

GEMÜ R480 Victoria

Absperrklappe mit freiem Wellenende

DE

SIL-Sicherheitshandbuch



Weitere Informationen
Webcode: GW-R480



Alle Rechte, wie Urheberrechte oder gewerbliche Schutzrechte, werden ausdrücklich vorbehalten.

Dokument zum künftigen Nachschlagen aufbewahren.

© GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG

06.05.2021

Inhalt

| | |
|---|-----------|
| 1 Allgemeines | 4 |
| 1.1 Begriffsbestimmungen | 4 |
| 1.2 Abkürzungen | 5 |
| 2 Normen / verwendete Literatur | 5 |
| 3 Funktionsbeschreibung | 6 |
| 3.1 Sicherheitsfunktion | 6 |
| 4 Fehlerkategorienbeschreibung | 6 |
| 5 Annahmen | 7 |
| 6 SIL-Herstellererklärung GEMÜ R480 (Stationäre Anwendung) | 8 |
| 7 SIL-Herstellererklärung GEMÜ R480 (Dynamische Anwendung) | 10 |

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_R480_de_gb | 88730584 |

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.

Gerät

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

Dynamische Anwendungen

Das Bewegungsintervall des Endelementgeräts beträgt weniger als 200 Stunden. Die Bewegung kann mittels Teilhubtest, Vollhub-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).

FIT

„Failure in Time“: Ausfallrate (1×10^9 Ausfälle pro Stunde)

FMEDA

„Failure Modes, Effects, and Diagnostic Analysis“: Fehlermöglichkeiten-, Einfluss- und Diagnoseanalyse

HFT

„Hardware Fault Tolerance“: Hardware-Fehlertoleranz

Betrieb mit geringer Beanspruchung

Modus, bei dem das Anforderungsintervall für den Betrieb bei einem sicherheitsbezogenen System größer ist als der Zeitabstand zwischen Proof-Tests.

PFD_{Avg}

„Average Probability of Failure on Demand“: durchschnittliche Ausfallwahrscheinlichkeit bei Anforderung

PVST

Partial Valve Stroke Test –Teilhubtest: Es wird davon ausgegangen, dass der Teilhubtest, sofern durchgeführt, automatisch um mindestens eine Größenordnung häufiger durchge-

führt wird als der Proof-Test; deshalb kann der Test als automatische Diagnose betrachtet werden. Aufgrund der Betrachtung als automatische Diagnose hat der Teilhubtest auch Auswirkungen auf den Anteil sicherer Ausfälle.

Robustheit gegenüber Zufällen

Die SIL-Beschränkung aufgrund der architektonischen Einschränkungen für jedes Element.

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.

SFF

Safe Failure Fraction – Anteil sicherer Ausfälle – fasst den Anteil an Ausfällen zusammen, die zu einem sicheren Zustand führen, sowie den Anteil an Ausfällen, die durch automatische Diagnosemaßnahmen erkannt werden und zu einer definierten Sicherheitsaktion führen.

SIF

„Safety Instrumented Function“: sicherheitstechnische Funktion

SIL

„Safety Integrity Level“: Sicherheitsintegritätslevel

SIS

Safety Instrumented System – Sicherheitsbezogenes System – Umsetzung mindestens einer sicherheitstechnischen Funktion. Ein SIS besteht aus einer beliebigen Kombination von Sensoren, Logiksystemen und Endelementen.

SSI

Site Safety Index – Werksicherheitsindex

Stationäre Anwendungen

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

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

DC

„Diagnostic Coverage“: Der Diagnosedeckungsgrad gefährlicher Ausfälle ($DC = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)

FIT

„Failure in Time“: Ausfallrate (1×10^{-9} Ausfälle pro Stunde)

FMEDA

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

HFT

„Hardware Fault Tolerance“: Hardware-Fehlertoleranz

MTBF

„Mean Time Between Failures“: mittlerer Ausfallabstand

MTTR

„Mean Time To Restoration“: mittlere Reparaturzeit

PFDAvg

„Average Probability of Failure on Demand“: durchschnittliche Ausfallwahrscheinlichkeit bei Anforderung

PVST

„Partial Valve Stroke Test“: Teilhubtest

SFF

„Safe Failure Fraction“: Anteil sicherer Ausfälle

SIF

„Safety Instrumented Function“: sicherheitstechnische Funktion

SIL

„Safety Integrity Level“: Sicherheitsintegritätslevel

TSO

„Tight Shut-Off“: dichte Abschaltung

T [Proof]

