

Zwenkaandrijvingen

SQ 05.2 – SQ 14.2/SQR 05.2 – SQR 14.2

SQEx 05.2 – SQEx 14.2/SQREx 05.2 – SQREx 14.2

met besturingseenheid voor de aandrijving

AC 01.2/ACExC 01.2

uitvoering SFC



AANWIJZING met betrekking tot het gebruik!

Dit document is alleen geldig in combinatie met de actuele, met het toestel meegeleverde bedieningsinstructies, het meegeleverde handboek, de meegeleverde orderspecifieke verklaring van de fabrikant, evenals de respectievelijke technische en elektrische gegevens. Deze dienen tevens als geldende documenten te worden opgevat.

Doel van dit document:

In dit document staat informatie over de noodzakelijke maatregelen die voor het gebruik van het toestel in veiligheidsrelevante systemen in overeenstemming met IEC 61508 c.q. IEC 61511 nodig zijn.

Referentiedocumentatie:

- exida report no. AUMA 15/07-029 R012
- Bedieningsinstructies (montage, bediening, inbedrijfstelling) bij de aandrijving
- Handboek (gebruik en instelling) besturingseenheid voor de aandrijving AC 01.2/ACExC 01.2
- Handboek (apparatuurintegratie veldbus) AC 01.2/ACExC 01.2 / ACV 01.2/ACVExC 01.2

Referentiedocumentatie is verkrijgbaar op het internet op <http://www.auma.com>.

Inhoudsopgave	Pagina
1. Terminologie.....	4
1.1. Afkortingen en begrippen	4
2. Toepassing en geldigheid.....	6
2.1. Toepassingsgebied	6
2.2. Normen	6
2.3. Geldige toesteltypen	6
3. Ontwerp, configuratie en gebruiksvoorwaarden.....	7
3.1. Ontwerp (berekening resp. bepaling van de aandrijving)	7
3.2. Configuratie (instelling)	7
3.3. Beveiliging tegen ongecontroleerde beweging (zelfremmendheid/rem)	8
3.4. Bedrijfsmodus (low/high demand mode)	8
3.5. Overige informatie en gegevens voor het ontwerp en de berekening	9
3.6. Gebruiksvoorwaarden (omgevingscondities)	9
4. Veiligheidstechnische systemen en veiligheidsfuncties.....	10
5. Installeren, inbedrijfstelling en gebruik.....	11
5.1. Installeren	11
5.2. Inbedrijfstelling	11
5.3. Gebruik en werking	11
5.4. Technische levensduur	12
5.5. Buitenbedrijfstelling	12
6. Controles en onderhoud.....	13
6.1. Veiligheidsvoorziening controleren	13
6.2. Proof-test (controle van de veilige werking van de aandrijving)	13
6.2.1. Controles vooraf	13
6.2.2. Controle en validatie van de veiligheidsfunctie "veilige terugmelding van de eindstanden"	13
6.2.3. Controle van de verzamelstoringsmelding	14
6.3. Partial Valve Stroke Test (PVST).	14
6.4. Onderhoud	15

7.	Veiligheidstechnische karakteristieke waarden.....	16
7.1.	Bepaling van de karakteristieke waarden	16
8.	SIL-conformiteitsverklaring (voorbeeld).....	18
	Trefwoordenregister.....	23

1. Terminologie

- Informatiebronnen**
- IEC 61508-4, Functionele veiligheid van veiligheidsrelevante elektrische/elektronische/programmeerbare elektronische systemen – deel 4: Begrippen en afkortingen
 - IEC 61511-1, Functionele veiligheid – Veiligheidstechnische systemen voor de procesindustrie – deel 1: Algemeen, begrippen, eisen aan systemen, soft- en hardware

1.1. Afkortingen en begrippen

Voor de beoordeling van de veiligheidsfuncties zijn in eerste instantie de lambdawaarden c.q. PFD-waarde (Probability of Dangerous Failure on Demand) en SFF-waarde (Safe Failure Fraction) nodig. Voor de beoordeling van de afzonderlijke componenten zijn meer karakteristieke waarden nodig. In de onderstaande tabel worden deze kort belicht.

Tabel 1: Afkortingen veiligheidstechnische karakteristieke waarden

Karakteristieke waarde	Engels	Beschrijving
λ_S	Lambda Safe	Aantal keren van veilige uitval
λ_D	Lambda Dangerous	Aantal keren van gevaarlijke uitval
λ_{DU}	Lambda Dangerous Undetected	Aantal keren van niet ontdekte gevaarlijke uitval
λ_{DD}	Lambda Dangerous Detected	Aantal keren van ontdekte gevaarlijke uitval
DC	Diagnostic Coverage	Diagnosedekkingsgraad - verhouding van het uitvalpercentage van de door middel van diagnosetesten herkende gevaarlijke fouten ten opzichte van het totale percentage gevaarlijke fouten van de componenten of het deelsysteem. De diagnosedekkingsgraad omvat geen bij herhalingstesten (proof-testen) vastgestelde fouten
MTBF	Mean Time Between Failures	Gemiddelde tijd tussen het ontstaan van twee opeenvolgende fouten
SFF	Safe Failure Fraction	Aandeel veilige, evenals detecteerbare gevaarlijke uitval
PFD_{avg}	Average Probability of dangerous Failure on Demand	Gemiddelde waarschijnlijkheid van gevaarlijke uitvalgebeurtenissen van een veiligheidsfunctie in geval van inschakeling
HFT	Hardware Fault Tolerance	Mogelijkheid van een functionele eenheid om een gevraagde functie tijdens fouten of afwijkingen te blijven uitvoeren. Een HFT = n betekent dat de functie tot aan n gelijktijdig optredende fouten nog veilig kan worden uitgevoerd.
T_{proof}	Proof-testinterval	Interval voor de herhalingstest

SIL Veiligheidsintegriteitsniveau (**Safety Integrity Level**).

In de norm IEC 61508 wordt 4 Level gedefinieerd (SIL 1 tot SIL 4).

Veiligheidsfunctie Functie die door een SIS of een veiligheidsrelevant systeem wordt uitgevoerd om risico's te reduceren, met als doel om in geval van een vastgelegd, gevaarlijk voorval een veilige toestand voor de installatie/voorziening te kunnen realiseren of in stand te houden.

Veiligheidstechnische functie (SIF) Functie met het vooraf vastgestelde veiligheidsintegriteitsniveau (SIL), dat voor het realiseren van de functionele veiligheid noodzakelijk is.

