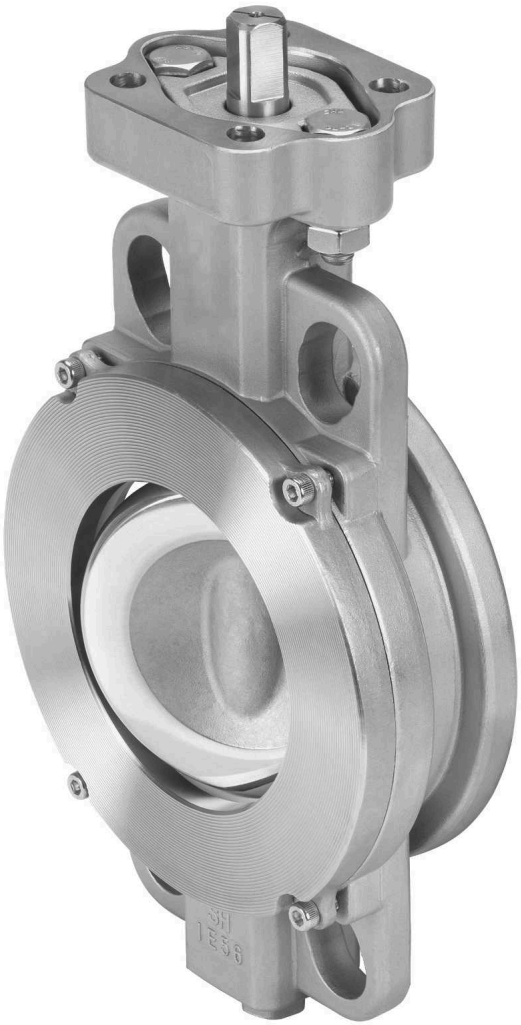
GEMÜ R470 Tugela

Doppelexzentrische Absperrklappe mit freiem Wellenende
Double-eccentric butterfly valve with bare shaft

DE **SIL-Sicherheitshandbuch**

EN **SIL Safety Manual**



Weitere Informationen
Webcode: GW-R470

Dokument zum künftigen Nachschlagen aufbewahren.
Keep the document for future reference.

20.06.2024

Inhalt

1 Allgemeines

Das Sicherheitshandbuch enthält Informationen und Sicherheitshinweise, die für den Einsatz der Absperrklappe in sicherheitsbezogenen Anwendungen gelten.

Das Sicherheitshandbuch gilt nur in Verbindung mit den jeweiligen Montage-, Betriebs- und Wartungsanleitungen.

Bezeichnung	Artikelnummer
ba_R470_de_gb	88740803

1.1 Begriffsbestimmungen

Automatische Diagnose

Tests, die intern im Prozess von dem Gerät oder, falls so festgelegt, extern von einem anderen Gerät ohne manuellen Eingriff durchgeführt werden.

Dichte Abschaltung

Zustand, in dem das Produkt geschlossen ist und so gut abdichtet, dass die Leckage nicht größer als die definierte Leckrate ist. Anforderungen bezüglich einer dichten Abschaltung müssen anwendungsspezifisch festgelegt werden. Wenn die Abschaltanforderungen einen größeren Durchfluss als ANSI Klasse V bzw. ANSI Klasse IV zulassen, können die Zahlen für die Endlage verwendet werden.

Dynamische Anwendungen

Das Bewegungsintervall des Endelementgeräts beträgt weniger als 200 Stunden. Die Bewegung kann mittels Teilöffnungstest, Proof-Test oder eine Anforderung des Systems erfolgen.

Element

Eine Sammlung von Geräten, die eine Element-Sicherheitsfunktion übernehmen, beispielsweise ein Endelement bestehend aus einer Logiksystemschnittstelle, einem Ventilantrieb und einem Ventil.

exida-Kriterien

Ein konservativer Ansatz zur Ermittlung von Ausfallraten, geeignet für den Einsatz in Gerätebewertungen, unter Verwendung des 2_H-Pfads nach IEC 61508-2.

Fehlertoleranz

Fähigkeit einer Funktionseinheit, bei Vorliegen von Fehlern oder Störungen eine geforderte Funktion weiterhin zu übernehmen (IEC 61508-4, 3.6.3).

Freisetzung nach außen

Ausfall, der dazu führt, dass Prozessmedien aus dem Produkt nach außen freigesetzt werden; eine Freisetzung nach außen wird nicht als Teil der Sicherheitsfunktion betrachtet. Die Ausfallraten mit Freisetzung nach außen finden keinen direkten Eingang in die Zuverlässigkeit eines Produkts, sie sollten jedoch im Hinblick auf sekundäre Sicherheits- und Umweltaspekte geprüft werden.

Gefahrbringender Ausfall

Ein gefahrbringender Ausfall („D“ für „dangerous“) ist definiert als Ausfall, der bei der Umsetzung der Sicherheitsfunktion eine Rolle spielt und der:

- verhindert, dass eine Sicherheitsfunktion bei Anforderung wirksam wird (Bedarfsbetrieb), oder der dazu führt, dass eine Sicherheitsfunktion ausfällt (Dauerbetrieb), sodass das EUC in einen gefährlichen oder potenziell gefährlichen Zustand versetzt wird; oder
- die Wahrscheinlichkeit verringert, dass die Sicherheitsfunktion bei Anforderung ordnungsgemäß arbeitet.

Gefahrbringend erkannt

Ein Ausfall, der gefahrbringend ist, jedoch durch externe Prüfungen erkannt wird.

Gefahrbringend nicht erkannt

Ein Ausfall, der gefahrbringend ist und nicht diagnostiziert wird.

Gerät

Ein Gerät ist Teil eines Elements, kann jedoch allein keine Element-Sicherheitsfunktion übernehmen.

Ohne Wirkung

Ausfallmodus einer Komponente, die bei der Umsetzung der Sicherheitsfunktion eine Rolle spielt, wobei es sich jedoch weder um einen sicheren Ausfall noch um einen gefahrbringenden Ausfall handelt.

PVST

"Partial Valve Stroke Test" – Teilöffnungstest: Es wird davon ausgegangen, dass der Teilöffnungstest, sofern durchgeführt, automatisch um mindestens eine Größenordnung häufiger durchgeführt wird als der Proof-Test; deshalb kann der Test als automatische Diagnose betrachtet werden. Aufgrund der Betrachtung als automatische Diagnose hat der Teilöffnungstest auch Auswirkungen auf den Anteil sicherer Ausfälle.

Severe Service

Zustand, der vorliegt, wenn das durch das Ventil strömende Medium Schleifpartikel enthält, im Gegensatz zum Clean Service, bei dem keine derartigen Partikel enthalten sind.

