

GEMÜ 0322

Elektrisch betätigtes Vorsteuer-Magnetventil
Electrically operated pilot solenoid valve

DE **SIL-Sicherheitshandbuch**

EN **SIL Safety Manual**



Alle Rechte, wie Urheberrechte oder gewerbliche Schutzrechte, werden ausdrücklich vorbehalten.
All rights including copyrights or industrial property rights are expressly reserved.

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

© GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
21.02.2022

Inhaltsverzeichnis

1	Allgemeine Informationen	4
1.1	Begriffsbestimmungen	4
1.2	Abkürzungen	5
2	Normen / verwendete Literatur	5
3	Funktionsbeschreibung	5
3.1	Sicherheitsfunktion	5
4	Beschreibung der Diagnosemöglichkeiten	6
4.1	Teilhubtest (PVST)	6
4.2	Vollhubtest (FVST)	6
5	Annahmen	7
6	exida-Profile	8
7	Durch die Luftqualität bedingte Ausfälle	9
8	SIL-Ausfallratenberechnung GEMÜ 0322	10

1 Allgemeine Informationen

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

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

Bezeichnung	Artikelnummer
ba_0322_de_gb	88660035

1.1 Begriffsbestimmungen

Ausfallsicherer Zustand

Der ausfallsichere Zustand ist als der Zustand definiert, in dem das Magnetventil stromlos ist und das Ventil in die Stellung ZU zurückkehrt (stromlos geschlossen, DTT). Bei GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG wird diese Konfiguration als „Schaltstellung a1“ bezeichnet.

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 ($DC = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)

DTT

„De-energize To Trip“: stromlos geschlossen

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

PFD_{AVG}

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

PVST

„Partial Valve Stroke Test“: Teilhubtest

SFF

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

SIF

„Safety Instrumented Function“: sicherheitstechnische Funktion

SIL

„Safety Integrity Level“: Sicherheitsintegritätslevel

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 0322 ist ein 3/2-Wege-Vorsteuer-Magnetventil. GEMÜ 0322 ist für die Einzelmontage (in Durchgangsform) oder für modulare Batteriemontage (mittels Klammern) von bis zu 12 Ventilen bestimmt.

3.1 Sicherheitsfunktion

Der ausfallsichere Zustand ist als der Zustand definiert, in dem das Magnetventil stromlos ist und das Ventil in die Stellung ZU zurückkehrt (stromlos geschlossen).

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 fest-sitzt. 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.

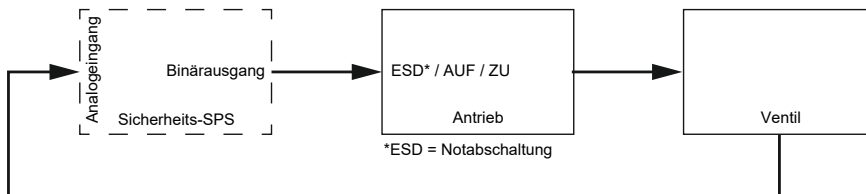


Abb. 1: Mögliche Testanordnung

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.
- Das System ist gemäß den Anweisungen des Herstellers eingebaut.
- 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.
- Für Anwendungen wird nur „Schaltstellung a1“ 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.
- 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 Temperatureauslenkung (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 0322**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 R002).

Produktbeschreibung:	3/2-Wege Vorsteuer-Magnetventil GEMÜ 0322
Gerätetyp:	A
Sicherheitsfunktion:	Durch die Sicherheitsfunktion wird das Ventil in die Geschlossen-Position gebracht. Hierzu wird das Magnetventil stromlos geschlossen (Schaltstellung a1).
HFT (Hardware Failure Tolerance):	0
MTTR (Mean time to restoration):	24 Stunden

