# GEMÜ 650 BioStar

Pneumatisch betätigtes Membranventil
Pneumatically operated diaphragm valve

DE **SIL-Sicherheitshandbuch**

EN **SIL Safety Manual**

Weitere Informationen
Webcode: GW-650

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


21.02.2022

## *Inhaltsverzeichnis*

# 1 Allgemeine Informationen

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

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

| Bezeichnung | Artikelnummer |
|---|---|
| ba_650_de_gb | 88245896 |

Wenn das Membranventil mit einem Vorsteuer-Magnetventil GEMÜ 032x kombiniert wird, sind auch die folgenden Dokumente zu beachten:

| Bezeichnung | Artikelnummer |
|---|---|
| ba_0322_de_gb | 88660035 |
| ba_0324_de_gb | 88660062 |
| ba_0326_de_gb | 88660095 |
| sh_0322_SIL_de_gb | - |
| sh_0324_SIL_de_gb | - |
| sh_0326_SIL_de_gb | - |

## 1.1 Begriffsbestimmungen

**Fehlersicherer Zustand**

Der ausfallsichere Zustand ist als der Zustand definiert, in dem das Ventil die Sicherheitsfunktion in die Stellung ZU (bei Steuerfunktion 1) oder Stellung AUF (bei Steuerfunktion 2) ausführt.

**Vollhub**

Zustand, in dem das Ventil geschlossen ist.

**Dichte Abschaltung**

Zustand, in dem das Ventil 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 Vollhub verwendet werden.

**Offen-Position**

Zustand, in dem das Ventil geöffnet ist.

**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.

**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 nicht erkannt**

Ein Ausfall, der gefahrbringend ist und nicht diagnostiziert wird.

**Gefahrbringend erkannt**

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

**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.

**Freisetzung nach außen**

Ausfall, der dazu führt, dass Prozessmedien aus dem Ventil 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 Ventils, sie sollten jedoch im Hinblick auf sekundäre Sicherheits- und Umweltaspekte geprüft werden.

**Betrieb mit geringer Beanspruchung**

Betriebsart, in der die Sicherheitsfunktion nur auf Anforderung ausgeführt wird, um das EUC in einen festgelegten sicheren Zustand zu versetzen, und bei der die Häufigkeit der Anforderung nicht größer ist als einmal pro Jahr.

**Teilhubtest**

Es wird davon ausgegangen, dass der Teilhubtest, 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 Teilhubtest auch Auswirkungen auf den Anteil sicherer Ausfälle.

**Anteil sicherer Ausfälle**

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

**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 (1x$10^{-9}$ 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

**$PFD_{AVG}$**

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

**PVST**

„Partial Valve Stroke Test“: Teilhubtest

**SIP**

Sterilization In Place

**SFF**

„Safe Failure Fraction“: Verhältnis sichere Ausfälle zu gefahrbringenden Ausfällen

**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, 3. Auflage, 2012 | exida LLC, Mechanical Component Reliability Handbook, dritte Auflage, 2012, ISBN 978-1-934977-05-7 |
| IEC 60654-1:1993-02, Ausgabe 2 | Leittechnische Einrichtungen für industrielle Prozesse; Umgebungsbedingungen; Teil 1: Klimatische Einflüsse |
| ISA-TR96.05.01-200_; Version B vom Februar 2006 | Entwurf des technischen Berichts „Partial Stroke Testing For Block Valve Actuators in Safety Instrumented Systems Applications“ |
| Final Elements, Chris O’Brien & Lindsey Bredmeyer, 2009 | exida LLC, Final Elements & the IEC 61508 and IEC 61511 Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9 |

## 3 Funktionsbeschreibung

GEMÜ 650 ist ein Membranventil aus Metall mit einem 2/2-Wege-Ventilkörper in T- oder Behälterausführung oder einer Ausführung als Mehrwegeblock. Es ist für den Einbau in Rohrleitungssysteme bestimmt. Das Membranventil GEMÜ 650 kann als Typ-A-Element mit einer Hardware-Fehlertoleranz von 0 betrachtet werden.

### 3.1 Sicherheitsfunktion

Der ausfallsichere Zustand ist als der Zustand definiert, in dem das Ventil die Sicherheitsfunktion in die Stellung ZU (bei Steuerfunktion 1) oder Stellung AUF (bei Steuerfunktion 2) ausführt.

