

GEMÜ BB02/BB06/BB07/BB0F/BB0M/B20

Schwimmend gelagerte Kugelhähne
Floating ball valves

DE SIL-Sicherheitshandbuch

EN SIL Safety Manual



Weitere Informationen
Webcode: GW-BB02/BB06/
BB07/BB0F/BB0M/B20



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
10.11.2023

Inhaltsverzeichnis

1	Allgemeine Informationen	4
1.1	Begriffsbestimmungen	4
1.2	Abkürzungen	5
2	Normen / verwendete Literatur	6
3	Funktionsbeschreibung	6
4	Proof-Test	6
4.1	Ohne automatischen Test	6
4.2	Mit automatischem Teilöffnungstest	6
5	Annahmen	6
6	Nutzungsdauer	6
7	SIL-Ausfallratenberechnung schwimmend gela- gerte Kugelhähne (BB02/BB06/BB07/BB0F/ BB0M/B20)	7

1 Allgemeine Informationen

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

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

Bezeichnung	Artikelnummer
ba_BB02_de_gb	88714595
ba_BB06_de_gb	88711005
ba_BB07_de_gb	88810263
ba_BB0F_de_gb	88884856
ba_BB0M_de_gb	88884854
ba_B20_de_gb	88675667

Das Sicherheitsintegritätsniveau (SIL) der gesamten sicherheitsgerichteten Funktion (SIF) muss durch eine Berechnung der PFD_{AVG} unter Berücksichtigung der redundanten Architekturen, des Proof-Test-Intervalls, der Proof-Test-Effektivität, jeglicher automatischer Diagnose, der durchschnittlichen Reparaturzeit und der spezifischen Ausfallraten aller in der SIF enthaltenen Produkte überprüft werden. Jedes Teilsystem muss geprüft werden, um die Einhaltung der Mindestanforderungen an die Hardware-Fehlertoleranz (HFT) zu gewährleisten.

Bei der Verwendung des Produkts in einer redundanten Konfiguration sollte ein Faktor für gemeinsame Ursachen von mindestens 10 % in die Berechnungen der Sicherheitsintegrität einbezogen werden.

1.1 Begriffsbestimmungen

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.

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.

Betrieb mit hoher Beanspruchung oder Dauerbetrieb

Betriebsart, in der die Sicherheitsfunktion kontinuierlich oder diskontinuierlich ausgeführt wird und bei der die Häufigkeit der Anforderung größer ist als einmal pro Jahr.

Endlage

Zustand, in dem das Produkt geschlossen ist.

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.

Grundlegende Sicherheit

Das Produkt muss so konstruiert und gefertigt sein, dass es vor Schäden durch elektrischen Schlag und andere Gefahren sowie vor daraus resultierenden Bränden und Explosionen schützt.

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.

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

Sicherheit

Freiheit von einem unannehmbaren Schadensrisiko.

Sicherheitsfunktion

Die Fähigkeit eines Systems, die notwendigen Aktionen auszuführen, um einen definierten sicheren Zustand für das Produkt unter der Kontrolle des Systems zu erreichen oder zu erhalten.

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.

β

Ausfallfaktor gemeinsamer Ursache für nicht erkennbare gefahrbringende Ausfälle. Der Ausfallfaktor ist gleich dem gesamten β -Faktor, der ohne Diagnosetests gelten würde

β_D

Ausfallfaktor gemeinsamer Ursache für erkennbare gefahrbringende Ausfälle.

λ_{DD}

Kumulative Ausfallrate in Bezug auf gefahrbringend erkannte Ausfallarten.

"Dangerous detected" (DD): Gefahrbringend erkannt

$\lambda_{DD,PST}$

Kumulative Ausfallrate in Bezug auf gefahrbringende Ausfallarten, die durch Teilöffnungstest mit Diagnosemerkmalen gemäß der Auslegung der IEC EN 61508 festgestellt werden können.