Veiligheidstechnisch systeem (SIS)	Veiligheidstechnisch systeem voor het uitvoeren van een of meerdere veiligheidstechnische functies. Een SIS is opgebouwd uit sensor(en), logisch systeem en actor(en).
Veiligheidsrelevant systeem	Een veiligheidsrelevant systeem omsluit alles (hardware, software, menselijke factoren) dat voor het uitvoeren van een of meerdere veiligheidsfuncties noodzakelijk is. Daarbij zouden uitvalgebeurtenissen van de veiligheidsfuncties een belangrijke toename van het veiligheidsrisico voor mensen en/of milieu betekenen. Een veiligheidsrelevant systeem kan een automatisch werkende installatie voor het uitvoeren van een bepaalde veiligheidsfunctie zijn of in een installatie zijn geïntegreerd.
Herhalingstest	Een voortdurend terugkerende test voor het ontdekken van uitvalgebeurtenissen in een veiligheidsrelevant systeem, zodat waar nodig het systeem in een “als nieuw” toestand wordt gebracht, of zo dicht als uit praktisch oogpunt mogelijk is in deze toestand wordt gebracht.
MTTR (Mean Time To Restoration)	Gemiddelde tijd totdat de fout is verholpen nadat deze is ontstaan. Deze tijd geeft aan hoe lang het herstellen van het systeem gemiddeld duurt. Deze waarde is daarom een belangrijke parameter voor de beschikbaarheid van het systeem. Deze tijd omvat ook de tijd tot het ontdekken van de fout, het plannen van de taken alsmede van de bedrijfsmiddelen. Deze moet zo kort mogelijk worden gehouden.
MRT (Mean Repair Time)	De gemiddelde reparatieduur geeft de gemiddelde duur aan die nodig is om een systeem te repareren. De MRT is belangrijk om de betrouwbaarheid en beschikbaarheid van het systeem te kunnen bepalen. De MRT moet zo kort mogelijk zijn.
Type toestel (type A en type B)	De besturingseenheid voor de aandrijving kan als toestel van het type A worden gezien, indien voor alle componenten, die voor het realiseren van de veiligheidstechnische functie noodzakelijk zijn, aan alle onderstaande voorwaarden is voldaan: • de soorten uitvalgebeurtenissen voor alle componenten zijn correct gedefinieerd. • het gedrag in geval van een fout kan helemaal worden voorspeld. • er zijn voldoende afhankelijke uitvalgegevens uit de praktijk beschikbaar, om te bewijzen dat aan de aangegeven uitvalcijfers is voldaan (Confidence Level min. 70%). De besturingseenheid voor de aandrijving moet als toestel van het type B worden gezien indien sprake is van een of meerdere van onderstaande voorwaarden: • de uitvalgebeurtenis van minimaal één element is niet goed gedefinieerd. • het gedrag in geval van een fout is niet volledig bekend. • er zijn geen betrouwbare foutgegevens van de veldapparatuur bekend om het uitvalcijfer voor de geregistreerde en niet ontdekte gevaarlijke uitvalgebeurtenissen te ondersteunen.
PTC (Proof Test Coverage)	De Proof Test Coverage beschrijft het aandeel van uitvalgebeurtenissen die door middel van een proof-test ontdekt worden.

2. Toepassing en geldigheid

2.1. Toepassingsgebied

AUMA aandrijvingen en besturingseenheden voor de aandrijving met de in dit handboek vermelde veiligheidsfuncties zijn bestemd voor de bediening van industriële afsluiters en zijn geschikt voor gebruik in veiligheidstechnische systemen in overeenstemming met IEC 61508 resp. IEC 61511.

2.2. Normen

De aandrijvingen en besturingseenheden voor de aandrijving voldoen aan de hieronder vermelde eisen:

Voor de veiligheidsfuncties "Veilige eindstandterugmelding": IEC 61508-2:2010

De veiligheidstechnische karakteristieke waarden van de beschreven apparaten voldoen aan de eisen van de IEC 61508 in de desbetreffende SIL-gerelateerde uitvalpercentages en eisen inzake de architectuur. Dit betekent echter niet dat aan alle overige eisen van de IEC 61508 wordt voldaan.

2.3. Geldige toesteltypen

De in dit handboek opgenomen informatie over de functionele veiligheid geldt voor de hier vermelde toesteltypen.

Tabel 2: Overzicht van de geschikte toesteltypen

Type aandrijving	Type besturingseenheid voor de aandrijving	Motor spanningsvoorziening	Bedrijfsmodus	Aansturing
SQ 05.2 – SQ 14.2 SQR 05.2 – SQR 14.2 in uitvoering SFC	AC 01.2 in uitvoering SFC	willekeurig	S2-15 min S2-30 min S4-25 % S4-50 %	Veilige eindstandterugmelding
SQEx 05.2 – SQEx 14.2 SQREx 05.2 – SQREx 14.2 in uitvoering SFC	ACExC 01.2 in uitvoering SFC	willekeurig	S2-15 min S2-30 min S4-25 % S4-50 %	Veilige eindstandterugmelding

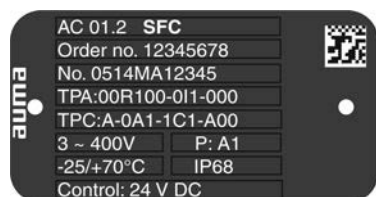
De hardware, software en de configuratie van de aandrijving en/of de besturingseenheid voor de aandrijving mogen zonder de schriftelijke toestemming van AUMA niet worden gewijzigd. Ongeautoriseerde wijzigingen kunnen de veiligheidsgerelateerde karakteristieke waarden en de SIL-eigenschappen van de producten negatief beïnvloeden.

Informatie

In toepassingen met vereisten inzake de functionele veiligheid mogen uitsluitend AUMA besturingseenheden voor de aandrijving en aandrijvingen in de uitvoering SFC of SIL worden gebruikt. Daarbij betekent SFC "Safety Figure Calculated" (veiligheidswaarden berekend). Deze benaming duidt op AUMA-producten waarbij de veiligheidstechnische karakteristieke waarden met behulp van een FMEDA uit veldgegevens en generieke gegevens zijn bepaald (voor details zie hoofdstuk <Bepaling van de karakteristieke waarden>).

AUMA besturingseenheden voor de aandrijving en aandrijvingen in de uitvoering SFC kan men o.a. daaraan herkennen dat er op het typeplaatje achter de typebenaming de letters "SFC" zijn te vinden.