# 4 Beschreibung der Diagnosemöglichkeiten

## 4.1 Teilhubtest (PVST)

Teilhubtest („Part Valve Stroke Testing“, PVST) bezeichnet die Betätigung des Antriebs / Ventils über einen Teil seines gesamten Hubbereichs. Durch diesen kurzen Arbeitshub wird geprüft, dass der Antrieb / das Ventil nicht in der Betriebsstellung festsitzt. Der begrenzte Hub des Antriebs / Ventils soll so kurz sein, dass er den Arbeitsablauf des Systems nicht stört. Der Zweck des PVST besteht darin, eine diagnostische Kontrolle der SIF-Funktion bereitzustellen. Eine mögliche Testanordnung ist in Abbildung 1 dargestellt.

Teilhubtests werden mit einer mindestens zehn mal höheren Rate durchgeführt als der erwarteten Anforderungsrate. Für Sicherheitsfunktionen gemäß SIL 2 muss der Teilhubtest mindestens die Anforderungen von SIL 1 erfüllen.

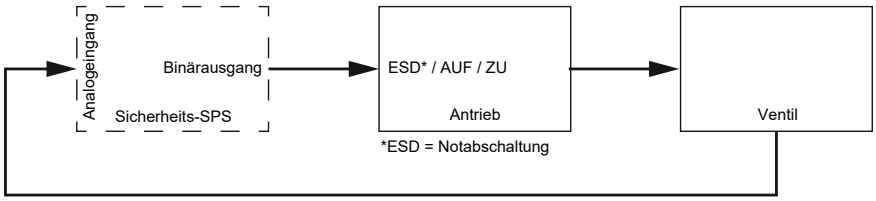


*Abb. 1: Mögliche Testanordnung*

## 4.2 Vollhubtest (FVST)

Vollhubtests („Full Valve Stroke Testing“, FVST) folgen einem ähnlichen Konzept wie der PVST, mit dem Unterschied, dass der Antrieb / das Ventil während des Tests durch seinen vollen Arbeitshub bewegt wird. Dies bietet einen höheren Diagnosedeckungsgrad, kann jedoch üblicherweise nicht während des laufenden Prozesses durchgeführt werden. Es ist ein sehr effektiver Test, der automatisch bei chargenweise arbeitenden Prozessen sowie bei Einrichtungen, die regelmäßig abgeschaltet werden, durchgeführt werden kann.

## 5 Annahmen

- Ausfallraten sind konstant, Verschleißmechanismen sind nicht berücksichtigt.
- Die Ausbreitung von Ausfällen ist nicht relevant.
- Die Geräte sind gemäß den Anweisungen des Herstellers installiert.
- Vor dem Versand werden ausreichende Tests durchgeführt, um sicherzustellen, dass keine Lieferanten- und/oder Herstellungsmängel vorliegen, die eine einwandfreie Arbeitsweise der spezifizierten Funktion gemäß Produktspezifikationen verhindern oder zu einem von der analysierten Auslegung abweichenden Betrieb führen.
- Werkstoffe sind mit Prozessbedingungen und Prozessmedien kompatibel.
- Die mittlere Reparaturzeit (MTTR) nach einem Ausfall beträgt 24 Stunden.
- Für Sicherheitsanwendungen werden nur die beschriebenen Varianten verwendet.
- Alle Komponenten, die nicht Bestandteil der Sicherheitsfunktion sind und keinen Einfluss auf die Sicherheitsfunktion ausüben können, sind ausgeschlossen.
- Ein Bruch oder ein Verschließen von Lufteinlass- und -auslassleitungen wurde nicht in die Analyse einbezogen.
- Saubere und trockene Betriebsluft wird gemäß der Qualitätsnorm für Instrumentenluft ANSI/ISA-7.0.01.1996 verwendet.
- Alle Einrichtungen werden in der Betriebsart mit geringer Beanspruchung betrieben.
- Vollhubtests werden mit einer mindestens einhundert mal höheren Rate durchgeführt als der erwarteten Anforderungsrate.
- Für die Berechnungen in Abschnitt 6.1 (Fehlermöglichkeits-, Einfluss- und Diagnoseanalyse, Bericht Nr. GEMÜ 13/08-046 R002) beträgt die Zeit für die Erkennung eines gefahrbringenden Ausfalls durch den Vollhubtest 730 Stunden.
- Für Sicherheitsfunktionen gemäß SIL x muss der Teilhubtest mindestens die Anforderungen von SIL (x-1) erfüllen. Wenn die Sicherheit beispielsweise SIL 3 erfüllen muss, dann sollte der Teilhubtest mindestens die Anforderungen von SIL 2 erfüllen.
- Durch Wartungsfähigkeiten verursachte Ausfälle sind standortspezifisch und können daher nicht einbezogen werden.
- Vollhubtest (FVST) und Proof-Test umfassen auch eine Ventilsignatur.
- Der Grad der Belastung entspricht Durchschnittswerten für eine Industrieumgebung im Freien und kann mit dem exida-Profil 3 verglichen werden, wobei die Temperaturgrenzwerte innerhalb der Auslegung des Herstellers liegen. Von den übrigen Umweltmerkmalen wird angenommen, dass sie innerhalb der Auslegung des Herstellers liegen.

