# GEMÜ 4242

Ventilanschaltung mit integriertem Vorsteuerventil

DE

## SIL-Sicherheitshandbuch

Weitere Informationen
Webcode: GW-4242

## *Inhaltsverzeichnis*

# 1 Allgemeine Informationen

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

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

| Bezeichnung | Artikelnummer |
|---|---|
| ba_4242_IO-Link_de_gb | 88393655 |

## 1.1 Begriffsbestimmungen

**Ausfallsicherer Zustand**

Der ausfallsichere Zustand ist definiert als High (24 V DC) Signal an Pin 4 (Geräteausführung 24 V IO-Link), wenn die aktuelle Position des integrierten Wegmesssystems kleiner ist als Schaltpunkt ZU (Werkseinstellung 12 %).

**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:

- bewirkt, dass der Wert der Ausgangsmessung um mehr als 2 % FS (Full Scale) abweicht, oder 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 durch eine externe Diagnostik diagnostiziert wird (DU, „Dangerous Undetected").

**Gefahrbringend erkannt**

Ein Ausfall, der gefahrbringend ist, jedoch durch eine externe Diagnostik diagnostiziert wird (DD, „Dangerous Detected").

**Ankündigung („Annunciation")**

Ausfall, der die Sicherheit nicht direkt beeinträchtigt, jedoch die Fähigkeit zur Erkennung eines künftigen Ausfalls verringert (beispielsweise in einem Fehlerdiagnosekreis). Ausfälle des Typs „Ankündigung" werden in erkannte („Annunciation Detected", AD) und nicht erkannte („Annunciation Undetected", AU) Ausfälle unterteilt.

**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.

**Nicht beteiligt**

Komponente, die bei der Umsetzung der Sicherheitsfunktion keine Rolle spielt, die jedoch Bestandteil des Schaltplans ist und der Vollständigkeit halber aufgeführt wird.

**Automatische Diagnose**

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

**Hardware-Fehlertoleranz**

Eine Hardware-Fehlertoleranz von N bedeutet, dass N+1 die Mindestanzahl an Fehlern ist, die zu einem Verlust der Sicherheitsfunktion führen könnte.

**Betrieb mit hoher 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 größer ist als einmal pro Jahr.

**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.

**Typ-B-Element**

„Komplexes" Element (mit Verwendung von Mikrocontrollern oder programmierbarer Steuerung); Einzelheiten siehe unter 7.4.4.1.3 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

**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 |
| Electrical Component Reliability Handbook, 3. Auflage, 2012 | exida LLC, Electrical Component Reliability Handbook, dritte Auflage, 2012, ISBN 978-1-934977-04-0 |
| 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“ |

## 3 Funktionsbeschreibung

Der elektrische Stellungsrückmelder GEMÜ 4242 ist ein programmierbarer, elektrischer Stellungsrückmelder für Linearantriebe. Er besitzt eine mikroprozessorgesteuerte, intelligente Stellungserfassung mit einem integrierten analogen Wegmesssystem. Die nicht sicherheitsbezogene optische Stellungsrückmeldung erfolgt durch Weitsicht-LEDs. Eine integrierte IO-Link-Schnittstelle bietet zusätzliche Parametrierungs- und Diagnosefunktionen. Das Gehäuseoberteil besteht aus korrosionsbeständigem Kunststoff, das Gehäuseunterteil aus Edelstahl, Aluminium oder PPS (Polyphenylensulfid). Die Schutzklasse ist IP 67.

Der elektrische Stellungsrückmelder GEMÜ 4242 kann als Typ-B-Element mit einer Hardware-Fehlertoleranz von 0 betrachtet werden.

### 3.1 Sicherheitsfunktion

Der ausfallsichere Zustand ist definiert als High (24 V DC) Signal an Pin 4 (Geräteausführung 24 V IO-Link), wenn die aktuelle Position des integrierten Wegmesssystems kleiner ist als Schaltpunkt ZU (Werkseinstellung 12 %).

# 4 Beschreibung der Diagnosemöglichkeiten

## 4.1 Zeitliche und logische Plausibilitätsprüfung

Die Ausfallraten, die als „mit Test" angegeben sind, erfordern, dass die verbundene Sicherheits-SPS eine zeitliche und logische Plausibilitätsprüfung an den erwarteten Signalübergängen ausführt. Ein erwartetes Zeit-Übergangs-Diagramm ist in Abbildung 1 dargestellt.

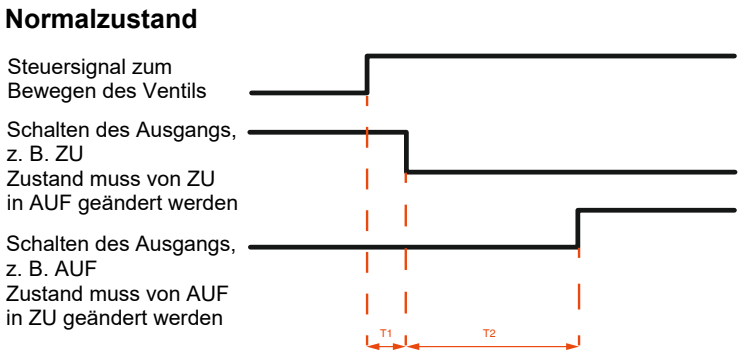



*Abb. 1: Zeitdiagramm*

Nachdem die Sicherheits-SPS ein Steuersignal gesendet hat, damit es sich z. B. aus der Stellung AUF in die Stellung ZU bewegt, muss überwacht werden, dass nach einer vorgegebenen Zeit T1 - T2 einer der Schaltausgänge seinen Zustand von ZU in AUF ändert (oder umgekehrt, je nach Konfiguration) und dass der andere Schaltausgang seinen Zustand von AUF in ZU ändert (oder umgekehrt, je nach Konfiguration).

