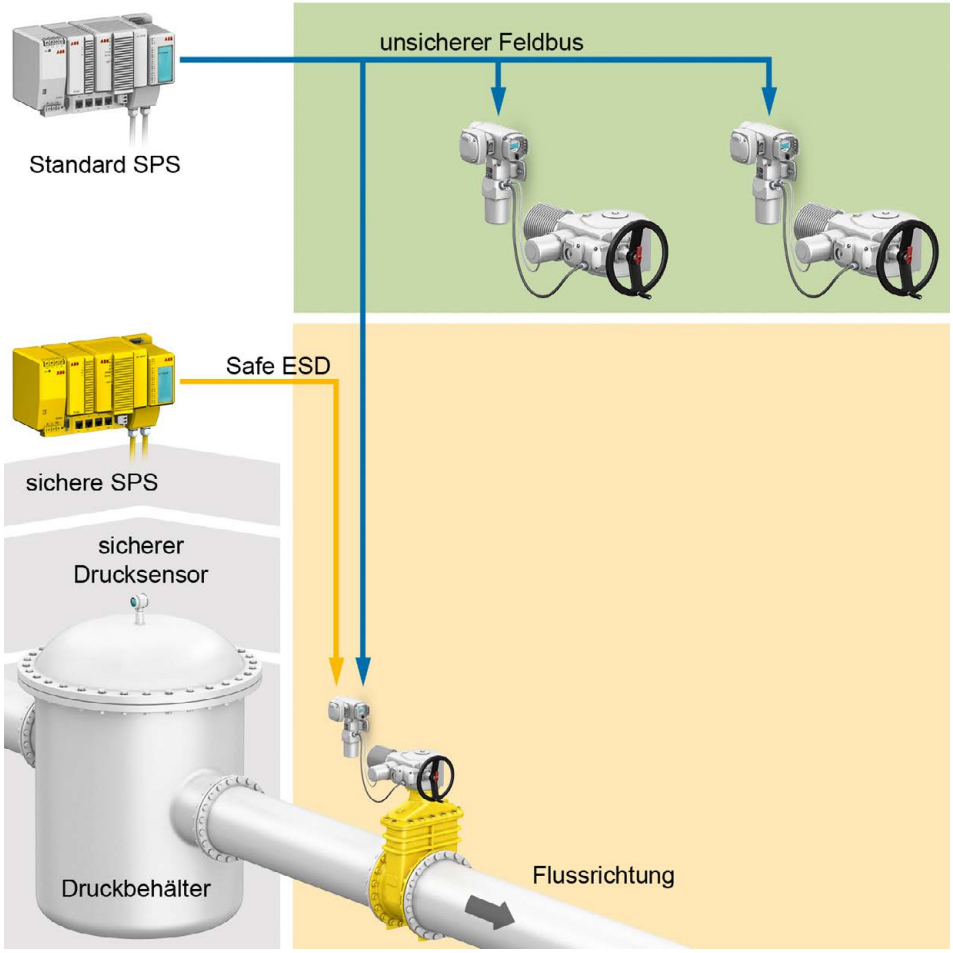
Bild 5: Redundantes System mit Safe ESD für sicheres ÖFFNEN

4.5. Anwendungsbeispiele

Sicheres Öffnen eines Druckbehälters mit der Safe ESD Funktion

Die Standard SPS steuert das gesamte System. Wenn der Druck im System unzulässig groß wird, muss von einem Fehler im System ausgegangen werden. In diesem Falle öffnet die sichere SPS sofort das Ventil, um den Druck sicher zu reduzieren.

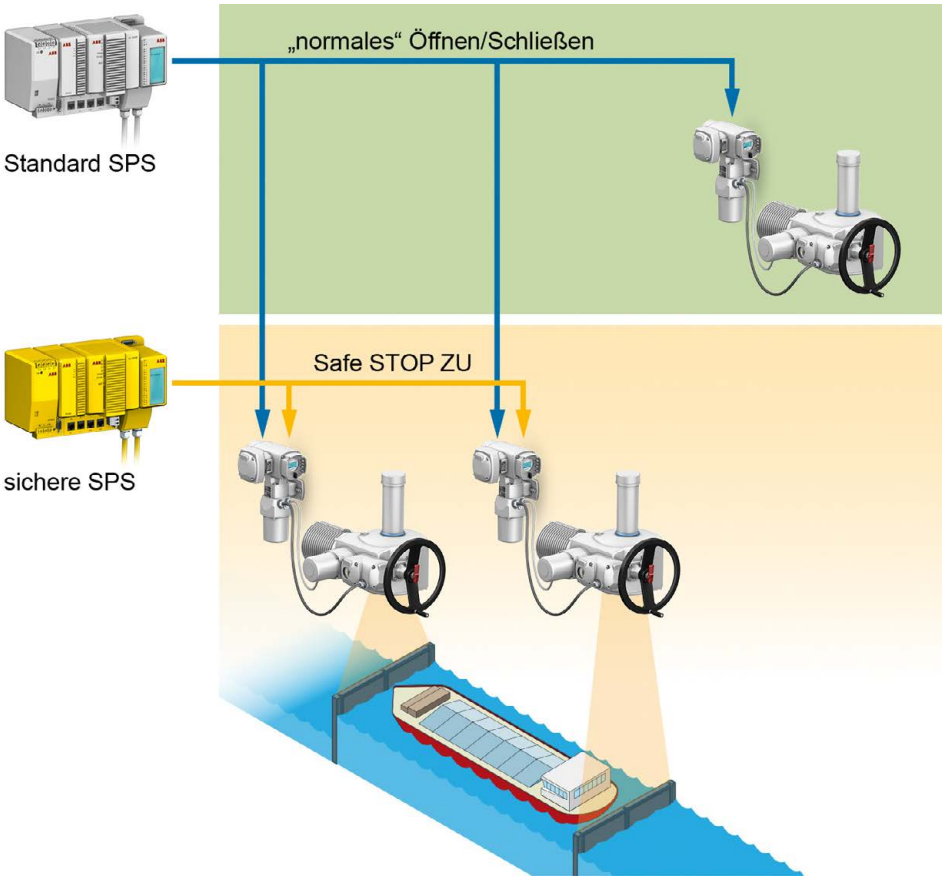
Bild 6: Anwendungsbeispiel: Druckbehälter



Sicherer Stopp der Schleuse als Schutz vor Zerstörung mit der Safe STOP Funktion

Im Bereich Schiffsschleusen steht die Betriebssicherheit im Vordergrund (Verhindern von Gefahren für Menschen und Anlagen). Wenn die Schleuse schließt, darf sich kein Boot mehr zwischen den Schleusenflügeln befinden. Andernfalls wird die Safe STOP Funktion (z.B. via NOT HALT Schalter) ausgeführt.

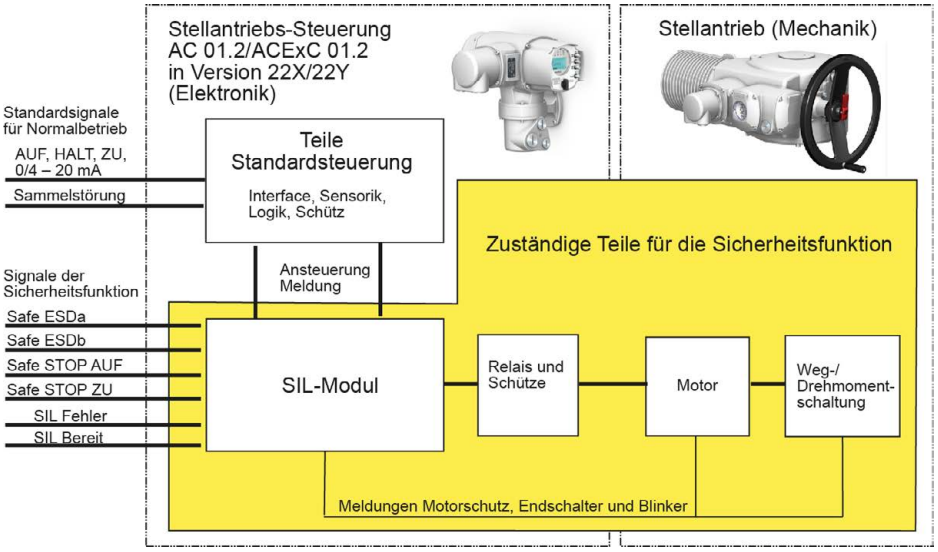
Bild 7: Anwendungsbeispiel: Schleuse



4.6. Systemdarstellung

Die folgende Darstellung stellt einen vereinfachten Aufbau einer AC 01.2/ACExC 01.2 in Version 22X oder 22Y dar.

Bild 8: Vereinfachte Systemdarstellung



5. Installation, Inbetriebnahme und Betrieb

Information Installation und Inbetriebnahme müssen durch einen Montagebericht und ein Abnahmeprüfzeugnis dokumentiert werden. Die Installation und Inbetriebnahme darf nur durch autorisiertes Fachpersonal erfolgen, das in Funktionale Sicherheit geschult ist.

Für die Sicherstellung der Energieversorgung mit Über- und Unterspannungsschutz, während dem Ausführen einer Sicherheitsfunktion, ist der Anlagenbetreiber zuständig.

5.1. Installation

Information Die in diesem (und auch in anderen) Kapiteln genannten PIN-Belegungen (XK ...) sind die Standardbelegungen der AC 01.2-22X/-22Y / ACExC 01.2-22X/-22Y. In einigen Konfigurationen wird jedoch von dieser typischen Belegung abgewichen um besondere Ausstattungswünsche zu erfüllen. Im Zweifel gilt immer die auf dem zum jeweiligen Produkt gehörenden Schaltplan angegebene Belegung.

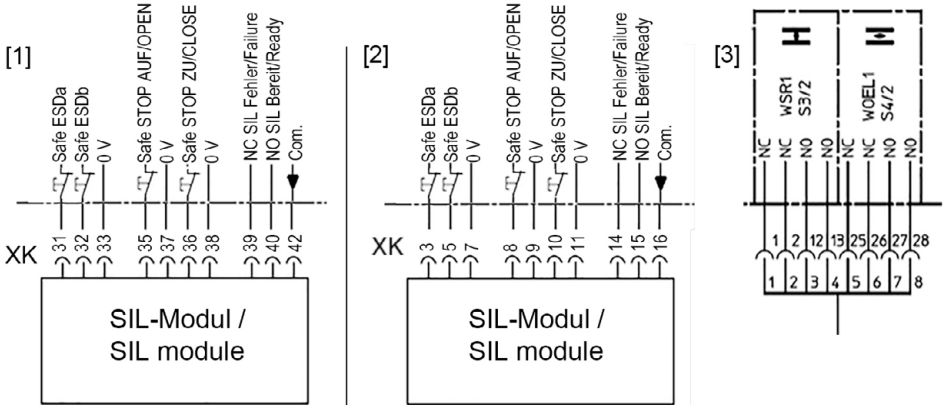
Die allgemeine Installation (Montage, Elektroanschluss) muss entsprechend der zum Gerät zugehörigen Betriebsanleitung und dem beigefügten, auftragsbezogenen Schaltplan durchgeführt werden.