## 6 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

## 7 Durch die Luftqualität bedingte Ausfälle

Die auf der Konformitätserklärung angegebenen Ausfallraten des Produkts entsprechen einer Situation, in der das Gerät mit sauberer, gefilterter Luft verwendet wird. Eine Kontamination durch schlechte Luftqualität kann die Funktion oder den Luftfluss in dem Gerät beeinträchtigen. Für Anwendungen, bei denen diese Annahmen nicht zutreffen, muss der Anwender die durch verunreinigte Luft bedingten Ausfallraten schätzen und diese Ausfallrate zu den produktbezogenen Ausfallraten addieren.

# 8 SIL-Ausfallratenberechnung GEMÜ 650

**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 (Failure Modes, Effects and Diagnostic Analysis) nach IEC 61508 ermittelt. Die Bewertung wurde durch exida.com durchgeführt (Berichtsnummer: GEMÜ 13/08-046 R003).

| | |
|---|---|
| **Produktbeschreibung:** | Membranventil GEMÜ 650 |
| **Gerätetyp:** | A |
| **Sicherheitsfunktion:** | Durch die Sicherheitsfunktion wird das Membranventil in die Geschlossen-Position (bei Steuerfunktion1) oder Offen-Position (bei Steuerfuktion 2) gebracht. |
| **HFT (Hardware Failure Tolerance):** | 0 |
| **MTTR (Mean time to restoration):** | 24 Stunden |

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

| | Ausfallraten (in FIT*) | | | | | |
|---|---|---|---|---|---|---|
| | ohne externen Test | | | mit externem Test | | |
| | Geschlossen-Position | | Offen-Position | Geschlossen-Position | | Offen-Position |
| | voller Hub | dicht-schließend | | voller Hub | dicht-schließend | |
| **Sicherheitsfunktion:** | 338 | 557 | 322 | 338 | 557 | 322 |
| **SIL** (Safety Integrity Level): [1)] | 2 | 1 | 2 | 2 | 2 | 3 |
| $\lambda_{DU}$ (Dangerous undetected): | 126 | 345 | 66 | 38 | 126 | 20 |
| $\lambda_{DD}$ (Dangerous detected): | 0 | 0 | 0 | 88 | 219 | 46 |
| $\lambda_{SU}$ (Safe undetected): | 212 | 212 | 257 | 212 | 212 | 257 |
| $\lambda_{SD}$ (Safe detected): | 0 | 0 | 0 | 0 | 0 | 0 |
| **SFF** (Safe Failure Fraction): | 62 % | 38 % | 79 % | 88 % | 77 % | 93 % |
| **PTC** (Proof Test Coverage): | 60 % | 22 % | 92 % | 39 % | 12 % | 74 % |
| **MTBF** (Mean Time Between Failures) (in Jahren): | 124 | 124 | 131 | 124 | 124 | 131 |

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

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

# 9 SIL-Ausfallratenberechnung GEMÜ 650 mit GEMÜ 032x

**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 (Failure Modes, Effects and Diagnostic Analysis) nach IEC 61508 ermittelt. Die Bewertung wurde durch exida.com durchgeführt (Berichtsnummer: GEMÜ 13/08-046 R003).