"Dangerous detected" (DD): Gefahrbringend erkannt

"Partial Stroke Test" (PST): Teilöffnungstest

λ_{DU}

Kumulative Ausfallrate in Bezug auf gefahrbringende Ausfallarten, die nur mit Hilfe von vollständigen Proof Tests festgestellt werden können.

"Dangerous undetected" (DU): Gefahrbringend nicht erkannt

$\lambda_{DU,FPT}$

Kumulative Ausfallrate in Bezug auf gefahrbringende Ausfallarten, die durch einen vollständigen Proof-Test mit Diagnosemerkmalen gemäß der Auslegung der IEC EN 61508 festgestellt werden können.

"Dangerous undetected" (DU): Gefahrbringend nicht erkannt

"Full Proof Test" (FPT): Vollständiger Proof-Test

λ_{NE}

Kumulative Ausfallrate in Bezug auf Ausfallarten ohne Wirkung auf die Sicherheitsfunktion.

"No effect" (NE): Ohne Wirkung

θ_{FPT}

Zeitintervall zwischen zwei aufeinanderfolgenden vollständigen Proof Tests in Stunden.

"Full Proof Test" (FPT): Vollständiger Proof-Test

θ_{PST}

Zeitintervall zwischen zwei aufeinanderfolgenden Teilöffnungstests in Stunden.

"Partial Stroke Test" (PST): Teilöffnungstest

1.2 Abkürzungen

E/E/EP

"Electrical, Electronic, Programmable Electronic": Elektrisch, Elektronisch, Programmierbare Elektronik

FMEDA

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

HFT

"Hardware Fault Tolerance": Hardware-Fehlertoleranz

MRT

"Mean Repair Time": Mittlere Reparaturdauer

MTTR

"Mean Time To Restoration": mittlere Reparaturzeit

PFDAVG

"Average Probability of Failure on Demand": durchschnittliche Ausfallwahrscheinlichkeit bei Anforderung

SFF

"Safe Failure Fraction": Verhältnis sichere Ausfälle zu gefahrbringenden Ausfällen

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).

2 Normen / verwendete Literatur

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

IEC EN 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme
---------------------	---

3 Funktionsbeschreibung

Die schwimmend gelagerten Kugelhähne aus Edelstahl verfügen über ein freies Wellenende. Dank dem Kopfflansch nach ISO 5211 ist eine einfache Antriebsmontage möglich.

4 Proof-Test

4.1 Ohne automatischen Test

Das Ziel der Proof-Tests ist die Erkennung von Fehlern innerhalb des Ventils, die nicht durch eine automatische Diagnose des Systems erkannt werden. Das Hauptaugenmerk liegt auf unerkannten Fehlern, die verhindern, dass die sicherheitsgerichtete Funktion ihre vorgesehene Funktion erfüllt.

Die Häufigkeit der Proof-Tests, oder das Proof-Test-Intervall, muss in den Zuverlässigkeitsberechnungen für die Sicherheitsfunktionen bestimmt werden.

Der Umfang der Proof-Tests für das Produkt ist im FMEDA-Bericht aufgeführt.

Personen, die den Proof-Test durchführen, sollten im SIS-Betrieb, einschließlich Bypass-Verfahren, Ventilwartung und unternehmensrelevanten Verfahren geschult sein.

4.2 Mit automatischem Teilöffnungstest

Ein automatisches Prüfprogramm, das den gesamten Hub des Produkts prüft und das Timing der Ventilbewegung misst, erkennt die meisten potenziell gefahrbringenden Ausfallarten.

Es wird empfohlen, eine physikalische Prüfung in regelmäßigen Abständen durchzuführen, wobei das Zeitintervall von den Anlagenbedingungen abhängt. Es wird ein maximales Inspektionsintervall von drei Jahren empfohlen.

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.

- 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.
- Endlagentests werden mit einer mindestens einhundert mal höheren Rate durchgeführt als der erwarteten Anforderungsrate.
- Für Sicherheitsfunktionen gemäß SIL x muss der Teilöffnungstest mindestens die Anforderungen von SIL (x-1) erfüllen. Wenn die Sicherheit beispielsweise SIL 3 erfüllen muss, dann sollte der Teilöffnungstest mindestens die Anforderungen von SIL 2 erfüllen.
- Durch Wartungsfähigkeiten verursachte Ausfälle sind standortspezifisch und können daher nicht einbezogen werden.