Bei Betrieb oder Lagerung unterhalb Umgebungstemperaturen von –25 °C ist das integrierte Heizsystem mit Spannung zu versorgen.

Die Sicherheitsfunktionen werden über das SIL-Modul, welches in der Stellantriebs-Steuerung AC 01.2 / ACExC 01.2 eingebaut ist, angeschlossen.

Der SIL-Fehler muss mit dem geforderten SIL Level entsprechenden kompatiblen Eingang einer Sicherheits-SPS verbunden und ausgewertet werden.

Bild 9: Anschlüsse für Sicherheitsfunktionen über das SIL-Modul sowie die direkt verdrahtete Sichere Endlagenrückmeldung



[1] Typische Anschlussbelegung bei Ansteuerung parallel

[2] Typische Anschlussbelegung bei Ansteuerung über Feldbus

[3] direkt verdrahtete Sichere Endlagenrückmeldung

Schaltverhalten der Eingänge `Safe ESDa/ESDb` und `Safe STOP AUF/ZU`:

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

Information Die Eingänge Safe ESDa und Safe ESDb sind redundante Eingänge für die gleiche Sicherheitsfunktion (je nach Konfiguration ESD AUF oder ESD ZU). An ihnen sollte deshalb immer der gleiche Pegel (high bzw. low) anliegen. Liegt an einem der beiden Eingänge ESDa und ESDb „high“ und am anderen „low“ an, so stellt dies einen Fehlerzustand des sicherheitstechnischen Systems dar. Der Antrieb meldet in diesem Fall „SIL-Fehler“. Da nicht klar ist, ob der Eingang mit „high“- oder derjenige mit „low“-Pegel fehlerhaft ist, wird in diesem Fall aus Sicherheitsgründen die Sicherheitsfunktion ausgeführt.

Information Die Eingänge Safe STOP AUF und Safe STOP ZU stellen zwei unabhängige Eingänge mit unabhängiger Funktionalität dar:

- Wenn Safe STOP AUF = low-Pegel, so verhindert die Sicherheitsfunktion Fahrten in Richtung AUF (Ausnahme ESD AUF)
- Wenn Safe STOP ZU = low-Pegel, so verhindert die Sicherheitsfunktion Fahrten in Richtung ZU (Ausnahme ESD ZU)

Zulässiger Spannungsbereich der Eingänge:

- High-Pegel: 15 – 30 V DC
- Low-Pegel: maximal 5 V DC

Meldeverhalten der Ausgänge `SIL-Bereit` und `SIL-Fehler`:

- SIL-Bereit/ Es liegt kein von der Diagnose detektierter Fehler vor:
  Ausgang NO (Schließer-Kontakt) = **geschlossen**
  Ausgang NC (Öffner-Kontakt) = **offen**
- SIL-Fehler/ Es liegt ein von der Diagnose detektierter Fehler vor:
  Ausgang NO (Schließer-Kontakt) = **offen**
  Ausgang NC (Öffner-Kontakt) = **geschlossen**

Bezeichnung Schaltplan	**Signal**	**Kundenschlüsse bei Ansteuerung (typische Belegung)**	
		[1] Parallel	**[2] Feldbus**
Safe ESDa	Digitaler Eingang für Safe ESD Funktion	XK 31	XK 3
Safe ESDb	Redundanter Eingang für Safe ESD Funktion	XK 32	XK 5
0 V	Bezugspotential für Safe ESDa und Safe ESDb	XK 33	XK 7
Safe STOP ZU	Digitaler Eingang für die Safe STOP Funktion in Richtung ZU	XK 35	XK 8
0 V	Bezugspotential für Safe STOP ZU	XK 37	XK 9
Safe STOP AUF	Digitaler Eingang für die Safe STOP Funktion in Richtung AUF	XK 36	XK 10
0 V	Bezugspotential für Safe STOP AUF	XK 38	XK 11
SIL-Bereit	Schließer Kontakt der Meldung SIL-Fehler	XK 40	XK 15
SIL-Fehler	Öffner Kontakt der Meldung SIL-Fehler	XK 39	XK 14
Com.	Bezugspotential für die Meldung SIL-Fehler	XK 42	XK 16

Über den Ausgang `SIL-Fehler` angezeigte SIL-Fehler

Fehlerursachen SIL	**Beschreibung**
Thermofehler	Motorschutz angesprochen
Drehmomentfehler	Drehmomentfehler in Richtung ZU und/oder AUF
Fehler Stellungsrückmeldung	Aktuelle Stellungsrückmeldung ist außerhalb des zulässigen Bereichs.
Phasenausfall	Eine Phase der Spannungsversorgung ist ausgefallen. Die Steuerung ist ohne Netzspannung.
Phasenfolgefehler	Die Außenleiteranschlüsse L1, L2 und L3 sind in der falschen Reihenfolge angeschlossen.
Fehler Spannungsversorgung	Der sicherheitsbezogene Teil der Steuerung ist ohne Spannungsversorgung.
Temperaturfehler	Temperatur im Steuerungsgehäuse zu hoch. Ausfall des Heizsystems bei Umgebungstemperatur unterhalb –25 °C.

Fehlerursachen SIL	Beschreibung
Fehler Antriebsüber-wachung	Antrieb oder Armatur verriegelt.
Fehler Redundante Verdrahtung Safe ESD	Beide Signale Safe ESDa und Safe ESDb sind nicht gleichzeitig auf demselben Pegel.
Interner Fehler	Interner Fehler des SIL-Moduls

Weitere Informationen zu SIL-Fehlern und insbesondere zur Unterstützung bei der Fehlersuche siehe Kapitel <Meldungen>.

Installation und Inbetriebnahme müssen dokumentiert und ein abschließender Installations- und Inbetriebnahmebericht erstellt werden.

Information Die Grundfunktion “automatische Drehrichtungskorrektur” steht in dieser Ausführung nicht zur Verfügung. Beim Anschluss der Spannungsversorgung muss daher darauf geachtet werden, dass die Phasen L1, L2 und L3 richtig angeschlossen werden. Zum Prüfen der Drehrichtung siehe Betriebsanleitung zum Stellantrieb.

Die Option “externe Versorgung der Elektronik” der Stellantriebs-Steuerung bezieht sich auf den Teil der Standard Stellantriebs-Steuerung. Das SIL-Modul wäre bei einem Netzausfall trotz externer Versorgung der Elektronik nicht mehr im Betrieb.

Information Die Einstellung der Wegschalter bei der Ausführung mit elektronischer Steuereinheit mit SIL-Wegschaltern erfolgt leicht unterschiedlich von der bei der elektromechanischen Steuereinheit gewohnten Einstellung. Für die korrekte Einstellung gibt es ein Zusatzblatt zur Betriebsanleitung (Y006.238).

5.2. Inbetriebnahme

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

Information Bei der Safe ESD Funktion ist eine Fahrt in die sichere Position unabhängig von der Wahlschalterstellung (ORT - AUS - FERN) oder dem Betriebszustand möglich. D.h. auch in den Stellungen ORT und AUS oder beim Systemstart wird der Antrieb bei Anforderung der Sicherheitsfunktion losfahren.

⚠ VORSICHT

Stellantrieb kann beim Einschalten sofort losfahren!

Personenschäden oder Schäden an Armatur möglich.

→ Sicherstellen, dass beim Einschalten an den Eingängen `Safe ESDa/ESDb` ein **High-Pegel** (Standard: +24 V DC) anliegt.

Nach der Inbetriebnahme muss eine Überprüfung auf sichere Funktion des Antriebs erfolgen. Siehe Kapitel <Proof-Test >.

⚠ VORSICHT

Falls der Stellantrieb über einen längeren Zeitraum mit ausgekuppeltem Motor läuft, führt dies zu erheblichem Verschleiß des Stellantriebs und im schlimmsten Fall zu unbeabsichtigtem Losfahren, zu ungewolltem Mitlaufen des Handrads oder zu einer Zerstörung des Stellantriebs!

Personenschäden oder Schäden am Stellantrieb möglich.

→ Durch betriebliche Maßnahmen sicherstellen, dass der Motor (mit Ausnahme des Proof-Tests) nicht im ausgekuppelten Zustand betrieben wird.

→ Motor nur kurzfristig während des Proof-Tests im ausgekuppelten Zustand betreiben.

Inbetriebnahme-Checkliste

Tabelle 9: Inbetriebnahme-Checkliste

1. Antrieb und Steuerung korrekt verdrahtet?	□ ✓
2. Weg- und Drehmomentschaltung eingestellt?	□ ✓
3. Sichere Funktion (je nach Konfiguration) anhand der Proof-Test-Checklisten geprüft?	□ ✓
4. Inbetriebnahme der Grundeinstellungen (Standard Stellantriebs-Steuerung) entsprechend der Betriebsanleitung durchgeführt?	□ Ja □ Nein
☒ ✓ = ausgeführt	

5.3. Betrieb

Voraussetzung für einen sicheren Betrieb ist die regelmäßige Wartung und die Überprüfung des Gerätes in den festgelegten 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 und das Handbuch (Betrieb und Einstellung) AC 01.2/ACExC 01.2 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. Diese liegt in der Verantwortung des Betreibers, der geeignete Maßnahmen zu ergreifen hat. Gerne unterstützen wir Sie auf Anfrage bei der Identifikation geeigneter Maßnahmen.

5.5. Außerbetriebsetzung

Falls der Antrieb 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.

6. Anzeigen im Display

Dieser Abschnitt enthält Anzeigen der Standard Stellantriebs-Steuerung, die nur in der Version 22X oder 22Y möglich sind.

Allgemeine Anzeigen und deren Einstellung bzw. Bedienung sind in der zum Gerät zugehörige Betriebsanleitung, sowie im Handbuch (Betrieb und Einstellung) 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.

6.1. Statusanzeigen zu den SIL-Funktionen

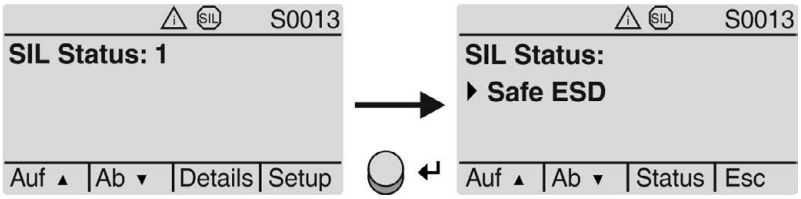
Die Stellantriebs-Steuerung kann Statusinformationen zu den sicherheitsbezogenen Funktionen im Display anzeigen.