## 4.2 Vollhubtest (FVST)

Vollhubtests („Full Valve Stroke Testing", FVST) folgen einem ähnlichen Konzept wie der PVST, mit dem Unterschied, dass das Prozessventil 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. Der Zweck des FVST besteht darin, eine diagnostische Kontrolle der SIF-Funktion, einschließlich Endschalterkasten, bereitzustellen. Eine mögliche Testanordnung ist in Abbildung 2 dargestellt.

Vollhubtests werden mit einer mindestens zehn mal höheren Rate durchgeführt als der erwarteten Anforderungsrate. Für Sicherheitsfunktionen gemäß SIL 2 muss der Vollhubtest (FVST) mindestens die Anforderungen von SIL 1 erfüllen.

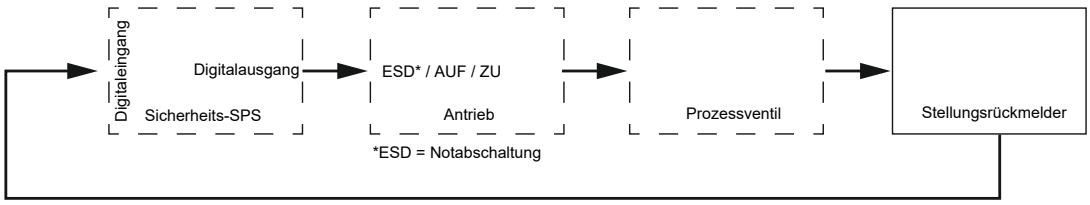



*Abb. 2: Mögliche Testanordnung*

## 5 Annahmen

- Ausfallraten sind konstant, Verschleißmechanismen sind nicht berücksichtigt.
- Die Ausbreitung von Ausfällen ist nicht relevant.
- 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.
- Die integrierte IO-Link-Schnittstelle wird nicht für eine Sicherheitsfunktion, sondern nur zur Parametrierung und für diagnostische Funktionen verwendet.
- Die korrekte Parametrierung wird vom Anwender überprüft.
- Werkstoffe sind mit Prozessbedingungen kompatibel.
- Die mittlere Reparaturzeit (MTTR) nach einem Ausfall beträgt 24 Stunden.
- Das Gerät ist gemäß den Anweisungen des Herstellers eingebaut.
- 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.
- 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.
- Tests werden mit einer mindestens zehn mal höheren Rate durchgeführt als der erwarteten Anforderungsrate.
- Für Sicherheitsfunktionen gemäß SIL 2 muss der Vollhubtest (FVST) mindestens die Anforderungen von SIL 1 erfüllen.
- Die Ausfallraten, bei denen die Durchführung eines Tests angenommen wird, erfordern, dass die verbundene Sicherheits-SPS eine zeitliche und logische Plausibilitätsprüfung an den erwarteten Signalübergängen ausführt.
- Die Ventilanschaltung GEMÜ 4242 wird nur in Verbindung mit Linearantrieben verwendet (Stellung ZU / AUF, keine Zwischenstellung).

## 6 SIL-Herstellererklärung GEMÜ 4242

# 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 (Failure Modes, Effects and Diagnostic Analysis) nach IEC 61508 ermittelt. Die Bewertung wurde durch exida.com durchgeführt (Berichtsnummer: GEMÜ 18/02-073 R006).

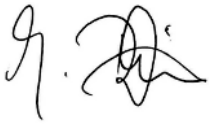
| | |
|---|---|
| **Produktbeschreibung:** | Elektrischer Stellungsrückmelder GEMÜ 4242 |
| **Gerätetyp:** | B |
| **Gültige Software-Version:** | V 1.0.1.2 |
| **Sicherheitsfunktion:** | Der ausfallsichere Zustand ist definiert als High (24 V DC) Signal an Pin 4 (Geräteausführung 24 V IO-Link), wenn die aktuelle Position des integrierten Wegmesssystems kleiner ist als Schaltpunkt ZU (Werkseinstellung 12 %). |
| **HFT (Hardware Failure Tolerance):** | 0 |
| **MTTR (Mean time to restoration):** | 24 Stunden |
| **MTBF (Mean Time Between Failures):** | 232 Jahre |

Die ermittelten Ausfallraten gelten für die Betriebsart mit hoher Anforderungsrate:

| | Ausfallraten (in FIT*) | |
|---|---|---|
| | ohne Test | mit Test |
| **Sicherheitsfunktion:** | 300 | 356 |
| **SIL** (Safety Integrity Level): | 1 | 2 |
| $\lambda_{DU}$ (Dangerous undetected): | 153 | 16 |
| $\lambda_{DD}$ (Dangerous detected): | 0 | 193 |
| $\lambda_{SU}$ (Safe undetected): | 147 | 147 |
| $\lambda_{SD}$ (Safe detected): | 0 | 0 |
| **SFF** (Safe Failure Fraction): | 49 % | 95 % |
| **DC** (Diagnostic Coverage of dangerous failures): | 0 % | 92 % |

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

Ingelfingen-Criesbach, 2019-09-12



Joachim Brien
Leiter Bereich Technik

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



09.2019