Sicherer Ausfall

Ein sicherer Ausfall („S“ für „safe“) ist definiert als Ausfall, der bei der Umsetzung der Sicherheitsfunktion eine Rolle spielt und der:

- dazu führt, dass die unerwünschte Arbeitsweise der Sicherheitsfunktion das EUC („Equipment Under Control“) (oder einen Teil davon) in einen sicheren Zustand versetzt oder einen sicheren Zustand aufrechterhält; oder
- die Wahrscheinlichkeit erhöht, dass die unerwünschte Funktionsweise der Sicherheitsfunktion das EUC (oder einen Teil davon) in einen sicheren Zustand versetzt oder einen sicheren Zustand aufrechterhält.

Stationäre Anwendungen

Das Bewegungsintervall des Endelementgeräts beträgt mehr als 200 Stunden. Die Bewegung kann mittels Teilöffnungstest, Proof-Test oder eine Anforderung des Systems erfolgen.

Teilöffnungstest

Es wird davon ausgegangen, dass der Teilöffnungstest, sofern durchgeführt, mindestens um eine Größenordnung häufiger durchgeführt wird als der Proof-Test; deshalb kann der Test als automatische Diagnose betrachtet werden. Aufgrund

der Betrachtung als automatische Diagnose hat der Teilöffnungstest auch Auswirkungen auf den Anteil sicherer Ausfälle.

Typ-A-Element

„Nicht komplexes“ Element (alle Fehlermöglichkeiten sind klar definiert); Einzelheiten siehe unter 7.4.4.1.2 von IEC 61508-2

1.2 Abkürzungen

FIT

„Failure in Time“: Ausfallrate ($1x10^{-9}$ Ausfälle pro Stunde)

FMEDA

"Failure Modes, Effects, and Diagnostic Analysis": Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse

HFT

"Hardware Fault Tolerance": Hardware-Fehlertoleranz

MTTFd

„Mean Time To Dangerous Failure“: Mittlere Zeit bis zum gefährlichen Ausfall in Jahren

PVST

„Partial Valve Stroke Test“: Teilöffnungstest

SIF

"Safety Instrumented Function": sicherheitstechnische Funktion

SIL

"Safety Integrity Level": Sicherheitsintegritätslevel

SIS

"Safety Instrumented System": Implementierung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus einer beliebigen Kombination von Sensor(en), Logiklöser(n) und Endelement(en).

SSI

"Site Safety Index": Werksicherheitsindex

2 Normen / verwendete Literatur

Die von der Prüforganisation exida erbrachten Leistungen wurden auf der Grundlage der folgenden Normen/Literatur durchgeführt:

IEC 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Component Reliability Database Handbook, 5. Auflage, 2021, Band 2	exida LLC, Component Reliability Database Handbook, fünfte Auflage, 2021, Band 2 - Electrical Components ISBN 978-1-934877-09-5
Component Reliability Database Handbook, 5. Auflage, 2021, Band 3	exida LLC, Component Reliability Database Handbook, fünfte Auflage, 2021, Band 3 - Electrical Sensor Components ISBN 978-1-934977-22-4
Goble, W.M.,2010	Control Systems Safety Evaluation and Reliability, dritte Auflage, ISA, ISBN 97B-1-934394-80-9. Referenz zu FMEDA-Methoden
IEC 60654-1:1993-02, 2. Auflage	Leittechnische Einrichtungen für industrielle Prozesse; Umgebungsbedingungen; Teil 1: Klimatische Einflüsse
O’Brien, C., Stewart, L., & Bredemeyer, L., 2018	Exida LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, 2018, ISBN 978-1-934977-18-7
Scaling the Three Barriers, Aufgezeichnetes Webinar, Juni 2013	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
Meeting Architecture Constraints in SIF Design, Aufgezeichnetes Webinar, März 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
Random versus Systematic – Issues and Solutions, September 2016	https://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
Bukowski, J.V. & Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
Bukowski, J.V. & Stewart, L.L., April 2016	Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York

Criteria for the Application of IEC 61508:2010 Route 2H, Dezember 2016	Exida-White Paper, Sellersville, PA www.exida.com
Goble, W.M. & Brombacher, A.C., November 1999, Band 66, No. 2	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Band 66, Nr. 2, November 1999.
ISO 13849-1:2016	Safety of machinery – Safety-related parts of control systems – Teil 1: General principles for design

3 Beschreibung

Die doppelexzentrische Absperrklappe GEMÜ R470 Tugela aus Metall verfügt über ein freies Wellenende mit Kopfflansch nach EN ISO 5211. Die Absperrklappe ist in den Nennweiten DN 50 bis 600 und in genormten Einbaulängen API 609 Kategorie A (DIN 3202 K1) verfügbar.

3.1 Sicherheitsfunktion

Die Sicherheitsfunktion der Absperrklappe besteht darin, bei Auslösung zu öffnen, bei Auslösung zu schließen oder bei Auslösung dicht abzusperren.

3.2 Nutzungsdauer

Basierend auf allgemeinen Ausfalldaten wird für die Absperrklappe Typ R470 eine Nutzungsdauer von ca. 15 Jahren erwartet.

Die Nutzungsdauer ist ein Begriff der Zuverlässigkeitstechnik, der das Betriebszeitintervall beschreibt, in dem die Ausfallrate eines Produkts relativ konstant ist. Es handelt sich nicht um einen Begriff, der Produktalterung, Garantie oder andere kommerzielle Probleme abdeckt.

4 Proof-Tests zur Erkennung unerkannter gefahrbringender Ausfälle

Gemäß Abschnitt 7.4.5.2 f) der IEC 61508-2 müssen Proof-Tests durchgeführt werden, um gefahrbringende Ausfälle zu erkennen, die durch automatische Diagnosetests nicht erkannt werden. Dies bedeutet, dass festgelegt werden muss, wie unerkannte gefahrbringende Ausfälle, die bei der Analyse der Fehlerarten, Fehlerauswirkungen und Fehlerdiagnose festgestellt wurden, bei der Nachweisprüfung entdeckt werden können.

Der vorgeschlagene Proof-Test besteht aus einem Schwenken des zugehörigen Geräts in die Endlage.