SIL-Status (S0013)

Die Anzeige S0013 meldet den Zustand der Sicherheitsfunktionen und der SIL-Fehlermeldung.

Falls das SIL-Symbol in der Kopfzeile des Displays angezeigt wird, ist eine der folgenden drei Meldungen aktiv: Safe ESD, Safe STOP oder SIL-Fehler.

Bild 10: Zustand Sicherheitsfunktionen und SIL-Fehlermeldung



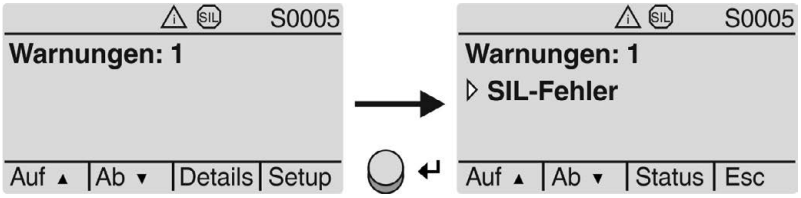
Statusanzeige im Display	Zustand
Safe ESD	Safe ESD Funktion (sicheres ÖFFNEN/SCHLIESSEN) ist aktiv: Stellantrieb fährt in die konfigurierte Richtung (ZU/AUF) (Eingänge Safe ESDa/Safe ESDb = 0 V bzw. offen)
Safe STOP	Safe STOP Funktion ist aktiv, Antrieb stoppt (Eingang Safe STOP AUF bzw. Safe STOP ZU = 0 V bzw. offen)
SIL-Fehler	SIL-Fehlermeldung aktiv, d.h. möglicherweise Probleme beim Ausführen einer Sicherheitsfunktion (Safe ESD bzw. Safe STOP)

Warnungen (S0005)

Die Anzeige S0005 zeigt die Anzahl der aufgetretenen Warnungen.

Falls ein SIL-Fehler auftritt, wird die Meldung SIL-Fehler in der Anzeige S0005 aufgelistet. Unter Details > Status sind weiter Details abrufbar.

Bild 11: Warnung: SIL-Fehler

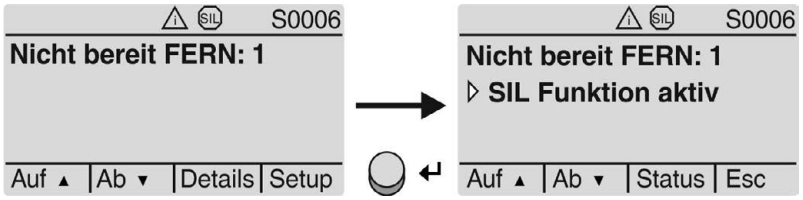


Nicht bereit FERN (S0006)

Die Anzeige S0006 zeigt die Anzahl der aufgetretenen Meldungen, die zur Gruppe Nicht bereit FERN gehören.

Falls eine Sicherheitsfunktion aktiv ist (Safe ESD oder Safe STOP), wird die Meldung SIL-Funktion aktiv in der Gruppe Nicht bereit FERN aufgelistet. Unter Details > Status sind weitere Details abrufbar.

Bild 12: Meldung: Sicherheitsfunktion aktiv



Information

Sobald eine Sicherheitsfunktion aktiv ist (Meldung SIL-Funktion aktiv), wird der Antrieb über die sichere SPS und das SIL-Modul angesteuert. Für die „normale Ansteuerung“ (Standard SPS) ist die Steuerung daher „Nicht bereit FERN“.

6.2. SIL-Konfigurationswarnung

Folgende Konfigurationen bzw. Einstellungen an der Standard Stellantriebs-Steuerung können in Verbindung mit den Sicherheitsfunktionen Einfluss auf die Standardfunktionen haben:

- Selbsthaltung Ort M0076 = AUF/ZU
- Selbsthaltung Fern M0100 = AUF/ZU

Wird in der Standard Stellantriebs-Steuerung eine dieser Konfigurationen gewählt, erzeugt die Steuerung bis zur Firmwareversion 5.08.xx die Warnung Konfig. SIL.

6.3. Hintergrundbeleuchtung

Im Normalbetrieb ist die Beleuchtung im Display der Stellantriebs-Steuerung weiß. Bei einem Fehler leuchtet die Displayanzeige rot. Die rote Hintergrundbeleuchtung bezieht sich NICHT auf den Zustand der sicheren Funktion, sondern auf Fehler, die im Handbuch (Betrieb und Einstellung) AC 01.2/ACExC 01.2 als „Fehler“ bezeichnet werden.

7. Meldungen

7.1. Meldungen über das SIL-Modul

Das integrierte SIL-Modul meldet über ein Fehlerrelais (Ausgänge `SIL-Bereit` bzw. `SIL-Fehler`) einen SIL-Fehler. Nur diese Signale dürfen in einem sicherheitsbezogenen System verwendet werden.

Für das Meldeverhalten der Ausgänge `SIL-Bereit/SIL-Fehler` siehe Kapitel <Installation>.

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

7.2. Meldung SIL-Fehler über das Display der Standard Stellantriebs-Steuerung (zur Unterstützung bei der Fehlersuche)

Falls über das Fehlerrelais des SIL-Moduls (Ausgänge `SIL-Bereit` bzw. `SIL-Fehler`) ein SIL-Fehler gemeldet wird, kann mit Hilfe der Anzeige im Display der Standard Stellantriebs-Steuerung der genaue Fehler ermittelt werden. Für Details zu allen Fehlermeldungen und Warnungen die über das Display der Standard Stellantriebs-Steuerung angezeigt werden siehe Handbuch (Betrieb und Einstellung) AUMATIC AC 01.2.

Das Fehlerrelais des SIL-Moduls dient als Sammelmeldung für die in der folgenden Tabelle aufgeführten Fehler.

Tabelle 10: Einzelmeldungen der Sammelmeldung SIL-Fehler

Anzeige im Display Standard Stellantriebs-Steuerung	**Beschreibung/ Fehlerursache**	**Auswirkung auf Sicherheitsfunktion → Abhilfe**
Thermofehler	Motorschutz hat angesprochen.	Bei Ausführung **“SIL-Motorschutz” = aktiv**: • Die sichere Funktion Safe ESD kann nicht ausgeführt werden. • Wird der Fehler während einer Sicherheitsfahrt ausgelöst, wird die Fahrt gestoppt. **Abhilfe** → Abkühlen, abwarten.
Drehmo Fehler ZU Drehmo Fehler AUF	Drehmomentfehler in Richtung ZU oder in Richtung AUF. Drehmomentfehler in Richtung ZU und in Richtung AUF (gleichzeitig).	Bei Konfiguration **“SIL-Abschaltart” = “wegabhängige Abschaltung mit Überlastschutz”**: • Die sichere Funktion Safe ESD kann nicht ausgeführt werden. • Wird der Fehler während einer Sicherheitsfahrt ausgelöst, wird die Fahrt gestoppt. • Wenn die Ursache für den Drehmomentfehler beseitigt und die Sicherheitsfahrt weiter angefordert ist, so wird die Sicherheitsfahrt sofort, ohne manuellen Reset, fortgesetzt. **Abhilfe** → Fahrbefehl in Gegenrichtung ausführen. → Einstellung der Drehmomentschaltung prüfen. → Prüfen, ob Fremdstoff das Schließen der Armatur verhindert. → Möglicherweise Probleme mit der Armatur.
Wrn Sighub Istpos.	Der aktuelle Signalhub der Stellungsrückmeldung befindet sich außerhalb des zulässigen Bereiches. Beide Wegschalter (AUF und ZU) sind gleichzeitig betätigt. Möglicherweise Defekt an der Mechanik des Antriebs.	Bei Konfiguration **“SIL-Abschaltart” = “wegabhängige Abschaltung mit Überlastschutz”**, **“SIL-Abschaltart” = “Abschaltung in der Weg-Endlage”**, oder **“SIL-Abschaltart” = “Abschaltung in der Drehmoment-Endlage”**: • Die sichere Funktion Safe ESD kann nicht ausgeführt werden. • Wird der Fehler während einer Sicherheitsfahrt ausgelöst, wird die Fahrt gestoppt. **Abhilfe** → Einstellung Untersetzungsgetriebe im Antrieb prüfen. → Bei möglichem Defekt am Antrieb: AUMA Service benachrichtigen.
Phasenfehler	Eine Phase der Spannungsversorgung ist ausgefallen. Die Steuerung ist ohne Netzspannung.	• Die sichere Funktion Safe ESD kann nicht ausgeführt werden. • Die sichere Funktion Safe STOP wird indirekt ausgeführt, da der Motor nicht mehr bestromt wird. **Abhilfe** → Phasen prüfen/anschließen.
Falsche Phasenfolge	Die Außenleiteranschlüsse L1, L2 und L3 sind in der falschen Reihenfolge angeschlossen.	Bei falscher Phasenfolge fährt der Antrieb bei einer Sicherheitsfahrt in die falsche Richtung. **Abhilfe** → Reihenfolge der Außenleiteranschlüsse L1, L2 und L3 durch Vertauschen von zwei Phasen korrigieren.
IE 24 V AC	Fehler der internen 24 V AC Spannungsversorgung. Der sicherheitsrelevante Teil der Steuerung ist ohne Spannungsversorgung.	• Die sichere Funktion Safe ESD kann nicht ausgeführt werden. • Wird der Fehler während einer Sicherheitsfahrt ausgelöst, wird die Fahrt gestoppt. • Die sichere Funktion Safe STOP wird indirekt ausgeführt, da das SIL-Modul nicht mehr bestromt wird. **Abhilfe** → Spannungsversorgung prüfen.
Wrn Temp. Steuerung	Temperatur im Steuerungsgehäuse zu hoch (außerhalb ihres spezifizierten Temperaturbereichs).	Die sicheren Funktionen Safe ESD und Safe STOP können möglicherweise nicht ausgeführt werden. **Abhilfe** → Steuerung abkühlen lassen (Anzeige der aktuellen Temperatur in der Steuerung unter: Diagnose M0022>Gerätetemperaturen M0524>Temp. Steuerung). → Einsatzbedingungen überprüfen.

Anzeige im Display Standard Stellantriebs-Steuerung	Beschreibung/ Fehlerursache	Auswirkung auf Sicherheitsfunktion → Abhilfe
Keine Meldung im Display	Interner Fehler Elektronikbaugruppe SIL-Modul.	Die sicheren Funktionen Safe ESD und Safe STOP können möglicherweise nicht ausgeführt werden. **Abhilfe** → Möglicherweise Defekt am SIL-Modul: AUMA Service benachrichtigen.
	Antriebsüberwachung Antrieb im Handbetrieb verriegelt. Möglicherweise Defekt am Antrieb.	Die sichere Funktion Safe ESD kann möglicherweise nicht ausgeführt werden. **Abhilfe** → Bei möglichem Defekt am Antrieb: AUMA Service benachrichtigen.
	Fehler der redundanten Verdrahtung des Safe ESD Eingangs. Beide Signale Safe ESDa und Safe ESDb sind nicht gleichzeitig auf demselben Pegel.	Die sichere Funktion Safe ESD kann ausgeführt werden. Ein SIL-Fehler wird über den Ausgang `SIL-Fehler` angezeigt. **Abhilfe** → Redundante Ansteuerung der Safe ESD Signale prüfen.