Zeitabstand zwischen Proof-Tests

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 |
| Mechanical Component Reliability Handbook, 4. Auflage, 2016 | exida LLC, Electrical & Mechanical Component Reliability Handbook, vierte Auflage, 2016 (Veröffentlichung anstehend, zum Zeitpunkt dieses Berichts nicht öffentlich verfügbar) |
| Safety Equipment Reliability Handbook, 4. Auflage, 2015 | exida LLC, Safety Equipment Reliability Handbook, vierte Auflage, 2015, ISBN 978-1-934977-13-2 |
| Goble, W.M., 2010 | Control Systems Safety Evaluation and Reliability, dritte Auflage, ISA, ISBN 978-1-934394-80-9. 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 IndexTM, 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. |

3 Funktionsbeschreibung

GEMÜ R480 Victoria® ist eine zentrische Absperrklappe mit einer Elastomerabsperrdichtung. Sie ist in den Nennweiten DN 25 bis 600 und in verschiedenen Gehäusevarianten wie Wafer, LUG und U-Form (angeflanscht) verfügbar.

3.1 Sicherheitsfunktion

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

4 Fehlerkategorienbeschreibung

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

Ausfallsicherer Zustand:

Ventil, Vollhub Zustand, in dem das Ventil geschlossen ist.

Ventil, dichte Absperlung 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 Absperlung einen größeren Durchfluss als ANSI-Klasse V bzw. ANSI-Klasse IV zulassen, können die Vollhubwerte 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 Teilhubtest, diagnostiziert wird.

Gefahrbringender erkannter Ausfall Ausfall, der gefährlich ist, aber von automatischer Diagnose, wie z. B. einem Teilhubtest, 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.

5 Annahmen

- Es wird die Worst-Case-Annahme eines Seriensystems getroffen. Daher führt der Ausfall einer Einzelkomponente zum Ausfall der gesamten Absperklappe 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 Teilhubtest zu beanspruchen, wird dieser automatisch mit einer Rate durchgeführt, die mindestens zehnmal schneller ist als die Anforderungshäufigkeit.
- Der Teilhubtest 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.

6 SIL-Herstellererklärung GEMÜ R480 (Stationäre Anwendung)

SIL-Herstellererklärung

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 13/08-046 R003).

Produktbeschreibung: GEMÜ-Absperrklappe R480 Victoria®

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:

| | Ausfallraten Clean Service* (in FIT**) | | | | | |
|--|---|-------------------|----------------|----------------------|-------------------|----------------|
| | Ohne externen Test | | | Mit externem Test | | |
| | Geschlossen-Stellung | | Offen-Stellung | Geschlossen-Stellung | | Offen-Stellung |
| | Vollhub | Dichtschlie- ßend | | Vollhub | Dichtschlie- ßend | |
| Sicherheitsfunktion: | 901 | 76 | 901 | 901 | 76 | 901 |
| Freisetzung nach außen | 436 | 436 | 436 | 436 | 436 | 436 |
| SIL (Safety Integrity Level): | 2 | 2 | 2 | 2 | 2 | 2 |
| λ_{DU} (Gefahrbringend nicht erkannt): | 556 | 1381 | 381 | 389 | 1214 | 214 |
| λ_{DD} (Gefahrbringend erkannt): | 0 | 0 | 0 | 167 | 167 | 167 |
| λ_{SU} (Sicher nicht erkannt): | 0 | 0 | 174 | 0 | 0 | 2 |
| λ_{SD} (Sicher erkannt): | 0 | 0 | 0 | 0 | 0 | 172 |
| PTC (Proof Test-Deckungsgrad): | 45 % | 18 % | 66 % | 22 % | 7 % | 39 % |