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

	Ausfallraten Vorsteuer-Magnetventil ohne Prozessventil (in FIT*)		Ausfallraten Vorsteuer-Magnetventil auf Prozessventil montiert (in FIT*)	
	ohne externen Test	mit externem Test	ohne externen Test	mit externem Test
Sicherheitsfunktion:	239	239	149	149
SIL (Safety Integrity Level): ¹⁾	1	2	-	-
λ_{DU} (Dangerous undetected):	129	36	39,4	0,4
λ_{DD} (Dangerous detected):	0	93	0	39
λ_{SU} (Safe undetected):	110	110	110	110
λ_{SD} (Safe detected):	0	0	0	0
SFF (Safe Failure Fraction):	45 %	84 %	-	-
PTC (Proof Test Coverage):	93 %	74 %	99 %	0 %
MTBF (Mean Time Between Failures) (in Jahren):	396	396	396	396

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 (1×10^{-9} Ausfälle pro Stunde)

Contents

1	General information	12
1.1	Definition of terms	12
1.2	Abbreviations	13
2	Standards / Literature used	13
3	Functional description	13
3.1	Safety function	13
4	Description of diagnostic possibilities	14
4.1	Partial Valve Stroke Testing (PVST)	14
4.2	Full Valve Stroke Testing (FVST)	14
5	Assumptions	15
6	exida profiles	16
7	Air quality failures	17
8	SIL failure rate calculation GEMÜ 0322	18

1 General information

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

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

Designation	Item number
ba_0322_de_gb	88660035

1.1 Definition of terms

Fail-Safe State

The fail-safe state is defined as the state where the solenoid valve is de-energized and the valve is returned to the CLOSED position (de-energized, DTT). At GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG this configuration is called "switch position a1".

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 ($DC = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)

DTT

"De-energize To Trip": Normally closed

FIT

Failure in Time: Failure rate (1×10^{-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

SFF

Safe Failure Fraction: Ratio of safe failures to dangerous failures

SIF

Safety Instrumented Function

SIL

Safety Integrity Level

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 0322 is a 3/2-way pilot solenoid valve. GEMÜ 0322 is designed for single mounting (straight through design) or for modular battery mounting of up to 12 valves (by using clips).

3.1 Safety function

The fail-safe state is defined as the state where the solenoid valve is de-energized and the valve is returned to the CLOSED position (de-energized).

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.

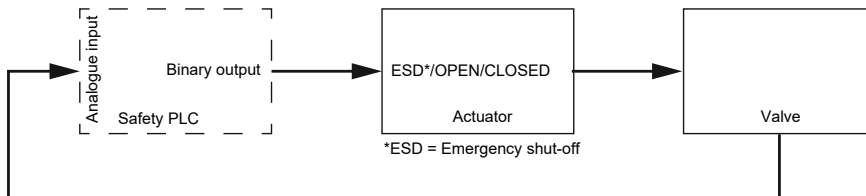


Fig. 1: Possible test set-up

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 system is 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 variants are used for safety applications.
- Only "switch position a1" is used for 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 per ANSI/ISA-7.0.01.1996 Quality Standard for Instrument Air.
- All devices are operated in the low demand mode of operation.
- 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 must be at least SIL (x-1) compliant. If, for example, the safety needs to fulfil SIL 3, 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.
- 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 0322**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 R002).

Product description: 3/2-way pilot solenoid valve GEMÜ 0322
Device type: A
Safety function: Due to the safety function, the valve is placed in the closed position. For this, the solenoid valve is closed when de-energized (switch position a1).
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 pilot solenoid valve without process valve (in FIT*)		Failure rates pilot solenoid valve mounted on process valve (in FIT*)	
	Without external test	With external test	Without external test	With external test
Safety function:	239	239	149	149
SIL (Safety Integrity Level): ¹⁾	1	2	-	-
λ_{DU} (Dangerous undetected):	129	36	39.4	0.4
λ_{DD} (Dangerous detected):	0	93	0	39
λ_{SU} (Safe undetected):	110	110	110	110
λ_{SD} (Safe detected):	0	0	0	0
SFF (Safe Failure Fraction):	45 %	84 %	-	-
PTC (Proof Test Coverage):	93 %	74 %	99 %	0 %
MTBF (Mean Time Between Failures) (in years):	396	396	396	396

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 (1×10^{-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