7.3. Zustandsmeldungen über Melderelais (Digitale Ausgänge) der Standard Stellantriebs-Steuerung

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

Information Zustandsmeldungen über die Ausgänge DOUT sind nicht Teil einer Sicherheitsfunktion! Sie dürfen nicht an Stelle von sicherheitsrelevanten Meldungen in einem sicherheitstechnischen System verwendet werden! Sie können jedoch z.B. als zusätzliche Information über die Standard SPS verwendet werden.

Information Werden Digitale Eingänge oder Ausgänge der Standard Stellantriebs-Steuerung mit der Sicherheits-SPS verbunden, so ist unbedingt darauf zu achten, dass eine hinreichende Rückwirkungsfreiheit aller nicht sicherheitsrelevanten Systemkomponenten bzgl. der Sicherheitsfunktion gewährleistet ist. Die Rückwirkungsfreiheit muss auch im Falle von Fehlern in Standardkomponenten gewährleistet sein. Wichtig (aber nicht unbedingt hinreichend) ist hierfür eine galvanische Trennung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Systemteilen.

Verfügbare Signale:

Safe ESD
Safe STOP
SIL-Fehler
SIL-Funktion aktiv

Belegung über das Menü im Display:

Erforderlicher Benutzerlevel: Spezialist (4) oder höher.

M ▷ Gerätekonfiguration M0053
I/O Interface M0139
Digitale Ausgänge M0110

Standardwerte:

Signal DOUT 5 = SIL-Funktion aktiv

Signal DOUT 6 = SIL-Fehler

7.4. Meldungen über Feldbus der Standard Stellantriebs-Steuerung

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

Information 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.

Im Prozessabbild verfügbare Signale:

Safe ESD
Bit: Safe STOP
Bit: SIL-Fehler
Bit: SIL-Funktion aktiv

Weitere Informationen zur Konfiguration der Parameter über die Feldbusschnittstelle siehe Handbuch (Geräteintegration Feldbus).

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.

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 sollte die Strategie zum Erreichen der Sicherheit und die verschiedenen Tätigkeiten während des Sicherheitslebenszykluses genannt sein.

8.2. Antriebsüberwachung für Sicherheitsfunktion ESD

Das Gerät, bestehend aus Stellantrieb mit Stellantriebs-Steuerung und integriertem SIL-Modul verfügt über eine interne Antriebsüberwachung. Durch das Ansteuern der Standard Stellantriebs-Steuerung/des Stellantriebs über die Standard-Fahrbefehle wird die interne Antriebsüberwachung automatisch ausgeführt. Die interne Antriebsüberwachung diagnostiziert einen Großteil der sicherheitsbezogenen Komponenten des Stellantriebs und würde in einem Fehlerfall einen Fehler über das Fehlerrelais des SIL-Moduls (`SIL Fehler`) signalisieren.

Um die Sicherheitskennzahlen der Sicherheitsfunktion Safe ESD zu gewährleisten, muss das Gerät mindestens einmal pro Monat über die Standard Stellantriebs-Steuerung angesteuert und zusätzlich das Fehlerrelais des SIL-Moduls (`SIL Fehler`) ausgewertet werden. Kennzahlen siehe Seite 43, Spezifische Kennzahlen für die Steuerung AC 01.2 in Version 22X oder 22Y mit Stellantrieben der Baureihe SA .1. Alternativ dazu kann statt dessen ein Partial Valve Stroke Test (PVST) durchgeführt werden. Siehe Seite 27, Partial Valve Stroke Test (PVST) durchführen.

Das Ansteuerungssignal und die damit verbundene Fahrt des Stellantriebs muss mindestens für einen Zeitdauer von 4 Sekunden anstehen. Steht das Ansteuerungssignal und die damit verbundene Fahrt des Antriebs für die Zeitdauer von mindestens 4 Sekunden an, ohne dass ein Fehler über das SIL Fehlerrelais (SIL-Modul: `SIL Fehler`) ausgegeben wird, so ist der Test erfolgreich. Sollte dies nicht der Fall sein, muss das Gerät mit einem Proof-Test überprüft werden. Proof-Test durchführen, siehe Seite 29, Proof-Test (Überprüfung auf sichere Funktion des Stellantriebs).

Andere Intervalle für die automatisierte Antriebsüberwachung können gewählt werden. In diesem Fall ist folgendes zu beachten:

- Die PFD-Werte und alle anderen Kennzahlen, in die das Diagnosetestintervall eingeht müssen neu berechnet werden. Die entsprechenden Werte (siehe Seite 43, Spezifische Kennzahlen für die Steuerung AC 01.2 in Version 22X oder 22Y mit Stellantrieben der Baureihe SA .1) haben keine Gültigkeit.
- Die automatisierte Diagnose soll mindestens 10 mal häufiger stattfinden, als der Proof-Test.
- Die automatisierte Diagnose soll mindestens 10 mal häufiger stattfinden, als die Anforderungsrate der Sicherheitsfunktion.

8.2.1. Partial Valve Stroke Test (PVST) durchführen

— Option —

Der PVST kann auf zwei verschiedene Arten durchgeführt werden.

1. Durchführung PVST unter Verwendung der sicheren Eingänge Safe ESDa und Safe ESDb:
   Der PVST muss von der externen Sicherheits-SPS gesteuert werden. Die Ansteuerung erfolgt von der Sicherheits-SPS über die sicheren Eingänge Safe ESDa und Safe ESDb. Durch die Auswertung des SIL-Fehlerrelais (SIL-Modul: SIL Fehler) findet die gewünschte Diagnose statt. Die Ansteuerungssignale und die damit verbundene Fahrt des Stellantriebs muss für ein Zeitdauer von mindestens 4 Sekunden anstehen.
   Stehen die Ansteuerungssignale und die damit verbundene Fahrt des Antriebs für mindestens 4 Sekunden an, ohne dass ein Fehler über das SIL-Fehlerrelais (SIL-Modul: SIL Fehler) ausgegeben wird, so ist der Test erfolgreich. Sollte dies nicht der Fall sein, muss das Gerät nach den in Kapitel <Proof-Test durchführen> genannten Schritten überprüft werden.
2. Durchführung des PVST unter Verwendung der PVST-Funktion der AC. 2:
   Ist die Standard Stellantriebs-Steuerung 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:
   - Zusätzliche rückwirkungsfreie Endlagenschalter für sichere Endlagenrückmeldung sind vorhanden und auf die Sicherheits-SPS verdrahtet.
   - Ein digitaler Eingang (von den anderen Eingängen galvanisch getrennt) der Standard Stellantriebs-Steuerung ist auf folgenden Wert konfiguriert: PVST ausführen (949), oder Ansteuerung des PVST über eine vorhandene Feldbusschnittstelle.
   - 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 > 4 Sekunden betragen.
   - Die Meldungen PVST Fehler (953) und PVST Abbruch (954) der Standard Stellantriebs-Steuerung werden über digitale Ausgänge der Standard Stellantriebs-Steuerung oder bei Verwendung einer Feldbusschnittstelle von der BPCS-SPS an die Sicherheits-SPS gemeldet. Hierbei ist unbedingt auf geeignete Maßnahmen zur Sicherstellung der Rückwirkungsfreiheit auf das sicherheitstechnische System (Sicherheits-SPS) zu achten.

   Der PVST wird entweder direkt von der Sicherheits-SPS am PVST-Eingang der Standard Stellantriebs-Steuerung angefordert oder das Signal zur Anforderung des PVST wird ebenfalls an die Sicherheits-SPS geleitet. Während die Standard Stellantriebs-Steuerung AC. 2 den PVST durchführt überwacht die Sicherheits-SPS ob
   - sich der Antrieb zu Beginn des PVST in einer der beiden Endlagen befunden hat (Kontrolle erfolgt über die sichere Endlagenrückmeldung).
   - sich der Antrieb innerhalb der eingestellten PVST Fahrzeit aus der Endlage heraus bewegt hat (Kontrolle erfolgt über die sichere Endlagenrückmeldung).
   - sich der Antrieb nach Abschluss des PVST wieder in der korrekten Endlage befindet (Kontrolle erfolgt über die sichere Endlagenrückmeldung).
   - Ob während der PVST Fahrzeit ein Fehler über das SIL-Fehlerrelais (SIL-Modul: SIL-Fehler) gemeldet wurde.

   Nur wenn sich der Antrieb zu Beginn des PVST in einer Endlage befunden hat, sich während des PVST aus dieser Endlage heraus bewegt hat, von der Standard Stellantriebs-Steuerung kein PVST Fehler (953) oder PVST Abbruch (954) sowie vom SIL-Modul kein SIL-Fehler gemeldet wurde, war der PVST erfolgreich. Sollte dies nicht der Fall sein, muss das Gerät nach den in Kapitel <Proof-Test> genannten Schritten überprüft werden.
   Hinweis: Mit „sichere Endlagenrückmeldung“ sind Endlagenschalter gemeint, die direkt auf den Kundenausgang verdrahtet und von AUMA im Rahmen einer Herstellererklärung für Funktionale Sicherheit bewertet sind (SFC).

Information Werden Digitale Eingänge oder Ausgänge der Standard Stellantriebs-Steuerung mit der Sicherheits-SPS verbunden, so ist unbedingt darauf zu achten, dass eine hinreichende Rückwirkungsfreiheit aller nicht sicherheitsrelevanten Systemkomponenten bzgl. der Sicherheitsfunktion gewährleistet ist. Die Rückwirkungsfreiheit muss auch im Falle von Fehlern in Standardkomponenten gewährleistet sein. Wichtig (aber nicht unbedingt hinreichend) ist hierfür eine galvanische Trennung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Systemteilen.

Durch die Durchführung eines PVST findet eine Diagnose vieler sicherheitsbezogener Komponenten statt. Daher können die Sicherheitskennzahlen gegenüber einer Anwendung ohne bzw. mit geringer Diagnose verbessert werden.

8.3. Antriebsüberwachung für Sicherheitsfunktion „Sichere Endlagenrückmeldung“

Um die korrekte Funktion der „Sicheren Endlagenrückmeldung“ zu gewährleisten, muss das Meldeverhalten des Stellantriebs regelmäßig geprüft werden. Dies kann entweder im Rahmen einer sowieso stattfindenden betrieblichen Bewegung des Stellantriebs erfolgen (Reaktionsüberwachung), oder im Rahmen eines gezielt durchgeführten PVST.