Afbeelding 1: Voorbeeld typeplaatje met de aanduiding "SFC"



3. Ontwerp, configuratie en gebruiksvoorwaarden

3.1. Ontwerp (berekening resp. bepaling van de aandrijving)

Voor het ontwerp (berekening resp. bepaling van de aandrijving) van de aandrijvingen wordt in eerste instantie rekening gehouden met de vereiste maximale draaimomenten, werk- resp. regelmomenten en de insteltijden.

LET OP

Een verkeerd ontwerp van de aandrijving kan schade aan de apparatuur in het veiligheidsrelevante systeem veroorzaken!

Mogelijke gevolgen zijn bijv.: schade aan de afsluiter, oververhitting van de motor, vast blijven plakken van de schakelrelaiscontacten, schade aan de elektronica, warm worden resp. beschadiging van kabels.

- Bij het ontwerp moet zonder meer rekening worden gehouden met de technische specificaties van de aandrijvingen.
- Er moet voldoende reserve worden ingepland om te kunnen waarborgen dat de aandrijvingen in staat zijn om de afsluiters, ook in het geval van een fout en bij omstandigheden waarbij sprake is van te lage spanningen, op betrouwbare wijze te sluiten en te openen.

Informatie

Let er bij de veiligheidsfunctie “veilige terugmelding van de eindstanden” op dat de signalering via mechanische schakelaars wordt uitgevoerd. Aangezien deze elementen een onvermijdbare hysteresis hebben, verlaat de aandrijving de eindstand minimaal voordat de eindstandmelding wordt gewist. Bijgevolg bestaat er een aan de veiligheidsstand grenzend bereik van de aandrijvingsstanden waarin bij een beweging vanuit de veiligheidsstand de eindstand nog steeds wordt gemeld, de aandrijving deze echter reeds heeft verlaten. Indien het bereik in kwestie vanuit de tegengestelde richting wordt bereikt, bestaat de beschreven beperking niet. Normaliter is het bereik klein, het kan echter in ongunstige configuraties (gering aantal omwentelingen per slag) tot meer dan 10 % van de instelhoek bedragen. Indien het bovenstaande effect als gevolg van de ongunstige randvoorwaarden een onaanvaardbare beperking voor de veiligheidsfunctie oplevert, adviseren wij om voor de eindstandmelding zowel van de weg- alsook draaimomentschakelaars gebruik te maken.

Energievoorziening

Informatie

De eigenaar/gebruiker van de installatie is verantwoordelijk voor het waarborgen van de energievoorziening.

3.2. Configuratie (instelling)

De configuratie (instelling) van de veiligheidsrelevante functies wordt uitgevoerd zoals in de bedieningsinstructies resp. zoals hier in het handboek (Functionele veiligheid) is beschreven.

Informatie

Een exacte instelling van de weg- en draaimomentschakelaars voor de eindstanden is absoluut noodzakelijk teneinde een correcte werking van de “veilige terugmelding van de eindstanden” te waarborgen. Details over het instellen van de respectievelijke schakelaars zijn in de bedieningsinstructies beschreven.

Configuratie van de diagnose reactiebewaking en Partial Valve Stroke Test (PVST)

Al naar gelang van de verlangde diagnose moeten de configuraties voor de reactiebewaking resp. de Partial Valve Stroke Test worden gecontroleerd en eventueel worden aangepast.

De gedetailleerde configuratiemogelijkheden voor de reactiebewaking en informatie over de Partial Valve Stroke Test (PVST) vindt u in het handboek (gebruik en instelling) AUMATIC AC 01.2.

3.3. Beveiliging tegen ongecontroleerde beweging (zelfremmendheid/rem)

Bij zelfremmende AUMA'-aandrijvingen kan ervan worden uitgegaan dat bij een belasting tot aan het maximale draaimoment, er geen ongecontroleerde beweging van de afsluiter vanuit stilstand op grond van de draaimomentbelasting van de afsluiter plaatsvindt. In zoverre is in deze gevallen een verdere beveiliging tegen ongecontroleerde bewegingen niet absoluut noodzakelijk. Dit kan nodig worden, als bijvoorbeeld door vibraties de zelfremmendheid eventueel niet gewaarborgd of onvoldoende is. Bepaalde toepassingen kunnen bovendien desondanks een actieve beveiliging van de positie, bijv. door een rem, vereisen. Daarnaast zijn er toepassingsspecifieke normen die dit vereisen. Om deze reden moet er projectspecifiek worden gecontroleerd of een verdere beveiliging noodzakelijk is. In ieder geval is dit bij aandrijvingen zonder zelfremmendheid noodzakelijk.

Alle ten tijde van het ter perse gaan beschikbare aandrijvingen uit de series SQ 05.2 – SQ 14.2, SQR 05.2 – SQR 14.2, SQEx 05.2 – SQEx 14.2 en SQREx 05.2 – SQREx 14.2 zijn zelfremmend.

3.4. Bedrijfsmodus (low/high demand mode)

De veiligheidsfuncties van de door AUMA geleverde aandrijvingen zijn voor de bedrijfsmodus met een laag vraagpercentage (low demand mode) ontworpen en mogen uitsluitend in deze bedrijfsmodus worden gebruikt. In het geval dat er, afgezien van de veiligheidsfunctie, via dezelfde aandrijving tevens een niet-veiligheidstechnische functie van het PCS wordt uitgevoerd, dient erop te worden gelet dat tevens bij inachtneming van het totaal van niet-veiligheidstechnische functies, noodzakelijke tests en veiligheidsfuncties het voor de betreffende aandrijving gedefinieerde maximaal toelaatbare aantal schakelingen¹⁾, evenals het maximaal toelaatbare aantal starts²⁾ tijdens het gebruik van de aandrijving in een veiligheidstechnisch systeem niet mag worden overschreden.