6 Nutzungsdauer

Die normale Lebensdauer des Produkts beträgt 3000 Zyklen.

7 SIL-Ausfallratenberechnung schwimmend gelagerte Kugelhähne (BB02/BB06/BB07/BB0F/BB0M/B20)**SIL-Ausfallratenberechnung****Funktionale Sicherheit nach IEC EN 61508:2010**

Wir, die Firma

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

erklären, dass für die unten aufgeführten Produkte in sicherheitsbezogenen Anwendungen gemäß IEC EN 61508 die unten aufgeführten Ausfallraten ermittelt wurden.

Die Ausfallraten wurden durch eine FMEDA (Failure Modes, Effects and Diagnostic Analysis) nach IEC EN 61508 ermittelt. Die Bewertung wurde durch TÜV Italia durchgeführt (Zertifikatsnummer: C-IS-722264081).

Produktbeschreibung: Schwimmend gelagerte Kugelhähne
(BB02/BB06/BB07/BB0F/BB0M/B20)

Gerätetyp: A

Die ermittelten Ausfallraten gelten für die Betriebsart mit niedriger Anforderungsrate:

E/EE/EP Sicherheitsrelevantes System (letztes Element)	Kugelhähne der Serie OM, hergestellt von Zhejiang Ouming Fluid Casting Industry Co, Ltd.	
Systemtyp	Typ A	
Systematische Fähigkeit	SC3	
Definition der Sicherheitsfunktion	SIF1: "Korrektes Schalten bei Bedarf (offen bis geschlossen) und dicht für die Schließphase, bei Betriebsart mit geringem Bedarf"	SIF2: "Korrektes Schalten bei Bedarf (geschlossen zu offen), in der Betriebsart mit geringem Bedarf"
Max SIL⁽¹⁾	SIL3	SIL3
λ_{TOT} (Gesamt)	9,188E-08	9,188E-08
λ_{NE} (Ohne Wirkung)	2,198E-08	3,143E-08
λ_S (Sicherer Ausfall)	0,000E+00	0,000E+00
$\lambda_{DD,PST}^{(2)}$ (Gefahrbringend erkannt mit Teilhubtest)	1,864E-08	4,449E-08
$\lambda_{DU,FPPT}$ (Gefahrbringend nicht erkannt, erkennbar mit periodischem Full Proof test)	5,125E-08	1,596E-08
β and β_D Faktor	10%	10%
MRT	8 Stunden	8 Stunden
Integrität der Hardware-Sicherheit	Strecke 2_H	Strecke 2_H
Systematische Sicherheitsintegrität	Strecke 2_S	Strecke 2_S

Erläuterungen:

⁽¹⁾ Das Sicherheitsintegritätsniveau (SIL) der gesamten sicherheitsgerichteten Funktion (SIF) muss durch eine Berechnung der PFD_{AVG} unter Berücksichtigung der redundanten Architekturen, des Proof-Test-Intervalls, der Proof-Test-Effektivität, jeglicher automatischer Diagnose, der durchschnittlichen Reparaturzeit und der spezifischen Ausfallraten aller in der SIF enthaltenen Produkte überprüft werden. Jedes Teilsystem muss geprüft werden, um die Einhaltung der Mindestanforderungen an die Hardware-Fehlertoleranz (HFT) zu gewährleisten.

⁽²⁾ Berücksichtigung eines automatischen Teilöffnungstest.

Contents

1	General information	9
1.1	Definition of terms	9
1.2	Abbreviations	10
2	Standards / Literature used	10
3	Functional description	10
4	Proof test	10
4.1	Without automatic test	10
4.2	With automatic partial opening test	10
5	Assumptions	10
6	Usage period	11
7	SIL failure rate calculation for floating ball valves (BB02/BB06/BB07/BB0F/BB0M/B20)	12

1 General information

The safety manual contains general information and safety information applying to the use of the ball valves in safety-related applications.