Schritt	Aktion
1	Überbrücken Sie die Sicherheitsfunktion und ergreifen Sie geeignete Maßnahmen, um eine Fehlauslösung zu vermeiden.
2	Unterbrechen oder ändern Sie die Luftzufuhr / den Eingang zum Antrieb, um die Antriebs-/Ventilbaugruppe in den ausfallsicheren Zustand zu zwingen, und bestätigen Sie, dass der sichere Zustand innerhalb der richtigen Zeit erreicht wurde. Hinweis: Damit werden alle Fehler geprüft, die das Funktionieren des Stellventils und des übrigen Stellglieds verhindern könnten.
3	Prüfen Sie den Antrieb und das Gehäuse auf undichte Stellen, sichtbare Schäden oder Verunreinigungen.
4	Stellen Sie die ursprüngliche Luftzufuhr / den ursprünglichen Eingang zum Antrieb wieder her und bestätigen Sie, dass der normale Betriebszustand erreicht wurde.
5	Entfernen Sie den Bypass und stellen Sie den Normalbetrieb wieder her.

Damit der Test wirksam ist, muss die Bewegung des Ventils bestätigt werden. Um die Wirksamkeit des Tests zu bestätigen, müssen sowohl der Ventilweg als auch die Schwenkgeschwindigkeit überwacht und mit den erwarteten Ergebnissen verglichen werden, um die Prüfung zu validieren.

5 Fehlerkategorienbeschreibung

Um das Versagensverhalten der Absperrklappe zu beurteilen, wurden folgende Definitionen für das Versagen des Geräts berücksichtigt.

Ausfallsicherer Zustand:	
Ventil, Endlage	Zustand, in dem das Ventil geschlossen ist.
Ventil, dichte Absperrung	Zustand, in dem das Ventil geschlossen und abgedichtet ist, wobei die Leckage nicht größer als die definierte Leckagerate ist. Die Anforderungen an die dichte Abschaltung müssen entsprechend der Anwendung spezifiziert werden. Wenn die Anforderungen an die Absperrung einen größeren Durchfluss als ANSI-Klasse V bzw. ANSI-Klasse IV zulassen, können die Werte für das Schwenken in die Endlage verwendet werden.
Ventil, Bei Auslösung öffnen	Zustand, in dem das Ventil geöffnet ist.
Sicherer Ausfall	Ausfall, der dazu führt, dass das Gerät ohne Anforderung durch den Prozess in den definierten ausfallsicheren Zustand wechselt.
Gefahrbringender Ausfall	Ausfall, der nicht auf eine Anforderung des Prozesses reagiert (d. h. nicht in der Lage ist, in den definierten ausfallsicheren Zustand zu wechseln).
Ventil	Ausfall, der verhindert, dass das Ventil innerhalb der normalen Zeitspanne in den definierten ausfallsicheren Zustand wechselt.
Gefahrbringender nicht erkannter Ausfall	Ausfall, der gefährlich ist und nicht durch eine externe automatische Diagnostik, wie z. B. einen Teilöffnungstest, diagnostiziert wird.
Gefahrbringender erkannter Ausfall	Ausfall, der gefährlich ist, aber von automatischer Diagnose, wie z. B. einem Teilöffnungstest, erkannt wird.
Ohne Wirkung	Ausfall eines Bauelements, das Teil der Sicherheitsfunktion ist, aber keinen Einfluss auf die Sicherheitsfunktion hat.
Freisetzung nach außen	Ausfall, bei dem Prozessflüssigkeiten, Gas, Hydraulikflüssigkeiten oder Betriebsmittel aus dem Ventil oder Ventilantrieb austreten. Freisetzung nach außen wird nicht als Teil der Sicherheitsfunktion betrachtet und daher ist diese Ausfallrate in keinem der Werte enthalten. Die Ausfallrate der Freisetzung nach außen sollte im Hinblick auf sekundäre Sicherheits- und Umweltaspekte überprüft werden.

Die oben aufgeführten Fehlerkategorien erweitern die in IEC 61508 aufgelisteten Kategorien, um einen vollständigen Satz von Daten zu liefern, die für die Designoptimierung benötigt werden.

6 Annahmen

- Es wird die Worst-Case-Annahme eines Seriensystems getroffen. Daher führt der Ausfall einer Einzelkomponente zum Ausfall der gesamten Absperrklappe und die Ausbreitung von Fehlern ist nicht relevant.
- Ausfallraten sind über die Nutzungsdauer konstant.
- Jedes Bauelement des Produkts, welches die Sicherheitsfunktion nicht beeinflussen kann, (rückwirkungsfrei) wird ausgeschlossen. Alle Bauelemente, die Teil der Sicherheitsfunktion sind, einschließlich derer, die für den normalen Betrieb benötigt werden, werden in die Analyse einbezogen.
- Die Belastungswerte sind in dem für die Analyse verwendeten exida-Profil angegeben und werden durch die vom Hersteller veröffentlichten Klassifizierungen begrenzt.
- Materialien sind mit den Umgebungs- und Prozessbedingungen kompatibel.
- Das Gerät wird gemäß den Anweisungen des Herstellers eingebaut und betrieben.
- Ventile sind so installiert, dass das geregelte Medium in der Richtung durch das Ventil strömt, die durch den am Ventilkörper angebrachten Durchflusspfeil angegeben ist.
- Um den Diagnosedeckungsgrad für den Teilöffnungstest zu beanspruchen, wird dieser automatisch mit einer Rate durchgeführt, die mindestens zehnmal schneller ist als die Anforderungshäufigkeit.
- Der Teilöffnungstest der sicherheitsgerichteten Funktion bietet einen vollständigen Zyklustest des Magnetventils / Pilotventils. In Fällen, in denen dies nicht zutrifft, muss eine andere Methode verwendet werden, um einen vollständigen Ventilzyklus während der automatischen Diagnose durchzuführen, damit die PVST-Nummern verwendet werden können.
- Der Teilöffnungstest des Endelements umfasst die Positionserfassung von am Antrieb montierten Stellungsensoren, die typisch für Installationen mit Schwenkbetätigung sind.
- Die interne Worst-Case-Fehlererkennungszeit ist das PVST-Testintervall.