Uitsluitend de veiligheidsfunctie “veilige terugmelding van de eindstanden” kan ongeacht de hierboven genoemde beperkingen onder bepaalde omstandigheden tevens in de bedrijfsmodus met een hoog vraagpercentage worden gebruikt indien de hieronder vermelde beperkingen in acht worden genomen:

- Bij inachtneming van het totaal van niet-veiligheidstechnische functies noodzakelijke tests en veiligheidsfuncties worden het voor de betreffende aandrijving gedefinieerde maximaal toelaatbare aantal schakelingen van de eindstandschakelaars, evenals het maximaal toelaatbare aantal starts tijdens het gebruik van de aandrijving, in een veiligheidstechnisch systeem niet overschreden.
- Bij inachtneming van het totaal van niet-veiligheidstechnische functies noodzakelijke tests en veiligheidsfuncties worden het voor de betreffende aandrijving met inachtneming van schaalregels vastgestelde toelaatbare maximale aantallen schakelingen¹⁾ resp. starts²⁾ niet overschreden.
- De smering wordt regelmatig gecontroleerd en indien nodig vervangen, ten minste echter om de 10 jaar.
- Om de 20 000 schakelingen¹⁾ resp. starts²⁾ (wat als eerste optreedt) wordt het kroonwiel, evenals het wormwiel op slijtage gecontroleerd en indien nodig vervangen.
- De eindgebruiker waarborgt dat voor de veiligheidsfunctie “veilige terugmelding van de eindstanden” een testpercentage (PVST) wordt bereikt dat evenredig is aan de voor de respectievelijke toepassing geldende normen voor het te verwachten vraagpercentage.
- Aan alle eisen conform het gegevensblad “Technische gegevens voor schakelaars” (Y004.619) wordt voldaan. Met name de toelaatbare minimale en maximale stroom- en spanningswaarden.
- Het aantal schakelingen¹⁾, evenals het aantal schakelingen van elke afzonderlijke eindstand- resp. draaimomentschakelaar overschrijdt niet de in de hieronder afgebeelde tabel vermelde waarden:

1) Definitie van “schakelingen” conform DIN EN 15714-2:2010

2) Definitie van “starts” conform DIN EN 15714-2:2010

Tabel 3:

	Klasse A en B		Klasse C (modulatie)			
	zilver	goud	zilver	zilver	goud	goud
Contactmateriaal						
Maximale elektrische belasting			30 V/30 mA	250 V AC/5 A	30 V/30 mA	50 V/400 mA
Aantal toelaatbare schakelingen van de eindstandschakelaar, evenals van de schakelingen conform DIN EN 15714-2:2010	< 20 000	< 20 000	< 100 000	< 20 000	< 100 000	< 20 000

3.5. Overige informatie en gegevens voor het ontwerp en de berekening

De HFT is 0.

Voor het aansluiten op de afsluiter mogen alleen flenzen van de bouwgrootten F07 resp. FA07 of groter worden gebruikt.

Voor de “veilige terugmelding van de eindstanden” kan de aandrijving als zijnde een type A toestel worden beschouwd.

Veiligheidstechnische karakteristieke waarden

De voor het respectievelijke uitgeleverde product relevante veiligheidstechnische karakteristieke waarden, evenals mogelijke verdere beperkingen zijn in de verklaring van de fabrikant vermeld. Deze verklaring van de fabrikant is specifiek voor de order opgesteld en wordt direct met de order uitgeleverd.

3.6. Gebruiksvoorwaarden (omgevingscondities)

Bij het ontwerp en het gebruik van de aandrijvingen in veiligheidstechnische systemen moet erop worden gelet dat de toegestane gebruiksvoorwaarden, evenals de eisen aan de elektromagnetische compatibiliteit (EMC), door naburige apparatuur worden aangehouden. De gebruiksvoorwaarden staan in het technische gegevensblad:

- beschermingsklasse
- corrosiebescherming
- omgevingstemperatuur
- trillingsbestendigheid (vibratie)

Indien de werkelijke omgevingstemperaturen gemiddeld boven de +40 °C liggen, moeten de lambdawaarden met een veiligheidsfactor worden aangepast. Bij een gemiddelde temperatuur van +60 °C bedraagt deze factor 2,5.

Voor de omgevingstest heeft de aandrijving met besturingseenheid voor de aandrijving de volgende normen doorlopen:

- Droge warmte: EN 60068-2-2
- Vochtige warmte: EN 60068-2-30
- Kou: EN 60068-2-1
- Trillingstest: IEC 60068-2-6
- Seismische beproevingsmethoden voor apparaten (aardbeving): IEC 60068-3-3³⁾
- Controle van beschermingsgraad IP68: EN 60529
- Zoutneveltest: EN ISO 12944-6
- Storingsbestendigheid: DIN EN 61326-3-1
- Storende uitstraling: DIN EN 61000-6-4

3) alleen in de uitvoering thyristor

4. Veiligheidstechnische systemen en veiligheidsfuncties

Voor de aandrijvingen werd voor de berekening van de veiligheidstechnische karakteristieke waarden rekening gehouden met de hieronder vermelde veiligheidsfunctie:

- **Veilige terugmelding van de eindstanden**
Er is een direct op de aandrijving bekabelde eindstandmelding aanwezig. De veiligheidsfunctie is de correcte melding dat de aandrijving zich in de bewuste eindstand van de aandrijving⁴⁾ bevindt of niet. Uitsluitend de melding via dit meldkanaal is veiligheidsrelevant. Een terugmelding van de eindstanden via de relais van de I/O interface, via een standmelder (RWG, MWG, potentiometer, ...) of via een veldbusinterface geldt niet als veilige terugmelding van de eindstanden.

4) Houd er rekening mee dat de veiligheidstechnische karakteristieke waarden alleen de componenten van de aandrijving bevatten. Met overige evt. te beschouwen componenten (bijv. integriteit van externe besturingen, tandwielkasten, asgat afsluiter, andere componenten van de afsluiter, ...) is in de door AUMA vermelde karakteristieke waarden van dit product geen rekening gehouden.

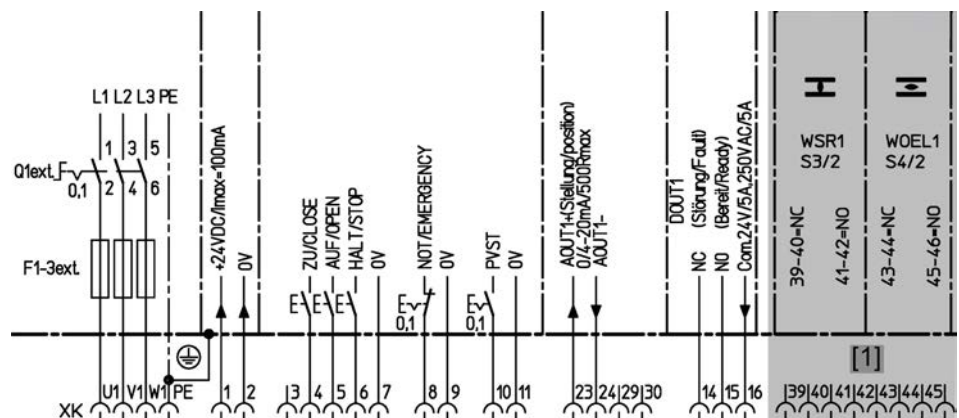
5. Installeren, inbedrijfstelling en gebruik

Informatie Het installeren en de inbedrijfstelling moeten door middel van een montagerapportage en een afnamecertificaat worden vastgelegd. Het installeren en de inbedrijfstelling mogen uitsluitend door geautoriseerd vakpersoneel worden uitgevoerd dat geschoold is op het gebied van de functionele veiligheid.