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

| | Ausfallraten Severe Service*** (in FIT**) | | | | | |
|--|--|------------------|----------------|----------------------|------------------|----------------|
| | Ohne externen Test | | | Mit externem Test | | |
| | Geschlossen-Stellung | | Offen-Stellung | Geschlossen-Stellung | | Offen-Stellung |
| | Vollhub | Dichtschlie-ßend | | Vollhub | Dichtschlie-ßend | |
| Sicherheitsfunktion: | 1727 | 76 | 1727 | 1727 | 76 | 1727 |
| Freisetzung nach außen | 544 | 544 | 544 | 544 | 544 | 544 |
| SIL (Safety Integrity Level): | 2 | 2 | 2 | 2 | 2 | 2 |
| λ_{DU} (Gefahrbringend nicht erkannt): | 953 | 2604 | 605 | 677 | 2328 | 329 |
| λ_{DD} (Gefahrbringend erkannt): | 0 | 0 | 0 | 276 | 276 | 276 |
| λ_{SU} (Sicher nicht erkannt): | 0 | 0 | 349 | 0 | 0 | 3 |
| λ_{SD} (Sicher erkannt): | 0 | 0 | 0 | 0 | 0 | 346 |
| PTC (Proof Test-Deckungsgrad): | 43 % | 16 % | 68 % | 20 % | 6 % | 42 % |

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 (1×10^9 Ausfälle pro Stunde)

*** Severe Service = mit Schleifpartikeln



ppa. Joachim Brien
Leiter Bereich Technik
Ingelfingen-Criesbach,

7 SIL-Herstellererklärung GEMÜ R480 (Dynamische Anwendung)

SIL-Herstellererklärung

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 13/08-046 R003).

Produktbeschreibung: GEMÜ-Absperrklappe R480 Victoria®

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:

| | Ausfallraten Clean Service* (in FIT**) | | | | | |
|--|---|-------------------|----------------|----------------------|-------------------|----------------|
| | Ohne externen Test | | | Mit externem Test | | |
| | Geschlossen-Stellung | | Offen-Stellung | Geschlossen-Stellung | | Offen-Stellung |
| | Vollhub | Dichtschlie- ßend | | Vollhub | Dichtschlie- ßend | |
| Sicherheitsfunktion: | 915 | 91 | 915 | 915 | 91 | 915 |
| Freisetzung nach außen | 457 | 457 | 457 | 457 | 457 | 457 |
| SIL (Safety Integrity Level): | 2 | 2 | 2 | 2 | 2 | 2 |
| λ_{DU} (Gefahrbringend nicht erkannt): | 356 | 1179 | 181 | 309 | 1132 | 134 |
| λ_{DD} (Gefahrbringend erkannt): | 0 | 0 | 0 | 47 | 47 | 47 |
| λ_{SU} (Sicher nicht erkannt): | 0 | 0 | 175 | 0 | 0 | 2 |
| λ_{SD} (Sicher erkannt): | 0 | 0 | 0 | 0 | 0 | 173 |
| PTC (Proof Test-Deckungsgrad): | 20 % | 6 % | 39 % | 8 % | 2 % | 17 % |

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

| | Ausfallraten Severe Service*** (in FIT**) | | | | | | |
|--|--|------------------|----------------|----------------------|------------------|----------------|--|
| | Ohne externen Test | | | Mit externem Test | | | |
| | Geschlossen-Stellung | | Offen-Stellung | Geschlossen-Stellung | | Offen-Stellung | |
| | Vollhub | Dichtschlie-ßend | | Vollhub | Dichtschlie-ßend | | |
| Sicherheitsfunktion: | 1739 | 91 | 1739 | 1739 | 91 | 1739 | |
| Freisetzung nach außen | 579 | 579 | 579 | 579 | 579 | 579 | |
| SIL (Safety Integrity Level): | 2 | 2 | 2 | 2 | 2 | 2 | |
| λ_{DU} (Gefahrbringend nicht erkannt): | 680 | 2327 | 331 | 601 | 2248 | 251 | |
| λ_{DD} (Gefahrbringend erkannt): | 0 | 0 | 0 | 79 | 79 | 80 | |
| λ_{SU} (Sicher nicht erkannt): | 0 | 0 | 350 | 0 | 0 | 3 | |
| λ_{SD} (Sicher erkannt): | 0 | 0 | 0 | 0 | 0 | 347 | |
| PTC (Proof Test-Deckungsgrad): | 18 % | 5 % | 36 % | 7 % | 2 % | 16 % | |

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 (1×10^9 Ausfälle pro Stunde)

*** Severe Service = mit Schleifpartikeln



ppa. Joachim Brien
Leiter Bereich Technik
Ingelfingen-Criesbach,



GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Fritz-Müller-Straße 6-8 D-74653 Ingelfingen-Criesbach
Tel. +49 (0)7940 123-0 · info@gemue.de
www.gemu-group.com

Änderungen vorbehalten

05.2021