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

Designation	Item number
ba_BB02_de_gb	88714595
ba_BB06_de_gb	88711005
ba_BB07_de_gb	88810263
ba_BB0F_de_gb	88884856
ba_BB0M_de_gb	88884854
ba_B20_de_gb	88675667

The Safety Integrity Level (SIL) of the total Safety Instrumented Function (SIF) must be checked via a calculation of the PFD_{AVG} under consideration of the redundant architectures, the proof test interval, the proof test effectiveness, any automatic diagnostics, the mean repair time and the specific failure rates of all products included in the SIF. Each part system must be tested, in order to ensure compliance with the minimum requirements regarding Hardware Fault Tolerance (HFT).

When using the product in a redundant configuration, a factor of at least 10% for common causes should be included in the calculations of safety integrity.

1.1 Definition of terms

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.

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.

High demand mode or continuous operation

Operating mode in which the fail safe function is continuously or discontinuously performed and at which the frequency of the requirement is greater than once a year.

End position

Condition where the product is closed.

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.

Basic safety

The product must be designed and manufactured so that it protects against damage due to electric shock and other dangers, and against any fires and explosions resulting from this.

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.

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 an automatic diagnostic. 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

Safety

Freedom from an unacceptable risk of damage.

Fail safe function

The capability of a system to perform the required actions for achieving or maintaining a defined safe state for the product under the control of the system.

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.

β

Failure factor of common cause for non-detectable dangerous failures. The failure factor is equivalent to the total β factor that would apply without diagnostic tests

β_D

Failure factor of common cause for detectable dangerous failures.

λ_{DD}

Cumulative failure rate in relation to Dangerous Detected failure types.

"Dangerous Detected" (DD): Dangerous Detected

$\lambda_{DD,PST}$

Cumulative failure rate in relation to dangerous failure types which can be determined through a partial opening test with diagnostic features in accordance with the configuration of IEC EN 61508.

"Dangerous Detected" (DD): Dangerous Detected

"Partial Stroke Test" (PST): Partial opening test

λ_{DU}

Cumulative failure rate in relation to dangerous failure types which can only be determined using full proof tests.

"Dangerous Undetected" (DU): Dangerous Undetected

$\lambda_{DU,FPT}$

Cumulative failure rate in relation to dangerous failure types which can be determined through a full proof test with diagnostic features in accordance with the configuration of IEC EN 61508.

"Dangerous Undetected" (DU): Dangerous Undetected

"Full Proof Test" (FPT): Full Proof Test

λ_{NE}

Cumulative failure rate in relation to failure types without an effect in the fail safe function.

"No effect" (NE): No effect

θ_{FPT}

Time interval between two successive full proof tests in hours.

"Full Proof Test" (FPT): Full Proof Test

θ_{PST}

Time interval between two successive partial opening tests in hours.

"Partial Stroke Test" (PST): Partial opening test

1.2 Abbreviations

E/E/EP

"Electrical, Electronic, Programmable Electronic": Electrical, Electronic, Programmable Electronic

FMEDA

"Failure Modes, Effects, and Diagnostic Analysis"

HFT

"Hardware Fault Tolerance"

MRT

"Mean Repair Time": Mean Repair Time

MTTR

"Mean Time To Restoration"

PFD_{AVG}

"Average Probability of Failure on Demand"

SFF

"Safe Failure Fraction": Ratio of safe failures to dangerous failures

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).

2 Standards / Literature used

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

IEC EN 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
---------------------	---

3 Functional description

The floating ball valves in stainless steel have a bare shaft. Thanks to the top flange according to ISO 5211, simple actuator mounting is possible.

4 Proof test

4.1 Without automatic test

The objective of the proof tests is the detection of faults within the valve which are not recognized through the automatic diagnostics of the system. The focus lies on undetected faults that prevent the Safety Instrumented Function from fulfilling its intended function.

The frequency of the proof tests, or the proof test interval, must be determined in the reliability calculations for the fail safe functions.