5.1. Installeren

De algemene installatiewerkzaamheden (montage, elektrische aansluitingen) dienen overeenkomstig de bij het toestel behorende bedieningsinstructies en het bijgevoegde, ordergerelateerde schakelschema te worden uitgevoerd.

Afbeelding 2: Voorbeeld schakelschema met veilige terugmelding van de eindstanden



[1] Wegschakelaars voor veilige terugmelding van de eindstanden

Het installeren en de inbedrijfstelling moeten worden gedocumenteerd en ter afsluiting dient er een installatie- en inbedrijfstellingsprotocol te worden opgemaakt.

Bij het aansluiten van de besturingseenheid voor de aandrijving op een veiligheids-plc en een PCS dient erop te worden gelet dat de respectievelijke gebruikte in- en uitgangen over gescheiden referentiepotentialen beschikken. Er moet via in- en uitgangen met een gemeenschappelijk referentiepotentiaal absoluut worden voorkomen dat een verbinding tussen het schakelcircuit van het veiligheidssysteem en het PCS tot stand wordt gebracht. Hierop dient vooral te worden gelet bij de keuze van de ingang voor het ESD-signaal, bij de in- en uitgangen van de PVST en bij de foutmelding (en evt. overige terugmeldingen).

Informatie De weergave van de stand van de afsluiter via een potentiometer of 4 – 20 mA signaal is mogelijk. Dit is echter geen bestanddeel van de vaststelling van de veiligheidstechnische karakteristieke waarden.

5.2. Inbedrijfstelling

Voor de algemene inbedrijfstelling moeten de bij het toestel behorende bedieningsinstructies in acht worden genomen.

Na de inbedrijfstelling moet de veilige werking van de aandrijving worden gecontroleerd.

5.3. Gebruik en werking

Regelmatig onderhoud en een regelmatige controle van het toestel in de door de eigenaar/gebruiker van de installatie vastgelegde T_{proof} intervallen zijn voorwaarden voor een betrouwbare werking.

Voor het gebruik moeten de bij het toestel behorende bedieningsinstructies in acht worden genomen.

De eigenaar/gebruiker van de installatie is verantwoordelijk voor het waarborgen van de energievoorziening.

Bij een fout dient het systeem direct te worden gecontroleerd en de installatie eventueel in de veilige toestand te worden gebracht.

5.4. Technische levensduur

De technische levensduur van de aandrijvingen is in de technische gegevens resp. in de bedieningsinstructies beschreven.

De veiligheidsrelevante karakteristieke waarden gelden voor de in de technische gegevens vastgelegde cycli resp. regelstappen en voor een typische gebruikperiode van maximaal 10 jaar (het als eerste bereikte criterium telt). Daarna zal het toestel waarschijnlijk vaker uitvallen.

Een verlenging van deze periode „door daartoe strekkende maatregelen door de fabrikant en de eigenaar/gebruiker“ als bedoeld in de nationale annotatie NOTE 3 met betrekking tot OPMERKING 3 van de Duitse versie van de norm IEC 61508-2:2010 7.4.9.5 b) is in veel gevallen principieel mogelijk. De verantwoordelijkheid te dezer zake berust bij de eigenaar/gebruiker die geschikte maatregelen dient te treffen. Op verzoek ondersteunen wij u graag bij het identificeren van geschikte maatregelen.

5.5. Buitenbedrijfstelling

Indien de aandrijving met veiligheidsfunctie buiten bedrijf wordt gesteld, dienen de hieronder vermelde aanwijzingen in acht te worden genomen:

- De invloed van de buitenbedrijfstelling op bijbehorende apparatuur, voorzieningen of andere werkzaamheden moet worden geëvalueerd.
- De veiligheidsvoorschriften en waarschuwingen in de bij de aandrijving behorende bedieningsinstructies moeten worden opgevolgd.
- De installatie mag uitsluitend door opgeleid en ter zake kundig personeel buiten bedrijf worden gesteld.
- De buitenbedrijfstelling moet adequaat worden gedocumenteerd.

6. Controles en onderhoud

Informatie	Controle- en onderhoudswerkzaamheden mogen uitsluitend door geautoriseerd vakpersoneel worden uitgevoerd, dat is geschoold op het gebied van de functionele veiligheid.
	De controle- en onderhoudsmiddelen dienen voorafgaand gekalibreerd te zijn.
	De controle/het onderhoud moet in een controle-/onderhoudsrapport worden vastgelegd.
	De invloed van de controle/het onderhoud op bijbehorende apparatuur, voorzieningen of andere werkzaamheden moet worden geëvalueerd.

6.1. Veiligheidsvoorziening controleren

Alle beschermende functies in een veiligheidsvoorziening dienen in gepaste intervallen op hun goede werking en veiligheid te worden gecontroleerd. Deze intervallen voor de controle van de veiligheidsvoorziening moeten door de eigenaar van de installatie worden vastgelegd.

Teneinde systematische fouten te voorkomen, dient de eigenaar/gebruiker van de installatie een veiligheidsplanning voor de gehele veiligheids-levenscyclus van de SIS op te stellen. Daarin dienen bijv. het beleid en de strategieën voor het bereiken van de veiligheid en de verschillende bezigheden resp. werkzaamheden tijdens de veiligheids-levenscyclus te zijn vermeld.