7 exida-Profile

exida-Profil	1	2	3	4	5	6
Beschreibung (Elektrisch)	Mit Gehäuse montiert Klimatisiert	Mit Niederspannung montiert nicht selbstbeheizt	Mit Normalspannung montiert selbstbeheizt	Tiefsee	Hochsee	Nicht verfügbar
Beschreibung (Mechanisch)	Mit Gehäuse montiert Klimatisiert	Mit Normalspannung montiert	Mit Normalspannung montiert	Tiefsee	Hochsee	Prozess berührt
IEC 60654-1 Profil	B2	C3 Auch anwendbar für D1	C3 Auch anwendbar für D1	Nicht verfügbar	C3 Auch anwendbar für D1	Nicht verfügbar
Durchschnittliche Umgebungstemperatur	30°C	25°C	25°C	5°C	25°C	25°C
Durchschnittliche Innentemperatur	60°C	30°C	45°C	5°C	45°C	Temperatur Betriebsflüssigkeit
Tägliche Temperaturauslenkung (Höhepunkt bis Höhepunkt)	5°C	25°C	25°C	0°C	25°C	Nicht verfügbar
Saisonaler Temperaturunterschied (Mittelwert Winter im Vergleich zum Mittelwert Sommer)	5°C	40°C	40°C	2°C	40°C	Nicht verfügbar
Elementen oder dem Wetter ausgesetzt	Nein	Ja	Ja	Ja	Ja	Ja
Feuchtigkeit [1)]	0-95% Nicht kondensierend	0-100% Kondensierend	0-100% Kondensierend	0-100% Kondensierend	0-100% Kondensierend	Nicht verfügbar
Stoß [2)]	10 g	15 g	15 g	15 g	15 g	Nicht verfügbar
Vibration [3)]	2 g	3 g	3 g	3 g	3 g	Nicht verfügbar
Chemische Korrosion [4)]	G2	G3	G3	G3	G3	Kompatibles Material
Anstieg [5)]						
Linie bis Linie	0,5 kV	0,5 kV	0,5 kV	0,5 kV	0,5 kV	Nicht verfügbar
Linie bis Grund	1 kV	1 kV	1 kV	1 kV	1 kV	Nicht verfügbar
EMI Anfälligkeit [6)]						
80 MHz bis 1,4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	Nicht verfügbar
1,4 GHz bis 2,0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	Nicht verfügbar
2,0 GHz bis 2,7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	Nicht verfügbar
ESD (Luft) [7)]	6 kV	6 kV	6 kV	6 kV	6 kV	Nicht verfügbar

1) Feuchtigkeitsklasse IEC 60068-2-3

2) Stoßklasse IEC 60068-2-6

3) Vibrationsklasse IEC 60770-1

4) Chemische Korrosionsklasse ISA 71.04

5) Anstiegsklasse IEC 61000-4-5

6) EMI Anfälligkeitsklasse IEC 6100-4-3

7) ESD (Luft) Klasse IEC 61000-4-2

8 Profile für den Werkssicherheitsindex

Der SSI ist eine Zahl von 0 bis 4, die das Niveau der Standortaktivitäten und -praktiken angibt, die zur Sicherheitsleistung der sicherheitstechnischen Funktionen am Standort beitragen. Es ist zu beachten, dass die Zahlen die Stufen der SIL-Zuordnung widerspiegeln und dass SSI 4 bedeutet, dass alle Anforderungen der Normen IEC 61508 und IEC 61511 am Standort erfüllt werden und dass es daher keine Beeinträchtigung der Sicherheitsleistung durch Aktivitäten oder Praktiken des Endnutzers gibt, d. h. dass die prinzipielle inhärente Sicherheitsleistung erreicht wird.

Bislang wurden mehrere Faktoren ermittelt, die sich auf die SSI auswirken. Dazu gehört die Qualität folgender Prüfungen:

- Inbetriebnahmeprüfung
- Proof-Test-Verfahren
- Dokumentation der Abnahmeprüfung
- Fehlerdiagnose- und Reparaturverfahren
- Verfahren zur Verfolgung der Nutzungsdauer und zum Austausch von Geräten
- SIS-Änderungsverfahren
- Verfahren zur Außerbetriebnahme des SIS
- und andere

Niveau	Beschreibung
SSI 3	Fast perfekt - Reparaturen werden korrekt durchgeführt - Prüfungen werden korrekt und termingerecht durchgeführt - Das Material wird in der Regel auf der Grundlage der spezifizierten Umweltgrenzwerte und einer guten Analyse der Prozesschemie und der kompatiblen Materialien ausgewählt - Die elektrischen Stromversorgungen sind in der Regel frei von Überspannungen und isoliert - Die pneumatischen Versorgungen und die Hydraulikflüssigkeiten werden meist sauber gehalten usw. - Geräte werden vor dem Ende der Lebensdauer ausgetauscht - usw.
SSI 2	Gut - Reparaturen werden in der Regel korrekt ausgeführt - Prüfungen werden korrekt und meist termingerecht durchgeführt - Die meisten Geräte werden vor Ablauf der Nutzungsdauer ersetzt - usw.
SSI 1	Mittel - Viele Reparaturen werden korrekt durchgeführt - Prüfungen werden durchgeführt und meist termingerecht durchgeführt - Einige Geräte werden vor Ablauf der Nutzungsdauer ersetzt - usw.
SSI 0	Keine - Reparaturen werden nicht immer durchgeführt - Prüfungen werden nicht durchgeführt - Geräte werden erst ersetzt, wenn sie defekt sind - usw.

9 SIL-Ausfallratenberechnung GEMÜ R470 (Stationäre Anwendung)

SIL-Ausfallratenberechnung

Funktionale Sicherheit nach IEC 61508 und IEC 61511

Wir, die Firma

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8
D-74653 Ingelfingen-Criesbach

erklären, dass für das unten aufgeführte Produkt in sicherheitsbezogenen Anwendungen gemäß IEC 61508 und IEC 61511 die unten aufgeführten Ausfallraten ermittelt wurden.

Die Ausfallraten wurden durch eine FMEDA (Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse) nach IEC 61508 ermittelt. Die Bewertung wurde durch exida.com durchgeführt (Berichtsnummer: GEMÜ 22/07-012 R006).

Produktbeschreibung:	GEMÜ-Absperrklappe R470 Tugela®
Gerätetyp:	A
Sicherheitsfunktion:	Die Sicherheitsfunktion der Absperrklappe besteht darin, bei Auslösung zu öffnen, bei Auslösung zu schließen oder bei Auslösung dicht abzusperren.
HFT (Hardware-Fehlertoleranz):	0
MTTR (Mittlere Zeit bis zur Wiederherstellung):	48 Stunden

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate (SSI=2):

	Ausfallraten Clean Service* (in FIT**)					
	Ohne externen Test			Mit externem Test		
	Geschlossen-Stellung		Offen-Stellung	Geschlossen-Stellung		Offen-Stellung
	Endlage	Dichtschließend		Endlage	Dichtschließend	
Sicherheitsfunktion:	1635	986	1635	1635	986	1635
Freisetzung nach außen	158	158	158	158	158	158
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Gefahrbringend nicht erkannt):	580	1230	462	339	989	221
λ $_{DD}$ (Gefahrbringend erkannt):	0	0	0	241	241	241
λ $_{SU}$ (Sicher nicht erkannt):	0	0	118	0	0	1
λ $_{SD}$ (Sicher erkannt):	0	0	0	0	0	117
PTC (Proof Test-Deckungsgrad):	62 %	29 %	78 %	36 %	12 %	55 %
MTTF Sicherheitsfunktion (Mittlere Zeit bis zum Ausfall):	205	83	206	205	83	206
MTTF Gesamtprodukt (Mittlere Zeit bis zum Ausfall):	60	60	60	60	60	60
MTTF D in a (Mittlere Zeit bis zum Ausfall):	205	83	300	205	83	300

1) Diese SIL-Einstufung bedeutet ausschließlich, dass die berechneten Werte innerhalb des Bereichs für hardwarebezogene architektonische Einschränkungen für den entsprechenden SIL liegen.