Der PVST dient der Funktionsüberprüfung von Stellantriebs-Steuerungen und Stellantrieben die nicht regelmäßig betrieben werden und somit die Reaktionsüberwachung nicht zur Diagnose nutzen können.

Die Diagnose durch den PVST bzw. die Reaktionsüberwachung soll mindestens 10-mal häufiger erfolgen als der Proof-Test und ebenfalls mindestens 10-mal häufiger, als die Anforderungsrate der Sicherheitsfunktion.

Die Überwachung und Auswertung des PVST bzw. der Reaktionsüberwachung muss durch die Logikeinheit des sicherheitstechnischen Systems erfolgen:

- Die Stellantriebsbewegung kann über einen beliebigen Eingang angefordert werden.
- Der SIL-Fehler des SIL-Moduls ist während der gesamten Testprozedur auszuwerten. Wird ein Fehler gemeldet, gilt der Test als nicht bestanden.
- Die Auswertung, ob die Sichere Endlagenmeldung wie gewünscht meldet, muss mittels der direkt auf den Kundenanschluss verdrahteten Endlagenschalter erfolgen.
- Der Stellantrieb muss sich in einer der folgenden Positionen befinden:
  - Vor Beginn der Testfahrt in einer der beiden Endlagen. Die Testfahrt führt dann aus der Endlage heraus und danach wieder in diese hinein.
  - Vor Beginn der Testfahrt hinreichend von beiden Endlagen entfernt. Die Testfahrt führt dann in eine Endlage hinein und aus dieser wieder hinaus.

  In beiden Fällen ist der Stellweg so zu bemessen, dass eine vollständige Betätigung des Endlagenschalters erwartet werden kann. Es ist zu prüfen, ob der Endlagenschalter sowohl vor Beginn, während des Tests, als auch nach Abschluss des Tests die jeweils zu erwartende Position meldet.
- Es muss eine dynamische Überwachung der Testfahrt erfolgen, d.h. dynamische Prüfung, ob die Änderung des Signals der Erwartungshaltung entspricht.

Information Wird der PVST nur aus bzw. in eine der beiden Endlagen ausgeführt, wird nur der Schalter dieser Endlage auf Funktionalität getestet. Sind beide Endlagenschalter (AUF/ZU) sicherheitsrelevant, kann z.B. ein Full Stroke Test durchgeführt 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.

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

1. Safe ESD Sicherheitsfahrt (sicheres ÖFFNEN/SCHLIESSEN) prüfen.
2. SIL-Fehlermeldung „Antriebsüberwachung“ prüfen.
3. Safe ESD Reaktion auf Meldungen „Motorschutz (Thermofehler)“ prüfen.
4. Safe ESD Reaktion auf „wegabhängige Abschaltung mit Überlastschutz“ prüfen (Auswertung Weg und/oder Drehmoment).
5. Safe ESD Reaktion auf „Abschaltung in der Weg-Endlage“ prüfen (Auswertung Weg) – für Stellantriebe mit elektromechanischer Steuereinheit.
6. Safe ESD Reaktion auf „Abschaltung in der Weg-Endlage“ prüfen (Auswertung Weg) – für Stellantriebe mit elektronischer Steuereinheit und Wegschaltern.
7. Safe ESD Reaktion auf „Abschaltung in der Drehmoment-Endlage“ prüfen (Auswertung Drehmoment nach Weg).
8. Safe ESD Reaktion auf „keine Abschaltung“ prüfen (keine Auswertung von Weg- und Drehmoment).
9. Safe STOP Funktion prüfen.
10. Kombination von Safe ESD und Safe STOP Funktion prüfen.
11. Sichere Endlagenrückmeldung prüfen.

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 Ausfallwahrscheinlichkeit der Sicherheitsfunktion bei Anforderung (PFD) ist abhängig von dem gewählten Proof-Test-Intervall und gilt in unserem angegebenen Beispiel für T_{proof} = 1 Jahr (siehe Kapitel <Sicherheitstechnische Kennzahlen>).

In jedem Fall müssen nach der Inbetriebnahme und nach jeder Wartung oder Reparatur, 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 **Ist die Sicherheitsfunktion als ESD ZU/ZU + Safe STOP AUF/ZU oder als ESD AUF/AUF + Safe STOP AUF/ZU konfiguriert, müssen alle zutreffenden Prüfungen für Safe ESD und für Safe STOP (sowie die Kombination von Safe ESD und Safe STOP) geprüft werden.**

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

8.4.1. Vorabprüfungen

Vorab muss das Antriebssystem folgenden Prüfungen unterzogen werden:

Prüfverfahren

- Optische Prüfung:
  - Sichtkontrolle auf äußere Schäden und Korrosion.
  - Elektrische und mechanische Anschlüsse überprüfen.
- Funktionskontrolle

- Stellantrieb mindestens einmal komplett von ZU nach AUF und wieder zurück (oder umgekehrt) fahren.
  - Während dieser Fahrt Stellantrieb bezüglich auffälliger Geräusche und Schwergängigkeit beobachten.
  - Prüfen, ob beide Endlagen wie erwartet erreicht und gemeldet werden.

8.4.2. Safe ESD Sicherheitsfahrt „sicheres ÖFFNEN/SCHLIESSEN“ prüfen

Konfiguration Diese Prüfung gilt für alle Ausführungen mit Safe ESD Funktion (unabhängig von der Konfiguration der „SIL-Abschaltart“). Die Safe ESD Reaktion auf die unterschiedlichen Abschaltarten wird in separaten Prüfungen getestet.

Prüfverfahren Bei entsprechender Beschaltung der Eingänge `Safe ESDa/Safe ESDb` muss eine Sicherheitsfahrt in die konfigurierte Richtung ausgelöst werden.

HINWEIS

Bei der Konfiguration „SIL-Abschaltart“ = „keine Abschaltung“ (ohne Endlagenschutz) können durch eine Fehlbedienung während der Prüfung Schäden an den Geräten im sicherheitsbezogenen System entstehen!

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

→ Vor dem Proof-Test Konfiguration der „SIL-Abschaltart“ prüfen. Die konfigurierte Abschaltart ist im Schaltplan (zweite Seite) angegeben.

→ Bei Stellantrieben mit „SIL-Abschaltart“ = „keine Abschaltung“: **Vor Erreichen der Endlage Sicherheitsfahrt unterbrechen** (Eingangssignale `Safe ESDa/Safe ESDb` auf +24 V DC setzen).

→ Zum Test sollte sich die Armatur in Mittelstellung bzw. in ausreichender Entfernung zu den Endlagen befinden.

→ Bei Schäden muss das Stellantriebssystem überprüft und ggf. repariert werden.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Fahrbefehl in entgegengesetzte Richtung der konfigurierten Safe ESD Sicherheitsfunktion ausführen:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Fahrbefehl in Richtung AUF starten.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Fahrbefehl in Richtung ZU starten.

   Information: Fahrbefehle (in Richtung AUF oder ZU) können für den Test sowohl von Fern (über die Leittechnik) als auch direkt vor Ort an der Steuerung (über die Drucktaster der Ortssteuerstelle) ausgeführt werden.
3. Während der Fahrt Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

➥ Die Sicherheitsfunktion ist korrekt, wenn der Stellantrieb stoppt und eine Sicherheitsfahrt in die konfigurierte Richtung bis in die sichere Endlage ausführt.

➥ Es darf **keine** SIL-Fehlermeldung erfolgen.

4. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.

8.4.3. SIL-Fehlermeldung „Antriebsüberwachung“ prüfen

Konfiguration Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

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

Prüfverfahren Zeigt die Antriebswelle nach dem Auslösen einer Sicherheitsfahrt innerhalb einer bestimmten Zeit keine Bewegung, muss eine SIL-Fehlermeldung erfolgen.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Motorbetrieb auskuppeln und so halten, dass der Handbetrieb eingekuppelt bleibt. Hebel dabei möglichst exakt parallel zur Antriebsachse halten.
3. Safe ESD Sicherheitsfahrt starten:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

➥ Die SIL-Fehlermeldung ist korrekt, wenn innerhalb 4 Sekunden über den Ausgang `SIL-Fehler` eine SIL-Fehlermeldung erfolgt.

4. Falls ein SIL-Fehler gemeldet wird: Motor sofort anhalten.

➥ Sollte nach maximal 10 Sekunden kein SIL-Fehler gemeldet werden, Motor ebenfalls anhalten. Falls nicht innerhalb von 4 Sekunden eine SIL-Fehlermeldung erfolgt ist der Test nicht bestanden, der Stellantrieb muss untersucht und instandgesetzt werden.

5. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen und Motorbetrieb wieder einkuppeln.

⚠ VORSICHT

Falls der Stellantrieb über einen längeren Zeitraum mit ausgekuppeltem Motor läuft, führt dies zu erheblichem Verschleiß des Stellantriebs und im schlimmsten Fall zu unbeabsichtigtem Losfahren, zu ungewolltem Mitlaufen des Handrads oder zu einer Zerstörung des Stellantriebs!

Personenschäden oder Schäden am Stellantrieb möglich.

→ Durch betriebliche Maßnahmen sicherstellen, dass der Motor (mit Ausnahme des Proof-Tests) nicht im ausgekuppelten Zustand betrieben wird.

→ Motor nur kurzfristig während des Proof-Tests im ausgekuppelten Zustand betreiben.

8.4.4. Safe ESD Reaktion auf Meldungen „Motorschutz (Thermofehler)“ prüfen

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

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

Prüfverfahren

Zum Schutz gegen Überhitzung und unzulässig hohe Oberflächentemperaturen am Stellantrieb sind in der Motorwicklung Kaltleiter oder Thermoschalter integriert. Der Motorschutz spricht an, sobald die maximal zulässige Wicklungstemperatur erreicht ist.

Bei einer Sicherheitsfahrt über die Safe ESD Funktion hängt die Reaktion des Stellantriebs beim Auslösen des Motorschutzes von der Konfiguration „SIL-Motorschutz“ ab:

- Bei Konfiguration „**SIL-Motorschutz**“ = **aktiv**
  = Sicherheitsfahrt wird gestoppt.
- Bei Konfiguration „**SIL-Motorschutz**“ = **inaktiv**
  = Sicherheitsfahrt wird nicht gestoppt.

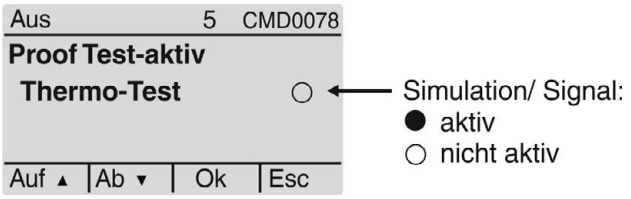
Die Prüfung erfolgt durch eine Simulation des Motorschutzsignals über die Ortssteuerstelle der AC 01.2:

Erforderlicher Zugriffslevel: Spezialist (4) oder höher.