6.2. Proof-test (controle van de veilige werking van de aandrijving)

Informatie	Met de proof-test worden de veiligheidsrelevante functies van de aandrijving en besturingseenheid voor de aandrijving getest.
	De proof-test moet gevaarlijke fouten opsporen, die anders tot het in werking stellen van een veiligheidsfunctie onontdekt blijven en dan tot een gevaar kunnen leiden.
	Ter controle van de veiligheidsrelevante werking wordt de uitgang van de veilige terugmelding van de eindstand dienovereenkomstig gecontroleerd.
	Alle in de aandrijving geïnstalleerde resp. gebruikte veiligheidsfuncties moeten worden gecontroleerd en alle controlepunten overeenkomstig de bijbehorende checklists worden uitgevoerd.
	Intervallen: Een proof-test-interval beschrijft de tijd tussen twee proof-testen. De goede werking dient in gepaste intervallen te worden gecontroleerd. De eigenaar van de installatie moet deze intervallen vastleggen. In ieder geval dienen de veiligheidsrelevante functies na de inbedrijfstelling en na ieder onderhoud resp. iedere reparatie, evenals bij de in de veiligheidsbeschouwing vastgelegde T_{proof} intervallen te worden gecontroleerd.

6.2.1. Controles vooraf

Vooraf dient het aandrijfsysteem aan een visuele controle te worden onderworpen. Daarbij moet het systeem op uitwendige schade en corrosie worden gecontroleerd. Voorts dienen de elektrische en mechanische aansluitingen te worden gecontroleerd en de aandrijving met betrekking tot opvallende geluiden te worden geobserveerd terwijl hij ten minste eenmaal compleet van DICT naar OPEN en weer terug beweegt.

6.2.2. Controle en validatie van de veiligheidsfunctie “veilige terugmelding van de eindstanden”

Testverloop (checklist)	1. Aandrijving in de eindstand OPEN bewegen – wordt de eindstand OPEN via de veilige terugmelding van de eindstand gesignaleerd? 2. Aandrijving vanuit de eindstand OPEN bewegen – wordt de veilige terugmelding van de eindstand OPEN ingetrokken resp. geannuleerd? 3. Aandrijving weer in de eindstand OPEN bewegen – wordt de eindstand OPEN weer via de veilige terugmelding van de eindstand gesignaleerd?
--------------------------------	--

4. Aandrijving in de eindstand DICHT bewegen – wordt de eindstand DICHT via de veilige terugmelding van de eindstand gesignaleerd?
5. Aandrijving vanuit de eindstand DICHT bewegen – wordt de veilige terugmelding van de eindstand DICHT ingetrokken resp. geannuleerd?
6. Aandrijving weer in de eindstand DICHT bewegen – wordt de eindstand DICHT weer via de veilige terugmelding van de eindstand gesignaleerd?
7. Tijdens de gehele procedure geen foutmelding op het relais voor verzamelstoringsmeldingen K1?

6.2.3. Controle van de verzamelstoringsmelding

Configuratie	Deze controle geldt voor alle veiligheidsfuncties.
Testmethode	Controle of de verzamelstoringsmelding de fout correct meldt.
Testverloop	• Verzamelstoringsmelding (K1) door het simuleren van een fout afzonderlijk controleren. - Reageert signaleringsrelais op de gesimuleerde fout? - Reageert signaleringsrelais op het intrekken resp. annuleren van de gesimuleerde fout? • Na controle de foutsimulatie weer intrekken resp. annuleren.

6.3. Partial Valve Stroke Test (PVST).

— Optie —

Bij de Partial Valve Stroke Test (PVST) wordt het bewegen van de klep door middel van het voor een deel openen resp. sluiten binnen een ingestelde tijd gecontroleerd, zonder het proces te stoppen. Na een succesvol verlopen test beweegt de besturingseenheid voor de aandrijving de aandrijving weer terug naar de uitgangspositie.

De PVST dient voor de controle op goede werking van besturingen en aandrijvingen die niet regelmatig worden gebruikt en bijgevolg de reactiebewaking niet voor de diagnose kunnen gebruiken.

De diagnose door de PVST dient ten minste 10 maal vaker dan de proof-test te worden uitgevoerd.

De bewaking en evaluatie van de PVST moet door de rekenkundige-logische eenheid van het veiligheidstechnische systeem worden uitgevoerd. Hiervoor dient de verzamelstoringsmelding te worden geëvalueerd.

Veiligheidsfunctie veilige terugmelding van de eindstanden:

- Het bewegen van de aandrijving kan via een willekeurige ingang worden aangevraagd.
- De evaluatie, of de veiligheidsfunctie zoals gewenst meldt, moet door middel van de direct op de klantaansluiting bekabelde eindstandschakelaar worden uitgevoerd.
- De aandrijving moet zich in één van de volgende posities bevinden:
 - Voor de start van de testbeweging in één van beide eindstanden.
De testbeweging vindt dan vanuit de eindstand plaats en daarna weer terug in deze eindstand.
 - Voor de start van de testbeweging voldoende van beide eindstanden verwijderd.
De testbeweging vindt dan tot in de eindstand plaats en daarna weer uit deze eindstand.

In beide gevallen dient de stelweg zodanig te worden bepaald, dat een volledige bediening van de eindstandschakelaar kan worden verwacht. Controleer of de eindstandschakelaar zowel voor de start, tijdens de test, evenals na voltooiing van de test de respectievelijk te verwachten positie meldt.

- Verder moet er een dynamische bewaking van de testbeweging worden uitgevoerd d.w.z. een dynamische controle of de wijziging van het signaal overeenkomt met de verwachting.

Informatie Indien de PVST alleen vanuit resp. tot in één van beide eindstanden wordt uitgevoerd, wordt alleen de schakelaar van deze eindstand op goede werking gecontroleerd. Indien beide eindstandschakelaars (OPEN/DICHT) veiligheidsrelevant zijn, kan er bijv. een Full Stroke Test worden uitgevoerd.

6.4. Onderhoud

Onderhouds- en servicewerkzaamheden mogen uitsluitend door geautoriseerd vakpersoneel dat geschoold is op het gebied van de functionele veiligheid worden uitgevoerd.

Na onderhouds- en servicewerkzaamheden is ter controle van de werking bovendien een validatie van de veiligheidsfunctie, die minimaal alle in de hoofdstukken <Veiligheidsvoorziening controleren> en <Proof-test (controle van de veilige werking van de aandrijving)> beschreven controles omvat, absoluut noodzakelijk.

Indien tijdens het onderhoud een fout wordt geconstateerd, dan dient deze aan AUMA Riester GmbH & Co. KG te worden gemeld.

Informatie Bij AUMA aandrijvingen heeft het motorbedrijf voorrang op de handmatige bediening. Dat betekent dat de aandrijving indien nodig zelfstandig terugschakelt naar het motorbedrijf. Desondanks adviseren wij om na onderhouds- en servicewerkzaamheden het motorbedrijf in werking te stellen.