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate (SSI=2):

	Ausfallraten Severe Service*** (in FIT**)					
	Ohne externen Test			Mit externem Test		
	Geschlossen-Stellung		Offen-Stellung	Geschlossen-Stellung		Offen-Stellung
	Endlage	Dichtschließend		Endlage	Dichtschließend	
Sicherheitsfunktion:	2107	986	2107	2107	986	2107
Freisetzung nach außen	279	279	279	279	279	279
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Gefahrbringend nicht erkannt):	865	1987	629	556	1678	320
λ $_{DD}$ (Gefahrbringend erkannt):	0	0	0	309	309	309
λ $_{SU}$ (Sicher nicht erkannt):	0	0	236	0	0	2
λ $_{SD}$ (Sicher erkannt):	0	0	0	0	0	234
PTC (Proof Test-Deckungsgrad):	54 %	23 %	74 %	28 %	9 %	48 %
MTTF Sicherheitsfunktion (Mittlere Zeit bis zum Ausfall):	120	44	120	120	44	120
MTTF Gesamtprodukt (Mittlere Zeit bis zum Ausfall):	35	35	35	35	35	35
MTTF D in a (Mittlere Zeit bis zum Ausfall):	120	44	189	120	44	189

1) Diese SIL-Einstufung bedeutet ausschließlich, dass die berechneten Werte innerhalb des Bereichs für hardwarebezogene architektonische Einschränkungen für den entsprechenden SIL liegen.

Da die Ausfallraten für die Freisetzung nach außen eine Teilmenge der Ausfallraten ohne Wirkung sind, entspricht die Gesamtausfallrate ohne Wirkung der Summe der aufgelisteten Ausfallraten ohne Wirkung und der Freisetzungen nach außen. Die Ausfallraten mit Freisetzung nach außen finden keinen direkten Eingang in die Zuverlässigkeit des Geräts, sie sollten jedoch im Hinblick auf sekundäre Sicherheits- und Umweltaspekte geprüft werden.

* Clean Service = ohne Schleifpartikel

** FIT = Failure In Time – Ausfallrate ($1x10^{-9}$ Ausfälle pro Stunde)

*** Severe Service = mit Schleifpartikeln

10 SIL-Ausfallratenberechnung GEMÜ R470 (Dynamische Anwendung)

SIL-Ausfallratenberechnung

Funktionale Sicherheit nach IEC 61508 und IEC 61511

Wir, die Firma

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8
D-74653 Ingelfingen-Criesbach

erklären, dass für das unten aufgeführte Produkt in sicherheitsbezogenen Anwendungen gemäß IEC 61508 und IEC 61511 die unten aufgeführten Ausfallraten ermittelt wurden.

Die Ausfallraten wurden durch eine FMEDA (Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse) nach IEC 61508 ermittelt. Die Bewertung wurde durch exida.com durchgeführt (Berichtsnummer: GEMÜ 22/07-012 R006).

Produktbeschreibung:	GEMÜ-Absperrklappe R470 Tugela®
Gerätetyp:	A
Sicherheitsfunktion:	Die Sicherheitsfunktion der Absperrklappe besteht darin, bei Auslösung zu öffnen, bei Auslösung zu schließen oder bei Auslösung dicht abzusperren.
HFT (Hardware-Fehlertoleranz):	0
MTTR (Mittlere Zeit bis zur Wiederherstellung):	48 Stunden

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate (SSI=2):

	Ausfallraten Clean Service* (in FIT**)					
	Ohne externen Test			Mit externem Test		
	Geschlossen-Stellung		Offen-Stellung	Geschlossen-Stellung		Offen-Stellung
	Endlage	Dichtschließend		Endlage	Dichtschließend	
Sicherheitsfunktion:	1789	1080	1789	1789	1080	1789
Freisetzung nach außen	158	158	158	158	158	158
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ_{DU} (Gefahrbringend nicht erkannt):	304	1013	186	228	937	110
λ_{DD} (Gefahrbringend erkannt):	0	0	0	76	76	76
λ_{SU} (Sicher nicht erkannt):	0	0	118	0	0	1
λ_{SD} (Sicher erkannt):	0	0	0	0	0	117
PTC (Proof Test-Deckungsgrad):	38 %	11 %	61 %	17 %	4 %	35 %
MTTFd (Mittlere Zeit bis zum gefährlichen Ausfall):	376	113	614	-	-	-
MTTF Sicherheitsfunktion (Mittlere Zeit bis zum Ausfall):	321	97	321	321	97	321
MTTF Gesamtprodukt (Mittlere Zeit bis zum Ausfall):	66	66	66	66	66	66
MTTF D in a (Mittlere Zeit bis zum Ausfall):	321	97	631	321	97	631

1) Diese SIL-Einstufung bedeutet ausschließlich, dass die berechneten Werte innerhalb des Bereichs für hardwarebezogene architektonische Einschränkungen für den entsprechenden SIL liegen.

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate (SSI=2):

	Ausfallraten Severe Service*** (in FIT**)					
	Ohne externen Test			Mit externem Test		
	Geschlossen-Stellung		Offen-Stellung	Geschlossen-Stellung		Offen-Stellung
	Endlage	Dichtschließend		Endlage	Dichtschließend	
Sicherheitsfunktion:	2261	1080	2261	2261	1080	2261
Freisetzung nach außen	280	280	280	280	280	280
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ_{DU} (Gefahrbringend nicht erkannt):	512	1693	276	414	1595	178
λ_{DD} (Gefahrbringend erkannt):	0	0	0	98	98	98
λ_{SU} (Sicher nicht erkannt):	0	0	236	0	0	2
λ_{SD} (Sicher erkannt):	0	0	0	0	0	234
PTC (Proof Test-Deckungsgrad):	29 %	9 %	53 %	12 %	3 %	28 %
MTTF Sicherheitsfunktion (Mittlere Zeit bis zum Ausfall):	168	49	168	168	49	168
MTTF Gesamtprodukt (Mittlere Zeit bis zum Ausfall):	38	38	38	38	38	38
MTTF D in a (Mittlere Zeit bis zum Ausfall):	168	49	345	168	49	345

1) Diese SIL-Einstufung bedeutet ausschließlich, dass die berechneten Werte innerhalb des Bereichs für hardwarebezogene architektonische Einschränkungen für den entsprechenden SIL liegen.