M ▷ Diagnose M0022
Proof T. (Motorschutz) M1021

Simulationswert: Thermo Test

Bild 13: Displayanzeige an der Ortssteuerstelle



Die Simulation (aktiv/nicht aktiv) wird durch den Drucktaster Ok ein- und ausgeschaltet.

Ein Punkt im Display zeigt an, wenn die Simulation aktiv ist.

Punkt schwarz (●): Motorschutzsimulation aktiv (Thermofehler)

Punkt weiß (○): Signal nicht aktiv

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Wahlschalter in Stellung **0** (AUS) stellen.
3. Ins Hauptmenü wechseln und unter dem Parameter Proof T. (Motor-schutz)M1021 den Simulationswert: Thermo Test auswählen (Simulation noch nicht aktivieren: weißer Punkt).
4. Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

➥ Sicherheitsfahrt wird ausgelöst.

5. Motorschutzsimulation aktivieren: Drucktaster Ok drücken (schwarzer Punkt)

➥ Die Sicherheitsfunktion ist korrekt, wenn:

- Bei Konfiguration „**SIL-Motorschutz**“ = **aktiv**:
  - Die Sicherheitsfahrt gestoppt wird.
  - über den Ausgang `SIL-Fehler` eine SIL-Fehlermeldung erfolgt.
- Bei Konfiguration „**SIL-Motorschutz**“ = **inaktiv**:
  - Die Sicherheitsfahrt **nicht** gestoppt wird.
  - Trotzdem wird eine SIL-Fehlermeldung über den Ausgang `SIL-Fehler` signalisiert.

6. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.
7. Simulation zurücksetzen bzw. das Simulationsmenü verlassen und den Wahl-schalter in die ursprüngliche Stellung zurückstellen.

8.4.5. Safe ESD Reaktion auf „wegabhängige Abschaltung mit Überlastschutz“ prüfen (Auswertung Weg und/oder Drehmoment)

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Stellantrieb mit elektromechanischer Steuereinheit
- Eine der folgenden Sicherheitsfunktionen:
  - Safe ESD Funktion „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Konfiguration „SIL-Abschaltart“
  = **“wegabhängige Abschaltung mit Überlastschutz”**
  (Sicherheitsfahrt wird durch Auslösen der Wegschalter **und/oder** Auslösen der Drehmomentschalter (Überlastschutz) gestoppt).

Prüfverfahren

Bei dieser Prüfung wird die Reaktion der Safe ESD Funktion auf das Auslösen der Wegschalter und/oder Auslösen der Drehmomentschalter während einer Sicherheitsfahrt geprüft.

Bei einer Safe ESD Fahrt muss der Stellantrieb bei Erreichen der über die Wegschaltung eingestellten Position stoppen. Eine Safe ESD Fahrt muss auch

gestoppt werden, wenn das über die Drehmomentschaltung eingestellte Abschaltmoment überschritten wird.

Die Prüfung erfolgt über die roten Testknöpfe [1] und [2] der Steuereinheit. Über diese können die Schalter von Hand betätigt werden:

Bild 14: elektromechanische Steuereinheit

- Testknopf [1] in Pfeilrichtung WSR drehen: Wegschalter ZU löst aus.
- Testknopf [1] in Pfeilrichtung DSR drehen: Drehmomentschalter ZU löst aus.
- Testknopf [2] in Pfeilrichtung WÖL drehen: Wegschalter AUF löst aus.
- Testknopf [2] in Pfeilrichtung DÖL drehen: Drehmomentschalter AUF löst aus.

Information Wird einer der Testknöpfe (DSR/DÖL) gedreht ohne dass eine Sicherheitsfahrt ausgeführt wird erfolgt eine SIL-Fehlermeldung!

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Schaltwerkraum öffnen.
3. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

Abschaltung über Wegschalter prüfen:

4. Wegschalter betätigen und betätigt halten, bis die Prüfung beendet ist:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung WSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung WÖL drehen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Wegschalter korrekt, wenn die Sicherheitsfahrt gestoppt wird.

5. Nach der Auswertung der Wegschaltung:
   5.1 Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.
   5.2 Stellantrieb über die Ortssteuerstelle oder von FERN in die Endlage AUF und anschließend in die Endlage ZU fahren. (Dadurch wird die Positionierung neu erfasst).
   5.3 Stellantrieb wieder in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.

Abschaltung über Drehmomentschalter prüfen:

6. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

7. Drehmomentschalter betätigen und betätigt halten, bis die Prüfung beendet ist:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung DSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung DÖL drehen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Drehmomentschalter korrekt, wenn:

- die Sicherheitsfahrt gestoppt wird.
- über den Ausgang `SIL-Fehler` eine SIL-Fehlermeldung erfolgt.
- das Display rot leuchtet.

8. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.
9. Drehmomentfehler der Standard Stellantriebs-Steuerung quittieren.
10. Schaltwerkraum schließen.

8.4.6. Safe ESD Reaktion auf „Abschaltung in der Weg-Endlage“ prüfen (Auswertung Weg) – für Stellantriebe mit elektromechanischer Steuereinheit

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Stellantrieb mit elektromechanischer Steuereinheit
- Eine der folgenden Sicherheitsfunktionen:
  - Safe ESD Funktion „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Konfiguration „SIL-Abschaltart“
  = „**Abschaltung in der Weg-Endlage**“
  (Sicherheitsfahrt wird durch Auslösen der Wegschalter gestoppt)

Prüfverfahren

Bei dieser Prüfung wird die Reaktion der Safe ESD Funktion auf das Auslösen der Wegschalter während einer Sicherheitsfahrt geprüft.

Bei einer Safe ESD Fahrt muss der Stellantrieb bei Erreichen der über die Wegschaltung eingestellten Position stoppen.

Die Prüfung erfolgt über die roten Testknöpfe [1] und [2] der Steuereinheit. Über diese können die Schalter von Hand betätigt werden:

Bild 15: elektromechanische Steuereinheit

- Testknopf [1] in Pfeilrichtung WSR drehen: Wegschalter ZU löst aus.
- Testknopf [2] in Pfeilrichtung WÖL drehen: Wegschalter AUF löst aus.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Schaltwerkraum öffnen.
3. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

Abschaltung über Wegschalter prüfen:

4. Wegschalter betätigen und betätigt halten, bis die Prüfung beendet ist:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung WSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung WÖL drehen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Wegschalter korrekt, wenn die Sicherheitsfahrt gestoppt wird.

5. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.
6. Schaltwerkraum schließen.

8.4.7. Safe ESD Reaktion auf „Abschaltung in der Weg-Endlage“ prüfen (Auswertung Weg) – für Stellantriebe mit elektronischer Steuereinheit und Wegschaltern

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Stellantrieb mit elektronischer Steuereinheit und Wegschaltern
- Eine der folgenden Sicherheitsfunktionen:
  - Safe ESD Funktion „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Konfiguration „SIL-Abschaltart“
  = „**Abschaltung in der Weg-Endlage**“
  (Sicherheitsfahrt wird durch Auslösen der Wegschalter gestoppt)

Prüfverfahren

Bei dieser Prüfung wird die Reaktion der Safe ESD Funktion auf das Auslösen der Wegschalter während einer Sicherheitsfahrt geprüft.

Bei einer Safe ESD Fahrt muss der Stellantrieb bei Erreichen der über die Wegschaltung eingestellten Position stoppen.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

Abschaltung über Wegschalter prüfen:

3. Abwarten bis der Stellantrieb die Weg-Endlage erreicht und somit den entsprechenden Wegschalter aktiviert hat.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Wegschalter korrekt, wenn die Sicherheitsfahrt gestoppt wird.

4. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.

8.4.8. Safe ESD Reaktion auf „Abschaltung in der Drehmoment-Endlage“ prüfen (Auswertung Drehmoment nach Weg)

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Stellantrieb mit elektromechanischer Steuereinheit
- Eine der folgenden Sicherheitsfunktionen:
  - Safe ESD Funktion „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Konfiguration „SIL-Abschaltart“
  = „**Abschaltung in der Drehmoment-Endlage**“
  (Sicherheitsfahrt wird durch Auslösen der Drehmomentschalter (Überlastschutz) gestoppt. Voraussetzung hierfür ist, dass zuvor der entsprechende Wegschalter ausgelöst wurde).

Prüfverfahren

Bei dieser Prüfung wird die Reaktion der Safe ESD Funktion auf das Auslösen der Drehmomentschalter (nach Auslösen der Wegschalter) während einer Sicherheitsfahrt geprüft.

Die Prüfung erfolgt über die roten Testknöpfe [1] und [2] der Steuereinheit. Über diese können die Schalter von Hand betätigt werden:

Bild 16: elektromechanische Steuereinheit

- Testknopf [1] in Pfeilrichtung DSR drehen: Drehmomentschalter ZU löst aus.
- Testknopf [2] in Pfeilrichtung DÖL drehen: Drehmomentschalter AUF löst aus.

Prüfablauf

1. Stellantrieb über die **Standard Stellantriebs-Steuerung** in die Endlage der konfigurierten Safe ESD Funktion fahren (bis Weg-Endschalter anspricht).
2. Schaltwerkraum öffnen.

Abschaltung über Drehmoment- und Wegschalter prüfen:

3. Drehmomentschalter betätigen und betätigt halten.
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung DSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung DÖL drehen.
4. Während betätigtem Drehmomentschalter Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal für `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Drehmoment- und Wegschalter korrekt, wenn:

- die Sicherheitsfahrt nicht gestartet wird.
- über den Ausgang `SIL-Fehler` **keine** SIL-Fehlermeldung erfolgt.

5. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC (High) setzen.
6. Schaltwerkraum schließen.

8.4.9. Safe ESD Reaktion auf „keine Abschaltung“ prüfen (keine Auswertung von Weg- und Drehmoment)

Konfiguration

Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Stellantrieb mit elektromechanischer Steuereinheit, oder Stellantrieb mit elektronischer Steuereinheit und Wegschaltern.
- Eine der folgenden Sicherheitsfunktionen:
  - Safe ESD Funktion „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Konfiguration „SIL-Abschaltart“
  = „**keine Abschaltung**“
  (Sicheres Öffnen bzw. Schließen, ohne auf irgendeine Schutzeinrichtung zu regieren)

Prüfverfahren

Bei einer Safe ESD Fahrt muss der Stellantrieb in jedem Fall die Sicherheitsfahrt ohne Unterbrechung ausführen. Die Wegschaltung und/oder die Drehmomentschaltung dürfen die Sicherheitsfahrt nicht stoppen.

HINWEIS

Bei der Konfiguration “SIL-Abschaltart” = “keine Abschaltung” (ohne Endlagenschutz) können durch eine Fehlbedienung während der Prüfung Schäden an den Geräten im sicherheitsbezogenen System entstehen!