| | |
|---|---|
| **Produktbeschreibung:** | Membranventil GEMÜ 650 mit Vorsteuer-Magnetventil GEMÜ 032x |
| **Gerätetyp:** | A |
| **Sicherheitsfunktion:** | Durch die Sicherheitsfunktion wird das Membranventil in die Geschlossen-Position (bei Steuerfunktion1) oder Offen-Position (bei Steuerfuktion 2) gebracht. |
| **HFT (Hardware Failure Tolerance):** | 0 |
| **MTTR (Mean time to restoration):** | 24 Stunden |

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

| | Ausfallraten (in FIT*) | | | | | |
|---|---|---|---|---|---|---|
| | ohne externen Test | | | mit externem Test | | |
| | Geschlossen-Position | | Offen-Position | Geschlossen-Position | | Offen-Position |
| | voller Hub | dicht-schließend | | voller Hub | dicht-schließend | |
| **Sicherheitsfunktion:** | 487 | 706 | 472 | 487 | 706 | 472 |
| **SIL** (Safety Integrity Level): [1)] | 2 | 1 | 2 | 3 | 2 | 3 |
| $\lambda_{DU}$ (Dangerous undetected): | 165 | 384 | 105 | 39 | 126 | 21 |
| $\lambda_{DD}$ (Dangerous detected): | 0 | 0 | 0 | 126 | 258 | 84 |
| $\lambda_{SU}$ (Safe undetected): | 322 | 322 | 367 | 322 | 322 | 367 |
| $\lambda_{SD}$ (Safe detected): | 0 | 0 | 0 | 0 | 0 | 0 |
| **SFF** (Safe Failure Fraction): | 66 % | 45 % | 77 % | 92 % | 82 % | 95 % |
| **PTC** (Proof Test Coverage): | 69 % | 30 % | 95 % | 39 % | 12 % | 73 % |
| **MTBF** (Mean Time Between Failures) (in Jahren): | 94 | 94 | 98 | 94 | 94 | 98 |

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

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

## *Contents*

# 1 General information

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

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

| Designation | Item number |
|---|---|
| ba_650_de_gb | 88245896 |

When combining the diaphragm valve with a GEMÜ 032x pilot solenoid valve, the following documents must also be observed:

| Designation | Item number |
|---|---|
| ba_0322_de_gb | 88660035 |
| ba_0324_de_gb | 88660062 |
| ba_0326_de_gb | 88660095 |
| sh_0322_SIL_de_gb | - |
| sh_0324_SIL_de_gb | - |
| sh_0326_SIL_de_gb | - |

## 1.1 Definition of terms

**Fail-Safe State**

This fail-safe state is defined as the state where the valve performs the safety function to CLOSE (with control function 1) or to OPEN (with control function 2).

**Full stroke**

State where the valve is closed.

**Tight Shut-Off**

State where the valve is closed and sealed with leakage no greater than the defined leak rate. Tight Shut-Off requirements shall be specified according to the application. If Shut-Off requirements allow flow greater than ANSI class V, respectively ANSI class IV, then Full Stroke numbers may used.

**Open position**

State where the valve is open.

**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.

**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 Undetected**

Failure that is dangerous and that is not being diagnosed.

**Dangerous Detected**

Failure that is dangerous but is detected by external testing.

**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.

**External Leakage**

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

**Low demand mode**

Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.

**Partial Valve Stroke Test**

It is assumed that the Partial Valve Stroke Test, when performed, is performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Test also has an impact on the Safe Failure Fraction.

**Safe Failure Fraction**

Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.

**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

**DC**

Diagnostic Coverage: Diagnostic coverage of dangerous failures (DC = $\lambda_{dd}$ / ($\lambda_{dd}$ + $\lambda_{du}$))