Da die Ausfallraten für die Freisetzung nach außen eine Teilmenge der Ausfallraten ohne Wirkung sind, entspricht die Gesamtausfallrate ohne Wirkung der Summe der aufgelisteten Ausfallraten ohne Wirkung und der Freisetzungen nach außen. Die Ausfallraten mit Freisetzung nach außen finden keinen direkten Eingang in die Zuverlässigkeit des Geräts, sie sollten jedoch im Hinblick auf sekundäre Sicherheits- und Umweltaspekte geprüft werden.

* Clean Service = ohne Schleifpartikel

** FIT = Failure In Time – Ausfallrate ($1x10^{-9}$ Ausfälle pro Stunde)

*** Severe Service = mit Schleifpartikeln

Contents

1 General information

The safety manual contains information and safety notes which apply to the use of the butterfly valve in safety-related applications.

The safety manual only applies in connection with the respective installation, operating and maintenance instructions.

Designation	Item number
ba_R470_de_gb	88740803

1.1 Definition of terms

Automatic Diagnostics

Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.

Tight Shut-Off

State where the product is closed and sealed with leakage no greater than the defined leakage rate. Tight Shut-Off requirements shall be specified according to the application. If Shut-Off requirements allow a flow greater than ANSI class V or ANSI class IV, then the end position numbers may be used.

Dynamic Applications

The movement interval of the final element device is less than 200 hours. Movement may be accomplished by a partial opening test, proof testing or a demand on the system.

Element

A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.

exida criteria

A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.

Fault tolerance

Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).

External Leakage

Failure that causes process media to leak outside of the product; External Leakage is not considered part of the fail safe function. External Leakage failure rates do not directly contribute to the reliability of a product but should be reviewed for secondary safety and environmental issues.

Fail Dangerous

A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:

- Prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state, or
- Decreases the probability that the safety function operates correctly when required.

Dangerous Detected

Failure that is dangerous but is detected by external testing.

Dangerous Undetected

Failure that is dangerous and that is not being diagnosed.

Device

A device is something that is part of an element; but, cannot perform an element safety function on its own.

No effect

Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.

PVST

"Partial Valve Stroke Test" – partial opening test: It is assumed that the partial opening test, when carried out, is automatically carried out at least an order of magnitude more frequently than the proof test. Therefore, the test can be assumed to constitute automatic diagnostics. Because of the automatic diagnostics assumption, the partial opening test also has an impact on the Safe Failure Fraction.

Severe Service

Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.

Fail safe

A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:

- Results in the spurious operation of the safety function to put the EUC (Equipment Under Control) (or part thereof) into a safe state or maintain a safe state, or
- Increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

Static Applications

The movement interval of the final element device is greater than 200 hours. Movement may be accomplished by a partial opening test, proof testing or a demand on the system.

Partial opening test

It is assumed that the partial opening test, when carried out, is carried out at least an order of magnitude more frequently than the proof test. Therefore, the test can be assumed to constitute automatic diagnostics. Because of the automatic diagnostic assumption, the partial opening test also has an impact on the Safe Failure Fraction.

Type A element

"Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2

1.2 Abbreviations

FIT

Failure in Time: Failure rate ($1x10^{-9}$ failures per hour)

FMEDA

"Failure Modes, Effects, and Diagnostic Analysis"

HFT

"Hardware Fault Tolerance"

MTTFd

"Mean Time To Dangerous Failure": Mean time until dangerous failure in years

PVST

"Partial Valve Stroke Test": Partial opening test

SIF

"Safety Instrumented Function"

SIL

"Safety Integrity Level"

SIS

"Safety Instrumented System": Implementation of one or several Safety Instrumented Functions. An SIS comprises any combination of sensor(s), logic solver(s) and final element(s).

SSI

"Site Safety Index"

2 Standards / Literature used

The services delivered by the testing organization exida were carried out based on the following standards/literature:

IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems
Component Reliability Database Handbook, fifth edition, 2021, Vol. 2	exida LLC, Component Reliability Database Handbook, fifth edition, 2021, Vol. 2 – Electrical Components ISBN 978-1-934877-09-5
Component Reliability Database Handbook, fifth edition, 2021, Vol. 3	exida LLC, Component Reliability Database Handbook, fifth edition, 2021, Vol. 3 – Electrical Sensor Components ISBN 978-1-934977-22-4
Goble, W.M., 2010	Control Systems Safety Evaluation and Reliability, third edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions
O'Brien, C., Stewart, L., & Bredemeyer, L., 2018	Exida LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, 2018, ISBN 978-1-934977-18-7
Scaling the Three Barriers, recorded webinar, June 2013	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
Meeting Architecture Constraints in SIF Design, recorded webinar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
Random versus Systematic – Issues and Solutions, September 2016	https://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
Bukowski, J.V. and Stewart, L.L., April 2016	Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York

Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	Exida White Paper, Sellersville, PA www.exida.com
Goble, W.M. and Brombacher, A.C., November 1999, Vol. 66, No. 2	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
ISO 13849-1:2016	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

3 Description

The GEMÜ R470 Tugela double-eccentric metal butterfly valve has a bare shaft with a top flange in accordance with EN ISO 5211. The butterfly valve is available in nominal sizes DN 50 to 600 and in standardized installation lengths API 609 category A (DIN 3202 K1).

3.1 Safety function

The safety function of the Butterfly Valve is to open on trip, close on trip, or close with a tight shutoff on trip.

3.2 Usage period

Based on general failure data, a usage period of approx. 15 years is expected for the type R470 butterfly valve.

The usage period is a reliability engineering term that describes the operating time interval in which the failure rate of a product is relatively constant. It is not a term that covers product ageing, warranty or other commercial issues.

4 Proof tests to detect undetected dangerous failures

In accordance with Section 7.4.5.2 f) of IEC 61508-2, proof tests must be carried out to detect dangerous failures that are not recognized by automatic diagnostic tests. This means that it must be determined how undetected dangerous failures, which were identified during the analysis of the error types, error effects and error diagnosis, can be detected during the compliance test.

The suggested proof test comprises swinging the associated device into the end position.

Step	Action
1	Bypass the fail safe function and take appropriate measures to prevent false tripping.
2	Interrupt or change the air supply/input to the actuator in order to force the actuator/valve assembly into the fail-safe state, and confirm that the safe state has been achieved within the correct time. Note: This tests for any errors that could prevent the positioning valve and the remaining positioning element from functioning.
3	Check the actuator and the housing for leaks, visible damage or impurities.
4	Restore the original air supply/original input to the actuator, and confirm that the normal operating state has been achieved.
5	Remove the bypass and restore normal operation.