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

→ **Vor Erreichen der Endlage Sicherheitsfahrt unterbrechen** (Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC setzen).

→ Zum Test sollte sich die Armatur in Mittelstellung bzw. in ausreichender Entfernung zu den Endlagen befinden.

→ Bei Schäden muss das Stellantriebssystem überprüft und ggf. repariert werden.

Prüfablauf

Information: Bei der Ausführung elektronische Steuereinheit mit Wegschaltern entfallen die Schritte 6 – 9.

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Schaltwerkraum öffnen.
3. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

Auswertung Wegschaltung

4. Wegschalter betätigen:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung WSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung WÖL drehen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Wegschalter korrekt, wenn die Sicherheitsfahrt **nicht** gestoppt wird.

5. Nach der Auswertung Weg:
   5.1 Eingangssignale `Safe ESDa` und `Safe ESDb` **vor** Erreichen der Endlage auf +24 V DC (High) setzen.
   5.2 Stellantrieb über die Ortssteuerstelle oder von FERN in die Endlage AUF und anschließend in die Endlage ZU fahren. (Dadurch wird die Positionierung neu erfasst).
   5.3 Stellantrieb wieder in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.

Auswertung Drehmomentschaltung

6. Sicherheitsfahrt auslösen:
   → Dazu Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.
7. Drehmomentschalter betätigen:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Testknopf [1] in Pfeilrichtung DSR drehen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Testknopf [2] in Pfeilrichtung DÖL drehen.

➥ Die Sicherheitsfunktion reagiert auf die Signale der Drehmomentschalter korrekt, wenn:

- die Sicherheitsfahrt **nicht** gestoppt wird
- über den Ausgang `SIL-Fehler` eine SIL-Fehlermeldung erfolgt
- das Display rot leuchtet

8. Nach der Prüfung Eingangssignale `Safe ESDa` und `Safe ESDb` **vor** Erreichen der Endlage auf +24 V DC (High) setzen.

9. Drehmomentfehler der Standard Stellantriebs-Steuerung quittieren.
10. Schaltwerkraum schließen.

8.4.10. Safe STOP Funktion prüfen

Konfiguration Diese Prüfung gilt für die Konfigurationen „SIL-Funktion“ = „**Safe STOP ZU/AUF**“ (sicherer STOPP). Die Konfiguration der Abschaltart hat keine Bedeutung für die Prüfung, da diese auf die Safe STOP Funktion keinen Einfluss hat.

Prüfverfahren Bei entsprechender Beschaltung der Eingangssignale Safe STOP ZU bzw. Safe STOP AUF muss der Stellantrieb stoppen.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Fahrbefehl in Richtung AUF starten.

   Information: Fahrbefehle (in Richtung AUF oder ZU) können für den Test sowohl von Fern (über die Leittechnik) als auch direkt vor Ort an der Steuerung (über die Drucktaster der Ortssteuerstelle) ausgeführt werden.
3. Freigabesignale für die Fahrtrichtungen ZU und AUF nacheinander aufheben:

   3.1 Zuerst Eingangssignal Safe STOP ZU auf 0 V (Low) setzen.

   ➥ Stellantrieb muss weiterfahren.

   ➥ Es darf **keine** SIL-Fehlermeldung erfolgen.

   3.2 Dann Eingangssignal Safe STOP AUF auf 0 V (Low) setzen.

   ➥ Die Sicherheitsfunktion ist korrekt, wenn der Stellantrieb stoppt.

   ➥ Es darf **keine** SIL-Fehlermeldung erfolgen.
4. Eingangssignale Safe STOP ZU und Safe STOP AUF wieder auf +24 V DC (High) setzen.

   Information: Falls der Fahrbefehl AUF von FERN über die Leitwarte noch anliegt, kann der Stellantrieb losfahren!
5. Fahrbefehl in Richtung ZU starten.
6. Freigabesignale für die Fahrtrichtungen AUF und ZU nacheinander aufheben:

   6.1 Zuerst Eingangssignal Safe STOP AUF auf 0 V (Low) setzen.

   ➥ Stellantrieb muss weiterfahren.

   ➥ Es darf **keine** SIL-Fehlermeldung erfolgen.

   6.2 Dann Eingangssignal Safe STOP ZU auf 0 V (Low) setzen.

   ➥ Die Sicherheitsfunktion ist korrekt, wenn der Stellantrieb stoppt.

   ➥ Es darf **keine** SIL-Fehlermeldung erfolgen.
7. Eingangssignale Safe STOP ZU und Safe STOP AUF wieder auf +24 V DC (High) setzen.

   Information: Falls der Fahrbefehl AUF von FERN über die Leitwarte noch anliegt, kann der Stellantrieb losfahren!

8.4.11. Kombination von Safe ESD und Safe STOP Funktion prüfen

Konfiguration Diese Prüfung ist bei folgenden Ausführungen bzw. Konfigurationen erforderlich:

- Eine der folgenden Safe ESD Sicherheitsfunktionen mit beliebiger Konfiguration der Abschaltart:
  - Safe ESD Funktion: „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU)
  - Safe ESD Funktion: „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF)
- Safe STOP Funktion

HINWEIS

Bei der Konfiguration „SIL-Abschaltart“ = „keine Abschaltung“ (ohne Endlagenschutz) können durch eine Fehlbedienung während der Prüfung Schäden an den Geräten im sicherheitsbezogenen System entstehen!

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

→ Vor dem Proof-Test Konfiguration der „SIL-Abschaltart“ prüfen.

→ Bei Stellantrieben mit „SIL-Abschaltart“ = „keine Abschaltung“: **Vor Erreichen der Endlage Sicherheitsfahrt unterbrechen** (Eingangssignale `Safe ESDa` und `Safe ESDb` auf +24 V DC setzen).

→ Zum Test sollte sich die Armatur in Mittelstellung bzw. in ausreichender Entfernung zu den Endlagen befinden.

→ Bei Schäden muss das Stellantriebssystem überprüft und ggf. repariert werden.

Prüfverfahren

Diese Prüfung dient dazu, die korrekte Funktion der Kombination aus Safe ESD Sicherheitsfahrt und der Safe STOP Funktion zu bestätigen.

Prüfablauf

1. Stellantrieb in Mittelstellung bzw. in ausreichende Entfernung zu den Endlagen fahren.
2. Safe STOP Befehl in Richtung der konfigurierten Safe ESD Sicherheitsfunktion ausführen:
   → Bei Konfiguration „sicheres SCHLIESSEN“ (Safe ESD in Richtung ZU): Eingangssignal `Safe STOP ZU` auf 0 V (Low) setzen.
   → Bei Konfiguration „sicheres ÖFFNEN“ (Safe ESD in Richtung AUF): Eingangssignal `Safe STOP AUF` auf 0 V (Low) setzen.
3. Sicherheitsfahrt auslösen:
   Eingangssignal `Safe ESDa` und `Safe ESDb` auf 0 V (Low) setzen.

➥ Die Sicherheitsfunktion ist korrekt, wenn der Stellantrieb eine Sicherheitsfahrt in die konfigurierte Richtung ausführt.

➥ Es darf **keine** SIL-Fehlermeldung erfolgen.

4. Nach der Prüfung Eingangssignale `Safe ESDa`, `Safe ESDb`, `Safe STOP AUF` und `Safe STOP ZU` auf +24 V DC (High) setzen.

Information

Zusätzlich zu diesem Test müssen bei der Kombination von Safe ESD und Safe STOP Funktion auch alle anderen, auf die jeweils einzelnen Sicherheitsfunktionen (Safe STOP bzw. ESD) zutreffenden Proof-Tests in diesem Handbuch durchgeführt werden.

8.4.12. Sicherheitsfunktion „Sichere Endlagenmeldung“ prüfen

Konfiguration

Diese Prüfung ist bei Ausführungen mit sicherer Endlagenrückmeldung (Variante „22Y“) erforderlich.

Prüfverfahren

Bei Erreichen der Endlage müssen die Endlagenschalter die Endlage korrekt an der Kundenschnittstelle XK melden. Bei wieder Verlassen der Endlage muss das Signal entsprechend wieder zurückgenommen werden.

Prüfablauf

1. Stellantrieb in Endlage AUF fahren – wird Endlage AUF über die Sichere Endlagenmeldung signalisiert?
2. Stellantrieb aus Endlage AUF herausfahren – wird Sichere Endlagenmeldung AUF zurückgenommen?
3. Stellantrieb wieder in Endlage AUF fahren – wird Endlage AUF wieder über die Sichere Endlagenmeldung signalisiert?
4. Stellantrieb in Endlage ZU fahren – wird Endlage ZU über die Sichere Endlagenmeldung signalisiert?
5. Stellantrieb aus Endlage ZU herausfahren – wird Sichere Endlagenmeldung ZU zurückgenommen?

6. Stellantrieb wieder in Endlage ZU fahren – wird Endlage ZU wieder über die Sichere Endlagenmeldung signalisiert?
7. Während der gesamten Prozedur darf **keine** SIL-Fehlermeldung erfolgen.

Information Zusätzlich zu diesem Test müssen auch immer die jeweils zutreffenden Tests für die konfigurierte Safe ESD und / oder Safe STOP Funktion (und ggfs. deren Kombination) durchgeführt werden.

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 unbedingt erforderlich. Die Validierung muss mindestens alle unter den folgenden Kapiteln beschriebenen Prüfungen enthalten:

Seite 27, Sicherheitseinrichtung überprüfen

Seite 29, Proof-Test (Überprüfung auf sichere Funktion des Stellantriebs)

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

Information Bei AUMA Stellantrieben hat der Motorbetrieb Vorrang vor dem Handbetrieb. Das heißt, dass der Stellantrieb im Anforderungsfall selbstständig in den Motorbetrieb zurückschaltet. Dennoch empfehlen wir, nach Wartungs- oder Servicearbeiten den Motorbetrieb kurzzeitig zu aktivieren, um ein sicheres Einrasten der Motorkupplung zu prüfen.

9. Sicherheitstechnische Kennzahlen

9.1. Bestimmung der Kennzahlen

Bei der Berechnung der sicherheitstechnischen Kennzahlen wurden die genannten Sicherheitsfunktionen zu Grunde gelegt. Die Bewertung der mechanischen, elektrischen und elektronischen Komponenten 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 gefährlicher Ausfälle des Gerätes bestimmt.