7. Veiligheidstechnische karakteristieke waarden

7.1. Bepaling van de karakteristieke waarden

- Aan de berekening van de veiligheidstechnische karakteristieke waarden liggen de genoemde veiligheidsfuncties ten grondslag. De beoordeling van de hardware vond op basis van een Failure Modes, Effects and Diagnostic Analysis (FMEDA) plaats. Een FMEDA is een stap in de beoordeling van de functionele veiligheid van een toestel in overeenstemming met IEC 61508. Op basis van de FMEDA worden de uitvalpercentages en het aandeel ongevaarlijke uitvallen van het toestel bepaald.
- De uitvalquota voor mechanische onderdelen werden afgeleid uit de veldrespons-gegevens en uit de exida-databank voor mechanische onderdelen. De elektronische uitvalpercentages zijn de basis-uitvalpercentages uit de SIEMENS-norm SN 29500.
- Overeenkomstig tabel 2 van de IEC 61508-1, ligt de gemiddelde PFD-waarde voor systemen, die voor de Low Demand Mode zijn geconstrueerd, op:
 - SIL 1-veiligheidsfuncties: $\geq 10^{-2}$ tot $< 10^{-1}$
 - SIL 2-veiligheidsfuncties: $\geq 10^{-3}$ tot $< 10^{-2}$
 - SIL 3-veiligheidsfuncties: $\geq 10^{-4}$ tot $< 10^{-3}$

Omdat aandrijvingen echter slechts een deel van de totale veiligheidsfuncties vormen, mag de PFD waarde van de aandrijving niet meer dan 25 % van de toegestane totale waarde (PFD_{avg}) van een veiligheidsfunctie bedragen. Daaruit resulteren de volgende waarden:

 - PFD aandrijving voor SIL 1-toepassingen: $\leq 2,50E-02$
- De veilige terugmelding van de eindstanden via direct op de klantgang bekabelde eindstandschakelaars kan als type A component met een hardware-fouttolerantie van 0 worden geclassificeerd. Voor het deelsysteem van type A moet de SFF bij $< 60\%$ overeenkomstig tabel 2 uit de norm IEC 61508-2 voor SIL 1 (deelsystemen met een hardware-fouttolerantie van 0) zijn. Voor het deelsysteem van type A moet de SFF tussen 60% en $< 90\%$ overeenkomstig tabel 2 uit de norm IEC 61508-2 voor SIL 2 (deelsystemen met een hardware-fouttolerantie van 0) zijn.
- Voor de berekening van de PFD-waarden werd van de hieronder vermelde aannames uitgegaan:
 - MRT = 72 uur
 - $T_d = 730$ uur = tijdsinterval PVST
 - MTTR = MRT + $T_d = 802$ uur

De in de verklaringen van de fabrikant en in dit veiligheidshandboek vermelde PFD-waarden dienen slechts als voorbeeld en zijn aan bepaalde aannames onderhevig bijv. over T_{proof} , MTTR, ... De PFD-berekening dient te allen tijde specifiek voor de installatie met de voor de respectievelijke installatie geldige parameters en operationele omgeving te worden uitgevoerd. Als input dienen de λ_{DU} en λ_{DD} waarden te worden gebruikt. Bij het naleven van de in dit veiligheidshandboek genoemde proof-testprocedures adviseren wij om met een Proof Test Coverage (PTC) van 90 % te rekenen.⁵⁾

Zoals reeds bij het ontwerp en de berekening werd aangegeven, is de eigenaar/gebruiker van de installatie verantwoordelijk voor het waarborgen van de energievoorziening en de daaruit resulterende berekeningen.

De eigenaar van de installatie is ervoor verantwoordelijk, fouten binnen de MTTR te verhelpen, omdat anders de gegevens van de kwantitatieve resultaten niet meer geldig zijn.

5) Bij de voorbeeldberekeningen in dit handboek en de verklaringen van de fabrikant is voor een deel van andere waarden voor PTC uitgegaan.

LET OP

De in dit veiligheidshandboek en in de verklaringen van de fabrikant vermelde veiligheidstechnische karakteristieke waarden zijn alleen geldig indien alle in dit veiligheidshandboek en in de verklaringen van de fabrikant genoemde voorwaarden worden nageleefd en de genoemde werkzaamheden worden uitgevoerd. Tevens moet rekening worden gehouden met de in de verklaringen van de fabrikant genoemde beperkingen inzake geldigheid en norm-conformiteit.

8. SIL-conformiteitsverklaring (voorbeeld)

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

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

**SIL Declaration of Conformity / SIL Declaration of Incorporation****Functional Safety according to IEC 61508****This document is only valid with order number imprinted by AUMA!****AUMA order no.**

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

Actuator type	Controls type/wiring diagram
SQ 05.2 – SQ 14.2 or SQR 05.2 – SQR 14.2 or SQEx 05.2 – SQEx 14.2 or SQREx 05.2 – SQREx 14.2 all with mounting flange F07 resp. FA07 or larger all in version SFC	AUMATIC AC 01.2/ACExC 01.2 or AUMA MATIC AM 01.1/AMExC 01.1 in version SFC with end position/torque switches directly wired to the customer connection or AUMA NORM (no control unit) with end position/ torque switches directly wired to the customer connection.

The above mentioned versions achieve the following safety integrity level for the "Safe End Position Feedback":

Hardware Safety Integrity	
Single channel use with PVST SQ 05.2 – 12.2 (HFT = 0)	SIL 2 capable
Single channel use with PVST SQ 14.2 (HFT = 0)	SIL 1 capable

For further details, please refer to supplement overleaf.