For the test to be effective, the movement of the valve must be confirmed. To confirm the effectiveness of the test, both the valve travel and the swinging speed must be monitored and compared with the expected results in order to validate the test.

5 Failure categories description

In order to judge the failure behaviour of the Butterfly Valve, the following definitions for the failure of the device were considered.

Fail-Safe State:

Valve, end position	State where the valve is closed.
Valve, Tight Shut-Off	State where the valve is closed and sealed with leakage no greater than the defined leak rate. The requirements for Tight Shut-Off must be specified according to the application. If requirements for shut-off allow a flow greater than ANSI class V or ANSI class IV, then values for swinging into the end position may be used.
Valve, open on trip	State where the valve is open.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not react to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Valve	Failure that prevents the valve from moving to the defined fail-safe state within the normal time span.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by external automatic diagnostics, such as a partial opening test.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics, such as a partial opening test.
No Effect	Failure of a component that is part of the fail safe function but that has no effect on the fail safe function.
External Leakage	Failure that causes process fluids, gas, hydraulic fluids or operating media to leak outside of the valve or actuator. External Leakage is not considered part of the fail safe function and therefore this failure rate is not included in any of the values. External Leakage failure rates should be checked for secondary safety and environmental issues.

The failure categories listed above expand on the categories listed in IEC 61508 in order to deliver a complete set of data needed for design optimization.

6 Assumptions

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Butterfly Valve, and propagation of errors is irrelevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the fail safe function (without any reactive effect) is excluded. All components that are part of the fail safe function, including those needed for normal operation, are included in the analysis.
- The stress levels are stated in the exida profile used for the analysis, and are limited by the manufacturer's published classifications.
- Materials are compatible with the environmental and process conditions.
- The device is installed and operated in accordance with the manufacturer's instructions.
- Valves are installed such that the controlled medium will flow through the valve in the direction indicated by the flow arrow, located on the valve body.
- In order to claim diagnostic coverage for the partial opening test, it is automatically carried out at a rate at least ten times faster than the Demand frequency.
- The partial opening test of the Safety Instrumented Function offers a complete cycle test of the solenoid valve/pilot valve. In cases where this does not apply, another method must be used to execute a complete valve cycle during automatic diagnostics so that the PVST numbers can be used.
- The partial opening test of the final element comprises position detection from actuator-mounted position sensors, typical of quarter turn installations.
- The worst-case internal fault detection time is the PVST test interval time.

7 exida profiles

exida profile	1	2	3	4	5	6
Description (electrical)	Installed with housing Air-conditioned	Installed with low voltage Not self-heated	Installed with normal voltage Self-heated	Deep sea	Open sea	Not available
Description (mechanical)	Installed with housing Air-conditioned	Installed with normal voltage	Installed with normal voltage	Deep sea	Open sea	In contact with the process
IEC 60654-1 profile	B2	C3 Can also be used for D1	C3 Can also be used for D1	Not available	C3 Can also be used for D1	Not available
Average ambient temperature	30 °C	25 °C	25 °C	5 °C	25 °C	25 °C
Average internal temperature	60 °C	30 °C	45 °C	5 °C	45 °C	Temperature of operating fluid
Daily temperature fluctuation (maximum to maximum)	5 °C	25 °C	25 °C	0 °C	25 °C	Not available
Seasonal temperature difference (winter average compared to summer average)	5 °C	40 °C	40 °C	2 °C	40 °C	Not available
Exposed to elements or the weather	No	Yes	Yes	Yes	Yes	Yes
Humidity [1)]	0–95% Non-condensing	0–100% Condensing	0–100% Condensing	0–100% Condensing	0–100% Condensing	Not available
Impact [2)]	10 g	15 g	15 g	15 g	15 g	Not available
Vibration [3)]	2 g	3 g	3 g	3 g	3 g	Not available
Chemical corrosion [4)]	G2	G3	G3	G3	G3	Compatible material
Surge [5)]						
Line to line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	Not available
Line to earth	1 kV	1 kV	1 kV	1 kV	1 kV	Not available
Susceptibility to EMI [6)]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	Not available
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	Not available
2.0 GHz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	Not available
ESD (air) [7)]	6 kV	6 kV	6 kV	6 kV	6 kV	Not available

1) Humidity class IEC 60068-2-3

2) Impact class IEC 60068-2-6

3) Vibration class IEC 60770-1

4) Chemical corrosion class ISA 71.04

5) Surge class IEC 61000-4-5

6) Susceptibility to EMI class IEC 6100-4-3

7) ESD (air) class IEC 61000-4-2

8 Profiles for the Site Safety Index

The SSI is a number from 0 to 4 that indicates the level of site activities and practices that contribute to the safety performance of the Safety Instrumented Functions at the site. It should be observed that the numbers reflect the levels of SIL assignment, and that SSI 4 means that all requirements of the IEC 61508 and IEC 61511 standards are fulfilled at the site and that there is therefore no impairment of safety performance due to activities or practices of the end user, i.e. that the principal inherent safety performance is achieved.

So far, several factors have been determined that affect the SSI. These include the quality of the following tests:

- Commissioning test
- Proof test procedure
- Documentation of the acceptance test
- Error diagnosis and repair procedures
- Procedure for monitoring the usage duration and for replacement of devices
- SIS modification procedure
- Procedure for decommissioning the SIS
- and others

Level	Description
SSI 3	Almost perfect - Repair work is correctly executed - Tests are carried out correctly and to deadline - The material is generally selected on the basis of the specified environmental limit values and a good analysis of the process chemistry and compatible materials - The electrical power supplies are generally free from overvoltage and are insulated - The pneumatic air supplies and the hydraulic fluids are usually kept clean, etc. - Devices are replaced before the end of their service life, - etc.
SSI 2	Good - Repair work is generally performed correctly - Tests are carried out correctly and usually to deadline - Most devices are replaced before the expiry of their usage period, - etc.
SSI 1	Medium - A lot of repair work is correctly executed - Tests are carried out, usually to deadline - Some devices are replaced before the expiry of their usage period, - etc.
SSI 0	Nothing - Repair work is not always carried out - Tests are not carried out - Devices are only replaced if they are faulty, - etc.

9 SIL failure rate calculation GEMÜ R470 (stationary applications)

SIL failure rate calculation

Functional safety in accordance with IEC 61508 and IEC 61511

We,

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8
74653 Ingelfingen-Criesbach, Germany

declare that, for the product listed below, the failure rates outlined below were detected in safety-related applications in accordance with IEC 61508 and IEC 61511.