Die Ausfallquoten für mechanische Teile wurden aus Feldrücklaufdaten und 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:

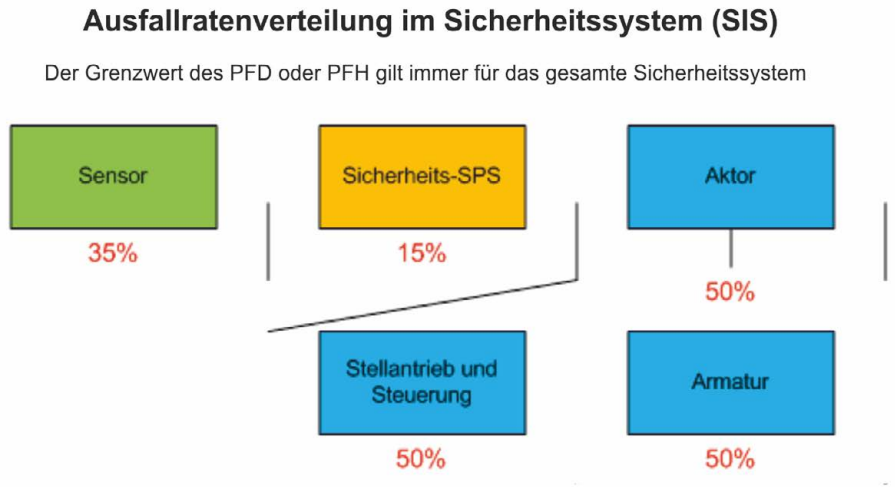
- SIL 2 Sicherheitsfunktionen: ≥ 10^{-3} bis < 10^{-2}
- SIL 3 Sicherheitsfunktionen: ≥ 10^{-4} bis < 10^{-3}

Da Stellantriebe aber nur einen Teil der gesamten Sicherheitsfunktion darstellen, sollte der PFD des Stellantriebes nicht mehr als ca. 25 % des zulässigen Gesamtwertes (PFD_{avg}) einer Sicherheitsfunktion betragen. Dies ergibt folgende Werte:

- PFD Stellantrieb für SIL 2 Anwendungen: ≤ 2,5E-03

Die elektrischen Stellantriebe mit Stellantriebs-Steuerung sind als Typ A Komponenten mit einer Hardwarefehlertoleranz 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 Hardwarefehlertoleranz von 0) sein.

Bild 17: Von AUMA angenommene, nicht-normative Fehlerverteilung



Information Die Energieversorgung des Systems ist in der Berechnung des Antriebs und der Stellantriebs-Steuerung nicht berücksichtigt.

Wie bereits bei der Projektierung erwähnt, ist für die Sicherstellung der Energieversorgung und die daraus resultierenden Berechnungen der Anlagenbetreiber zuständig.

Der Anlagenbetreiber ist dafür verantwortlich, die angenommene MTTR einzuhalten, da ansonsten die Angaben der quantitativen Ergebnisse nicht mehr gültig sind.

Information

Die in diesem Sicherheitshandbuch angegebenen sicherheitstechnischen Kennzahlen sind nur gültig, wenn **alle** in diesem Sicherheitshandbuch genannten Bedingungen eingehalten und die genannten Tätigkeiten durchgeführt werden.
Die in diesem Sicherheitshandbuch angegebenen PFD-Werte sind nur beispielhaft und unterliegen gewissen Annahmen z.B. über T_{proof}, MTTR, …
Die PFD-Berechnung sollte immer anlagenspezifisch mit den für die entsprechende Anlage gültigen Parametern und Rahmenbedingungen erfolgen. Als Input sollten die λ_{DU} und λ_{DD} Werte verwendet werden. Bei Einhaltung der in diesem Sicherheitshandbuch genannten Proof-Test Prozeduren empfehlen wir mit einer Proof-Test-Coverage (PTC) von 90 % zu rechnen.

9.2. Spezifische Kennzahlen für die Steuerung AC 01.2 in Version 22X oder 22Y mit Stellantrieben der Baureihe SA .1

Die nachfolgenden Kennzahlentabellen zeigen beispielhaft die sicherheitstechnischen Kennzahlen für die verschiedenen Versionen. Werden eine oder mehrere der im folgenden genannten Annahmen geändert, so muss insbesondere die Ausfallwahrscheinlichkeit im Anforderungsfall PFD, möglicherweise aber auch andere Kenngrößen neu berechnet werden.

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 = 90 % (Proof-Test Aufdeckungsgrad [%])
- T_1 = 1 Jahr (Proof-Test Intervall [h])
- T_2 = 10 Jahre (Anforderungsintervall = Lebensdauer [h])
- MRT = 72 Stunden (Mittlere Reparaturdauer [h])
- Td_ESD = 730 Stunden
  (Diagnosetestintervall der Antriebsüberwachung (für die Sicherheitsfunktion Safe ESD [h])
- Td_ESD_AVG = 365 Stunden (Mittlere Dauer zum Erkennen eines Ausfalls)
- Td_STOP = 0 Stunden (Diagnose Testintervall [h])
- Td_Endlage = 730 Stunden
- MTTR_ESD = 437 Stunden
- MTTR_STOP = 72 Stunden
- MTTR_Endlage = 802 Stunden

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

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

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DU}(1 - PTC)}{\lambda_D}\left(\frac{T_2}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTR = Td_{avg} + MRT$$

Information

Die in den nachfolgenden Tabellen angegebenen Kennzahlen für Safe STOP AUF bzw. Safe STOP ZU beziehen sich auf eine der beiden Funktionen. Soll ein genereller Safe STOP (Fahrt in beide Richtungen verhindert) durch gleichzeitige Aktivierung der Funktionen Safe STOP AUF und Safe STOP ZU realisiert werden, so muss die doppelte Ausfallrate der jeweiligen Einzelfunktionen (Safe STOP AUF/ZU) für die Bewertung verwendet werden.

Tabelle 11: Baureihe SA .1/SAEx .1 mit Steuerung AC/ACExC 01.2 in Version 22X/22Y

SA 25.1 – SA 40.1 / SAEx 25.1 – SAEx 40.1 Ausführung Leistungsteil: Schütze		
Sicherheitsfunktion	**Safe ESD mit PVST oder RM**	**Safe STOP AUF oder Safe STOP ZU**
λ_S	217 FIT	1 106 FIT
λ_{DD} [1)]	1 302 FIT	176 FIT
λ_{DU}	383 FIT	392 FIT
SFF	79,8 %	76,5 %
DC	77,2 %	30,9 %
PFD_{avg} T_{Proof} = 1 Jahr (1001)	$3{,}79 \times 10^{-3}$	$3{,}3 \times 10^{-3}$
PFD_{avg} T_{Proof} = 1 Jahr (1002)	$3{,}68 \times 10^{-4}$	$3{,}43 \times 10^{-4}$
SIL-Fähigkeit	SIL 2	SIL 2

1) Inklusive erkannter „Annunciation“- Ausfälle (λ_{AD}) (Ausfälle in der Diagnosefunktion)

Tabelle 12: Baureihe SA .1/SAEx .1 mit Steuerung AC/ACExC 01.2 in Version 22X/22Y, mit Sicherer Endlage

SA 25.1 – SA 40.1 / SAEx 25.1 – SAEx 40.1 Ausführung Leistungsteil: Schütze		
Sicherheitsfunktion	**Sichere Endlage**	**Sichere Endlage mit PVST oder RM**
λ_S	0 FIT	0 FIT
λ_{DD} [1)]	0 FIT	240 FIT
λ_{DU}	426 FIT	186 FIT
SFF	0 %	56,3 %
DC	0 %	56,3 %
PFD_{avg} T_{Proof} = 1 Jahr (1001)	$3{,}58 \times 10^{-3}$	$1{,}75 \times 10^{-3}$
SIL-Fähigkeit	SIL 1	SIL 1
Sicherheitstechnische Kennzahlen nach ISO 13849		
$MTTF_D$ [Jahre]	268 (hoch)	268 (hoch)
DC	0 % (kein)	56,3 % (kein)
berechneter Performance Level	$4{,}26 \times 10^{-7}$ 1/h	$1{,}86 \times 10^{-7}$ 1/h
erreichter Performance Level	CAT1: PL „c“ fähig	CAT1: PL „c“ fähig

1) Inklusive erkannter „Annunciation“- Ausfälle (λ_{AD}) (Ausfälle in der Diagnosefunktion)

10. SIL Herstellererklärung

AUMA Riester GmbH & Co. KG
Aumastr. 1
79379 Müllheim, Germany
www.auma.com

Tel +49 7631 809-0
Fax +49 7631 809-1250
Riester@auma.com

auma®
Solutions for a world in motion

Declaration of incorporation

Functional Safety according to IEC 61508

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

Actuator type	Controls type
SA 25.1 – 40.1 SAEx 25.1 – 40.1 SAR 25.1 – 30.1 SAREX 25.1 – 30.1 all in version 22X or 22Y only	AC 01.2 / ACExC 01.2 in version 22X or 22Y

The above-mentioned versions achieve the following Hardware Safety Integrity Level:

Hardware Safety Integrity		
Single channel use: ESD with PVST or RM	(HFT = 0)	SIL 2 capable
Single channel use: Safe Stop	(HFT = 0)	SIL 2 capable
Single channel use: Safe End Position Feedback with PVST or RM	(HFT = 0)	SIL 1 capable

For further details, please refer to enclosed supplement.

i.V. Michael Noll
Functional Safety Management Representative

2023-04-13
Date

i.A. Jörg Isenberg
Product management

2023-04-13
Date

Devices with failure rates calculated from field data

auma® Solutions for a world in motion	**Supplement** **Declaration of incorporation** Functional Safety according to IEC 61508	2023-04-13 V2R0

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

General		
Device designation and permissible types	SA 25.1 – 40.1 / SAEx 25.1 – 40.1 / SAR 25.1 – 30.1 / SAREX 25.1 – 30.1 all in version 22X or 22Y only With controls AC 01.2 / ACExC 01.2 in version 22X or 22Y	
Safety function(s)	Depending on configuration: ESD OPEN/CLOSE with PVST/RM and/or Safe STOP Only version 22Y: Safe End Position Feedback	
Device type according to IEC 61508	☒ Type A	☐ Type B
Operating mode	☒ Low Demand Mode	☐ High Demand or Continuous Mode
Safety manual	Y009.057	
Type of evaluation	☒	Hardware evaluation by FMEDA according to IEC 61508
Evaluation by	AUMA Riester GmbH & Co. KG	
Test report	-	

FMEDA	
Safety function	all
λ_{SAFE} *1)	See tables in safety manual
λ_{DD} *1)	See tables in safety manual
λ_{DU} *1)	See tables in safety manual
DC_D *2)	See tables in safety manual
MTBF - Mean Time Between Failures	See tables in safety manual
SFF - Safe Failure Fraction	See tables in safety manual
PFD_{avg} *3) with T[Proof] = 1 year	See tables in safety manual

Restrictions
All requirements and regulations of the safety manual shall imperatively be observed.

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

Stichwortverzeichnis

Solutions for a world in motion

AUMA Riester GmbH & Co. KG

Location Müllheim
Postfach 1362
DE 79373 Muellheim
Tel +49 7631 809 - 0
Fax +49 7631 809 - 1250
info@auma.com
www.auma.com

Location 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

Y009.057/001/de/1.23