The extent of the proof tests for the product is listed in the FMEDA (Failure Modes, Effects and Diagnostic Analysis) report.

Persons who carry out the proof test should be trained in SIS operation, including bypass procedure, valve maintenance and company-relevant procedure.

4.2 With automatic partial opening test

An automatic test programme, which checks the total stroke of the product and measures the timing of the valve movement, recognizes most potentially dangerous failure types.

It is recommended to carry out a physical examination at regular intervals where the time interval depends on the system conditions. A maximum inspection interval of three years is recommended.

5 Assumptions

- Failure rates are constant, wear mechanics are not considered.
- Propagation of failures is irrelevant.
- The devices are installed in accordance with the manufacturer's instructions.
- Adequate tests are carried out prior to dispatch to ensure the absence of supplier and/or manufacturing defects that prevent faultless operation of the specified function in accordance with product specifications or cause operation deviating from the design analysed.
- Materials are compatible with process conditions and process media.

- Only the described versions are used for safety applications.
- All components that are not part of the fail safe function and cannot influence the fail safe function (feedback immune) are excluded.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- Clean operating air that is free from moisture is used in accordance with ANSI/ISA-7.0.01.1996 Quality Standard for Instrument Air.
- All devices are operated in low-demand operating mode.
- End position tests are carried out at a rate at least one hundred times faster than the expected demand rate.
- For SIL x fail safe functions, the partial opening test must comply with at least the requirements of SIL (x-1). If, for example, the safety needs to comply with SIL 3, then the partial opening test should comply with at least the requirements of SIL 2.
- Failures caused by maintenance capability are site specific and therefore cannot be included.

6 Usage period

The normal service life of the product is 3000 cycles.

7 SIL failure rate calculation for floating ball valves (BB02/BB06/BB07/BB0F/BB0M/B20)**SIL failure rate calculation****Functional safety in accordance with IEC EN 61508:2010**

We,

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

declare that, for the products listed below, the failure rates outlined below were determined in safety-related applications in accordance with IEC EN 61508.

The failure rates were determined by means of an FMEDA in accordance with IEC EN 61508. The assessment has been carried out by TÜV Italia (certificate number: C-IS-722264081).

Product description: Floating ball valves
(BB02/BB06/BB07/BB0F/BB0M/B20)

Device type: A

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

E/EE/EP safety-relevant system (last element)	Ball valves of the OM series, produced by Zhejiang Ouming Fluid Casting Industry Co, Ltd.	
System type	Type A	
Systematic capability	SC3	
Definition of the fail safe function	SIF1: "Correct switching where necessary (open to closed) and sealed for the closing phase, in the event of operating mode with low requirements"	SIF2: "Correct switching where necessary (closed to open), in the operating mode with low requirements"
Max SIL⁽¹⁾	SIL3	SIL3
λ_{TOT} (total)	9.188E-08	9.188E-08
λ_{NE} (no effect)	2.198E-08	3.143E-08
λ_S (fail safe)	0.000E+00	0.000E+00
$\lambda_{DD,PST}$ ⁽²⁾ (Dangerous Detected with Partial Valve Stroke Test)	1.864E-08	4.449E-08
$\lambda_{DU,FPST}$ (Dangerous Undetected, detectable with periodic full proof test)	5.125E-08	1.596E-08
β and β_D factor	10%	10%
MRT	8 hours	8 hours
Integrity of hardware safety	System 2 _H	System 2 _H
Systematic safety integrity	System 2 _S	System 2 _S

Explanations:

⁽¹⁾ The Safety Integrity Level (SIL) of the total Safety Instrumented Function (SIF) must be checked via a calculation of the PF- D_{AVG} under consideration of the redundant architectures, the proof test interval, the proof test effectiveness, any automatic diagnostics, the mean repair time and the specific failure rates of all products included in the SIF. Each part system must be tested, in order to ensure compliance with the minimum requirements regarding Hardware Fault Tolerance (HFT).

⁽²⁾ Consideration of an automatic partial opening test.



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
11.2023