**FIT**

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

**FMEDA**

Failure Modes, Effects and Diagnostic Analysis

**HFT**

Hardware Fault Tolerance

**MTBF**

Mean Time Between Failures

**MTTR**

Mean Time To Restoration

**PFD** $_{AVG}$

Average Probability of Failure on Demand

**PVST**

Partial Valve Stroke Test

**SIP**

Sterilization In Place

**SFF**

Safe Failure Fraction: Ratio of safe failures to dangerous failures

**SIF**

Safety Instrumented Function

**SIL**

Safety Integrity Level

**TSO**

Tight Shut-Off

**T [Proof]**

Proof Test Interval

## 2 Standards / Literature used

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

| | |
|---|---|
| IEC 61508-2:2010 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |
| Mechanical Component Reliability Handbook, 3rd Edition, 2012 | exida LLC, Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7 |
| IEC 60654-1:1993-02, second edition | Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions |
| ISA-TR96.05.01-200_; version B of February 2006 | Draft technical report “Partial Valve Stroke Testing For Block Valve Actuators in Safety Instrumented Systems Applications” |
| Final Elements Chris O’Brien & Lindsey Bredmeyer, 2009 | exida LLC, Final Elements & the IEC 61508 and IEC 61511 Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9 |

## 3 Functional description

GEMÜ 650 is a metal diaphragm valve with a 2/2-way, T or tank bottom valve body or in multi-port block design. It is designed for installation in piping systems. The GEMÜ 650 diaphragm valve can be considered to be a Type A element with a hardware fault tolerance of 0.

### 3.1 Safety function

This fail-safe state is defined as the state where the valve performs the safety function to CLOSE (with control function 1) or to OPEN (with control function 2).

# 4 Description of diagnostic possibilities

## 4.1 Partial Valve Stroke Testing (PVST)

Partial Valve Stroke Testing (PVST) is the operation of the actuator/valve through a portion of its total stroke range. This short stroke of operation checks that the actuator / valve is not seized in the running position. The limited stroke of the actuator / valve is intended to be short enough so as not to interfere with the operating flow of the system. The purpose of PVST is to provide a diagnostic check of the SIF function. A possible test set-up is shown in Figure 1.

Partial Valve Stroke Testing is performed at a rate at least ten times faster than the expected demand rate. For SIL 2 safety functions the partial valve stroke test is at least SIL 1 compliant.

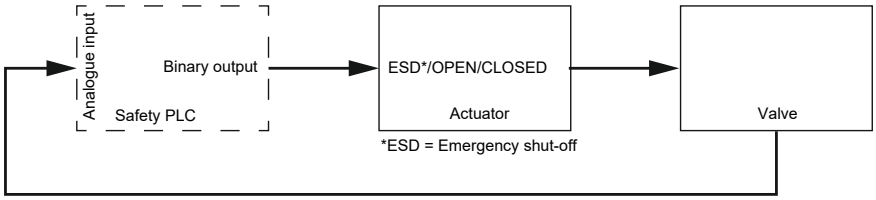


*Fig. 1: Possible test set-up*

## 4.2 Full Valve Stroke Testing (FVST)

Full Valve Stroke Testing (FVST) is similar in concept to a PVST, with the variation that the actuator/valve is moved through its full operation stroke during the test. This provides greater diagnostic coverage but typically cannot be performed while the process is running. It is a very effective test that can be automatically executed on batch processes and equipment that periodically shuts down.

## 5 Assumptions

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The devices are installed per the manufacturer's instructions.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions and process fluids.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- Only the described versions are used for safety applications.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- Clean and dry operating air is used in accordance with ANSI/ISA-7.0.01.1996 Quality Standard for Instrument Air.
- All devices are operated in low-demand mode.
- Full Valve Stroke Testing is performed at a rate at least one hundred times faster than the expected demand rate.
- For the calculations in Section 6.1 (Failure Modes, Effects and Diagnostic Analysis, report no. GEMÜ 13/08-046 R002), the time to detect a dangerous failure by full valve stroke testing is 730 hours.
- For SIL x safety functions the partial valve stroke test is at least SIL (x-1) compliant. If for example the safety needs to fulfil SIL 3 then the Partial Valve Stroke Test should be at least SIL 2 compliant.
- Failures caused by maintenance capability are site specific and therefore cannot be included.
- FVST and proof testing include a valve signature.
- The stress levels are average for an industrial outdoor environment and can be compared to exida Profile 3 with temperature limits within the manufacturer‘s rating. Other environmental characteristics are assumed to be within the manufacturer‘s ratings.

## 6 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

## 7 Air quality failures

The product failure rates that are specified on the declaration of conformity are failure rates that reflect the situation where the device is used with clean filtered air. Additionally, contamination from poor control air quality may affect the function or air flow in the device. For applications where these assumptions do not apply, the user must estimate the failure rates due to contaminated air and add this failure rate to the product failure rates.