The failure rates were determined by means of an FMEDA (Failure Modes, Effects and Diagnostic Analysis) in accordance with IEC 61508. The assessment was carried out by exida.com (report number: GEMÜ 22/07-012 R006).

Product description: GEMÜ R470 Tugela® butterfly valve
Type of valve: A
Fail safe function: The fail safe function of the Butterfly Valve is to open on trip, close on trip, or close with a tight shut-off on trip.
HFT (Hardware Fault Tolerance): 0
MTTR (Mean Time To Restoration): 48 hours

The determined failure rates apply to the operating mode with low demand rate (SSI=2):

	Failure rates Clean Service* (in FIT**)					
	Without external test			With external test		
	Closed position		Open position	Closed position		Open position
	End position	Seals tightly		End position	Seals tightly	
Fail safe function:	1635	986	1635	1635	986	1635
External Leakage	158	158	158	158	158	158
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Dangerous Undetected):	580	1230	462	339	989	221
λ $_{DD}$ (Dangerous Detected):	0	0	0	241	241	241
λ $_{SU}$ (Safe Undetected):	0	0	118	0	0	1
λ $_{SD}$ (Safe Detected):	0	0	0	0	0	117
PTC (Proof Test Coverage):	62 %	29 %	78 %	36 %	12 %	55 %
MTTF fail safe function (Mean Time To Failure):	205	83	206	205	83	206
MTTF full product (Mean Time To Failure):	60	60	60	60	60	60
MTTFd in a (Mean Time To Failure):	205	83	300	205	83	300

1) This SIL classification only means that the calculated values are within the range for hardware-related architectonic limitations for the corresponding SIL.

The determined failure rates apply to the operating mode with low demand rate (SSI=2):

	Failure rates Severe Service*** (in FIT**)					
	Without external test			With external test		
	Closed position		Open position	Closed position		Open position
	End position	Seals tightly		End position	Seals tightly	
Fail safe function:	2107	986	2107	2107	986	2107
External Leakage	279	279	279	279	279	279
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Dangerous Undetected):	865	1987	629	556	1678	320
λ $_{DD}$ (Dangerous Detected):	0	0	0	309	309	309
λ $_{SU}$ (Safe Undetected):	0	0	236	0	0	2
λ $_{SD}$ (Safe Detected):	0	0	0	0	0	234
PTC (Proof Test Coverage):	54 %	23 %	74 %	28 %	9 %	48 %
MTTF fail safe function (Mean Time To Failure):	120	44	120	120	44	120
MTTF full product (Mean Time To Failure):	35	35	35	35	35	35
MTTFd in a (Mean Time To Failure):	120	44	189	120	44	189

1) This SIL classification only means that the calculated values are within the range for hardware-related architectonic limitations for the corresponding SIL.

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure ratesdo not directly contribute to the reliability of the devicebut should be reviewed for secondary safety and environmental issues.

* Clean Service = without abrasive particles

** FIT = Failure In Time ($1x10^{-9}$ failures per hour)

*** Severe Service = with abrasive particles

10 SIL failure rate calculation GEMÜ R470 (dynamic applications)

SIL failure rate calculation

Functional safety in accordance with IEC 61508 and IEC 61511

We,

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8
74653 Ingelfingen-Criesbach, Germany

declare that, for the product listed below, the failure rates outlined below were detected in safety-related applications in accordance with IEC 61508 and IEC 61511.

The failure rates were determined by means of an FMEDA (Failure Modes, Effects and Diagnostic Analysis) in accordance with IEC 61508. The assessment was carried out by exida.com (report number: GEMÜ 22/07-012 R006).

Product description: GEMÜ R470 Tugela® butterfly valve
Type of valve: A
Fail safe function: The fail safe function of the Butterfly Valve is to open on trip, close on trip, or close with a tight shut-off on trip.
HFT (Hardware Fault Tolerance): 0
MTTR (Mean Time To Restoration): 48 hours

The determined failure rates apply to the operating mode with low demand rate (SSI=2):

	Failure rates Clean Service* (in FIT**)					
	Without external test			With external test		
	Closed position		Open position	Closed position		Open position
	End position	Seals tightly		End position	Seals tightly	
Fail safe function:	1789	1080	1789	1789	1080	1789
External Leakage	158	158	158	158	158	158
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Dangerous Undetected):	304	1013	186	228	937	110
λ $_{DD}$ (Dangerous Detected):	0	0	0	76	76	76
λ $_{SU}$ (Safe Undetected):	0	0	118	0	0	1
λ $_{SD}$ (Safe Detected):	0	0	0	0	0	117
PTC (Proof Test Coverage):	38 %	11 %	61 %	17 %	4 %	35 %
MTTFd (Mean Time To Dangerous Failure):	376	113	614	-	-	-
MTTF fail safe function (Mean Time To Failure):	321	97	321	321	97	321
MTTF full product (Mean Time To Failure):	66	66	66	66	66	66
MTTFd in a (Mean Time To Failure):	321	97	631	321	97	631

1) This SIL classification only means that the calculated values are within the range for hardware-related architectonic limitations for the corresponding SIL.

The determined failure rates apply to the operating mode with low demand rate (SSI=2):

	Failure rates Severe Service*** (in FIT**)					
	Without external test			With external test		
	Closed position		Open position	Closed position		Open position
	End position	Seals tightly		End position	Seals tightly	
Fail safe function:	2261	1080	2261	2261	1080	2261
External Leakage	280	280	280	280	280	280
SIL (Safety Integrity Level): [1)]	2	2	2	2	2	2
λ $_{DU}$ (Dangerous Undetected):	512	1693	276	414	1595	178
λ $_{DD}$ (Dangerous Detected):	0	0	0	98	98	98
λ $_{SU}$ (Safe Undetected):	0	0	236	0	0	2
λ $_{SD}$ (Safe Detected):	0	0	0	0	0	234
PTC (Proof Test Coverage):	29 %	9 %	53 %	12 %	3 %	28 %
MTTF fail safe function (Mean Time To Failure):	168	49	168	168	49	168
MTTF full product (Mean Time To Failure):	38	38	38	38	38	38
MTTFd in a (Mean Time To Failure):	168	49	345	168	49	345

1) This SIL classification only means that the calculated values are within the range for hardware-related architectonic limitations for the corresponding SIL.

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure ratesdo not directly contribute to the reliability of the devicebut should be reviewed for secondary safety and environmental issues.

* Clean Service = without abrasive particles

** FIT = Failure In Time ($1x10^{-9}$ failures per hour)

*** Severe Service = with abrasive particles

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8, 74653 Ingelfingen-Criesbach, Germany
Phone +49 (0) 7940 1230 · info@gemue.de
www.gemu-group.com

Änderungen vorbehalten
Subject to alteration
06.2024