Michael Noll
Functional Safety Manager

Jörg Isenberg
Product Management

Date

Date

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

 <i>Solutions for a world in motion</i>	Supplement SIL Declaration of Conformity/ SIL Declaration of Incorporation Functional Safety according to IEC 61508	2019-01-07
---	---	------------

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

General	
Device designation and permissible types	See page 1
Safety function(s)	Safe End Position Feedback
Device type according to IEC 61508-2	☒ Type A ☐ Type B
Operating mode	☒ Low Demand Mode ☐ High Demand or Continuous Mode
Safety manual	Y006.639 (hb_sil_sq2_ac2_sfc) Y006.654 (hb_sil_sq2_am1_sfc)
Type of evaluation	☒ Evaluation by FMEDA according to IEC 61508-2
Evaluation by	EXIDA and AUMA Riester GmbH & Co. KG
Test report and test report version	Based on AUMA 15/07-029 R012 V0R1

SIL Integrity			
Hardware safety integrity for the "Safe End Position Feedback" (The calculated values are within the range for the corresponding SIL. However this does not imply that all related IEC 61508 requirements are fulfilled.)	Single channel use with PVST SQ 05.2 – SQ 12.2 (HFT = 0)	☐ SIL 1 capable	☒ SIL2 capable ☐ SIL3 capable
	Single channel use with PVST SQ 14.2 (HFT = 0)	☒ SIL1 capable	☐ SIL2 capable ☐ SIL3 capable

Safety function	Safe End position Feedback with PVST SQ 05.2 – SQ 12.2	Safe End position Feedback with PVST SQ 14.2
$\lambda_{SAFE}^{*1)}$	0 FIT	0 FIT
$\lambda_{DD}^{*1)}$	135 FIT	135 FIT
$\lambda_{DU}^{*1)}$	81 FIT	120 FIT
$DC_D^{*2)}$	62 %	52 %
MTBF - Mean Time Between Failures	176 years	157 years
SFF - Safe Failure Fraction	62 %	52 %
$PFD_{avg}^{*3)}$ with T[Proof] = 1 year	7,89E-04	1,12E-03

According to ISO 13849-1 the following Safety Metrics are achieved^{*4)}:

Safety function	Safe End position Feedback with PVST SQ 05.2 – SQ 12.2	Safe End position Feedback with PVST SQ 14.2
MTTF _D	528 years (high)	447 years (high)
DC	62 % (low)	52 % (none)
Calculated Performance Level	8,11E-08 1/h	1,20E-07 1/h
Achieved Performance Level ^{*4)}	CAT 1 or 2: PL = „c“ capable	CAT 1: PL = „c“ capable

^{*1)} FIT = Failure In Time, Number of failures per 10⁹ h

^{*2)} DC_D = Diagnostic Coverage (dangerous)

^{*3)} PFD_{avg} = Probability of a failure on demand (average)

^{*4)} Depending on the application and possible external diagnostics a higher DC and therefore also a higher category and a higher Performance level might be possible to achieve.

 Solutions for a world in motion	Supplement SIL Declaration of Conformity/ SIL Declaration of Incorporation Functional Safety according to IEC 61508	2019-01-07
--	---	------------

Restrictions

- The safety figures for Safe End Position Feedback function are only valid if the end position switches **directly** wired to the customer connection are used for end position evaluation.
- In "low demand mode" monthly diagnostic of these switches via Partial Valve Stroke Test (PVST) (operation mode "end position test" of safety handbook or equivalent) controlled by the Safety PLC is necessary.
- The failure rates are only valid if safety switches with extension "-S or "-SIL" are used (e.g. characteristics 8-S, 8.2-S, ...)
- The failure rates are only valid for the useful lifetime (see safety handbook)
- The average operation temperature is assumed to be no higher than 40°C. If the actual ambient temperatures exceed an average of +40 °C, the lambda values have to be incremented by a safety factor.
- The SIL/PL has to be evaluated for the complete (sub) system. The numbers listed are for reference only.

High demand mode is feasible for the safe end position feedback if the following is observed:

- the total number of strokes and cycles allowed for the used actuator type is not exceeded during the useful lifetime and
- the total number of cycles of the end position feedback does not exceed 100.000 during the useful lifetime if control voltages/currents of maximum 30 V AC/DC and 30 mA are applied and
- the total number of cycles of the end position feedback does not exceed 20.000 during the useful lifetime if control voltages/currents of up to 250 V AC/DC and 5A are applied for switches with silver contacts and
- the total number of cycles of the end position feedback does not exceed 20.000 during the useful lifetime if control voltages/currents of up to 50 V AC/DC and 400mA are applied for switches with gold contacts and
- every 20.000 cycles of the end position feedback the crown wheel and worm wheel are checked for wear and exchanged if necessary and
- the user has to ensure that for the safety function "Safe End Position Feedback" a test rate (PVST) per the requirements of the applicable standard(s) is achieved.
- the grease is exchanged at least every 10 years or earlier if necessary.

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

²⁾ DC_D = Diagnostic Coverage (dangerous)

³⁾ PFD_{avg} = Probability of a failure on demand (average)

⁴⁾ Depending on the application and possible external diagnostics a higher DC and therefore also a higher category and a higher Performance level might be possible to achieve.

Trefwoordenregister

A

Aandeel ongevaarlijke uitvalgebeurtenissen (SFF) 4

B

Bedrijfsmodus 8
Berekening resp. bepaling van de aandrijving 7
Buitenbedrijfstelling 12

C

Configuratie 7
Conformiteitsverklaring 18
Controles 13

D

DC 4
Diagnosedekkingsgraad 4

E

Energievoorziening 7

G

Gebruik en werking 11
Gebruiksvoorwaarden 9
Gemiddeld risico van uitvallen (MTBF) 4

H

Herhalingscontrole 13
Herhalingstest 5
HFT 4

I

Inbedrijfstelling 11
Installeren 11
Instelling 7
Interval voor herhalingstest 4

K

Karakteristieke waarden 16

L

Lambdawaarden 4
Low Demand Mode 16

M

MRT (Mean Repair Time) 5
MTBF 4
MTTR (Mean Time To Restoration) 5

N

Normen 6

O

Omgevingscondities 9
Onderhoud 15
Ontwerp 7

P

Partial Valve Stroke Test (PVST). 14
PFD 4
PFD-aandrijving 16
Proof-test 13

R

Rem 8
Risico van uitvallen 4

S

SFF 4
SIL 4

T

Technische levensduur 12
Toepassingsgebied 6
Toesteltypen 6
T proof 4

U

Uitvalwaarschijnlijkheid 12

V

Veiligheidsfunctie 4
Veiligheidsfuncties 10
Veiligheidsrelevant systeem 5
Veiligheidstechnische functie (SIF) 4
Veiligheidstechnisch systeem (SIS) 5

Z

Zelfremmendheid 8

AUMA Riester GmbH & Co. KG

P.O. Box 1362
DE 79373 Muellheim
Tel +49 7631 809 - 0
Fax +49 7631 809 - 1250
info@auma.com
www.auma.com

AUMA BENELUX B.V.
NL 2314 XT Leiden
Tel +31 71 581 40 40
Fax +31 71 581 40 49
office@auma.nl
www.auma.nl