# 8 SIL failure rate calculation GEMÜ 650

## 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 calculated by means of an FMEDA (Failure Modes, Effects and Diagnostic Analysis) in accordance with IEC 61508. The evaluation was performed by exida.com (report number: GEMÜ 13/08-046 R003).

| | |
|---|---|
| **Product description:** | GEMÜ diaphragm valve 650 |
| **Type of valve:** | A |
| **Safety function:** | Due to the safety function, the diaphragm valve is placed in the closed position (with control function 1) or in the open position (with control function 2). |
| **HFT (Hardware Fault Tolerance):** | 0 |
| **MTTR (Mean Time To Restoration):** | 24 hours |

The determined failure rates apply to the operating mode with low demand rate:

| | Failure rates (in FIT*) | | | | | |
|---|---|---|---|---|---|---|
| | Without external test | | | With external test | | |
| | Closed position | | Open position | Closed position | | Open position |
| | Full stroke | Tightly sealed | | Full stroke | Tightly sealed | |
| **Safety function:** | 338 | 557 | 322 | 338 | 557 | 322 |
| **SIL** (Safety Integrity Level): [1)] | 2 | 1 | 2 | 2 | 2 | 3 |
| $\lambda_{DU}$ (Dangerous undetected): | 126 | 345 | 66 | 38 | 126 | 20 |
| $\lambda_{DD}$ (Dangerous detected): | 0 | 0 | 0 | 88 | 219 | 46 |
| $\lambda_{SU}$ (Safe undetected): | 212 | 212 | 257 | 212 | 212 | 257 |
| $\lambda_{SD}$ (Safe detected): | 0 | 0 | 0 | 0 | 0 | 0 |
| **SFF** (Safe Failure Fraction): | 62% | 38% | 79% | 88% | 77% | 93% |
| **PTC** (Proof Test Coverage): | 60% | 22% | 92% | 39% | 12% | 74% |
| **MTBF** (Mean Time Between Failures) (in years): | 124 | 124 | 131 | 124 | 124 | 131 |

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

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

# 9 SIL failure rate calculation GEMÜ 650 with GEMÜ 032x

## 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 calculated by means of an FMEDA (Failure Modes, Effects and Diagnostic Analysis) in accordance with IEC 61508. The evaluation was performed by exida.com (report number: GEMÜ 13/08-046 R003).

| | |
|---|---|
| **Product description:** | GEMÜ 650 diaphragm valve with GEMÜ 032x pilot solenoid valve |
| **Type of valve:** | A |
| **Safety function:** | Due to the safety function, the diaphragm valve is placed in the closed position (with control function 1) or in the open position (with control function 2). |
| **HFT (Hardware Fault Tolerance):** | 0 |
| **MTTR (Mean Time To Restoration):** | 24 hours |

The determined failure rates apply to the operating mode with low demand rate:

| | Failure rates (in FIT*) | | | | | |
|---|---|---|---|---|---|---|
| | Without external test | | | With external test | | |
| | Closed position | | Open position | Closed position | | Open position |
| | Full stroke | Tightly sealed | | Full stroke | Tightly sealed | |
| **Safety function:** | 487 | 706 | 472 | 487 | 706 | 472 |
| **SIL** (Safety Integrity Level): [1)] | 2 | 1 | 2 | 3 | 2 | 3 |
| $\lambda_{DU}$ (Dangerous undetected): | 165 | 384 | 105 | 39 | 126 | 21 |
| $\lambda_{DD}$ (Dangerous detected): | 0 | 0 | 0 | 126 | 258 | 84 |
| $\lambda_{SU}$ (Safe undetected): | 322 | 322 | 367 | 322 | 322 | 367 |
| $\lambda_{SD}$ (Safe detected): | 0 | 0 | 0 | 0 | 0 | 0 |
| **SFF** (Safe Failure Fraction): | 66% | 45% | 77% | 92% | 82% | 95% |
| **PTC** (Proof Test Coverage): | 69% | 30% | 95% | 39% | 12% | 73% |
| **MTBF** (Mean Time Between Failures) (in years): | 94 | 94 | 98 | 94 | 94 | 98 |

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

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

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
02.2022