GEMÜ 1235

Elektrischer Stellungsrückmelder
Electrical position indicator

DE **SIL-Sicherheitshandbuch**

EN **SIL Safety Manual**

Weitere Informationen
Webcode: GW-1235

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 elektrischen Stellungsrückmelders in sicherheitsbezogenen Anwendungen gelten.

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

Bezeichnung	Artikelnummer
ba_1235_3S_4S_de_gb	88586076
ba_1235_3E_4E_de_gb	88586077

1.1 Begriffsbestimmungen

Ausfallsicherer Zustand

Der ausfallsichere Zustand ist definiert als High (24 V DC) Signal an Pin 5 (Geräteausführung 3S/4S) und an Pin 4 (Geräteausführung 3E/4E), 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 interne oder externe Diagnostik diagnostiziert wird (DU, „Dangerous Undetected").

Gefahrbringend erkannt

Ein Ausfall, der gefahrbringend ist, jedoch durch eine interne oder 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 = λ_{dd} / (λ_{dd} + λ_{du}))

FIT

„Failure in Time“: Ausfallrate (1x10^{-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 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
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 1235 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 PVDF. Die Schutzklasse ist IP 67.

Der elektrische Stellungsrückmelder GEMÜ 1235 kann als Typ-B-Element mit einer Hardware-Fehlertoleranz von 0 betrachtet werden.

3.1 Sicherheitsfunktion

Die Sicherheitsfunktion wird definiert als High (24 V DC) Signal an Pin 5 (Geräteausführung 3S/4S) und an Pin 4 (Geräteausführung 3E/4E), 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.

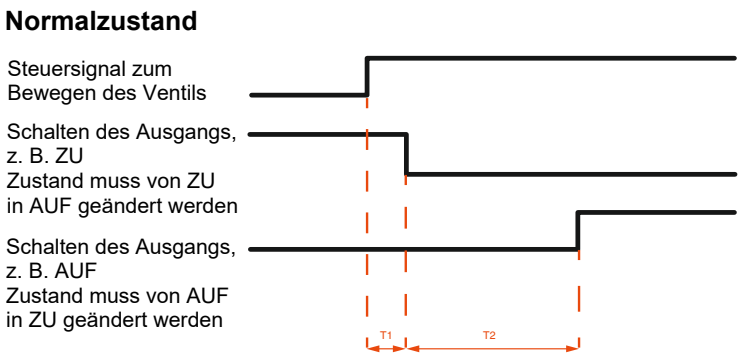

Abb. 1: Zeitdiagramm

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

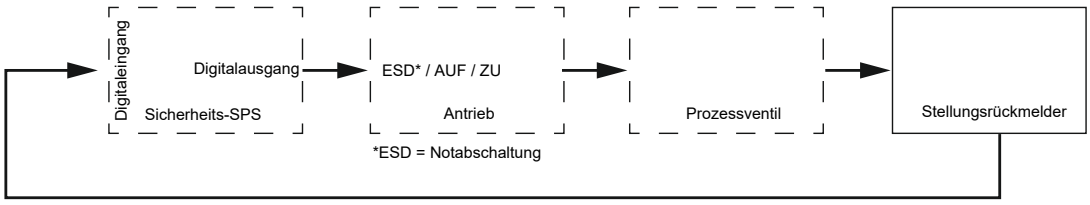

Abb. 2: Mögliche Testanordnung

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 einhundert mal höheren Rate durchgeführt als der erwarteten Anforderungsrate.
- Für Sicherheitsfunktionen gemäß SIL 2 muss der Vollhubtest (FVST) mindestens SIL 1 konform sein.
- 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.
- Der elektrische Stellungsrückmelder GEMÜ 1235 wird nur in Verbindung mit Linearantrieben verwendet (Stellung ZU / AUF, keine Zwischenstellung).
- Für die funktionale Sicherheit des Systems ist die Sicherheitssteuerung ein entscheidender Teil. Sie steuert den Ventilantrieb. Durch die Rückmeldung aus dem Stellungsrückmelder und seiner Ausfallratenangabe kann eine Gesamtbewertung bis SIL1 abgeleitet werden. Diese Bewertung aufzustellen und zu validieren ist Aufgabe des Systemintegrators.
- In Kombination mit einem Vollhubtest kann dabei SIL2 erreicht werden.
- Grundsätzlich sollte dabei ein geschlossenes Ventil als sicherer Zustand angenommen werden, was der Stellungsrückmelder als High (24V) signalisiert. Dies bewirkt, dass ein Ausfall der Versorgungsspannung als Fehler erkannt werden kann.

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 SIL-Ausfallratenberechnung GEMÜ 1235

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 R004).

Produktbeschreibung:	Elektrischer Stellungsrückmelder GEMÜ 1235
Gerätetyp:	B
Gültige Software-Version:	V 1.0.0.4
Sicherheitsfunktion:	Die Sicherheitsfunktion wird definiert als High (24 V DC) Signal an Pin 5 (Geräteausführung 3S/4S) und an Pin 4 (Geräteausführung 3E/4E), 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):	346 Jahre

Die ermittelten Ausfallraten gelten für die Betriebsart mit hoher Anforderungsrate:

	Ausfallraten (in FIT*)	
	ohne Test	mit Test
Sicherheitsfunktion:	161	180
SIL (Safety Integrity Level): [1)]	1	2
λ_{DU} (Dangerous undetected):	48	5
λ_{DD} (Dangerous detected):	0	62
λ_{SU} (Safe undetected):	113	113
λ_{SD} (Safe detected):	0	0
SFF (Safe Failure Fraction):	70 %	97 %
DC (Diagnostic Coverage of dangerous failures):	0 %	93 %

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 electrical position indicator in safety-related applications.

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

Designation	Item number
ba_1235_3S_4S_de_gb	88586076
ba_1235_3E_4E_de_gb	88586077

1.1 Definition of terms

Fail-Safe State

The fail-safe state is defined as a high (24 V DC) signal at pin 5 (device version 3S/4S) and at pin 4 (device version 3E/4E), if the current position of the integrated travel sensor is smaller than the switch point CLOSED (default setting 12 %).

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:

- deviates the output measurement value by more than 2 % of full scale or 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 is not detected by internal or external diagnostics (DU).

Dangerous Detected

Failure that is dangerous but is detected by internal or external diagnostics (DD).

Annunciation

Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.

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.

No part

Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

Automatic Diagnostics

Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.

Hardware Fault Tolerance

A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.

High 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 greater than one per year.

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.

Type B element

"Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

1.2 Abbreviations

DC

Diagnostic Coverage: Diagnostic coverage of dangerous failures (DC = λ_{dd} / (λ_{dd} + λ_{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

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
Electrical Component Reliability Handbook, 3rd Edition, 2012	exida LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
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 Stroke Testing For Block Valve Actuators in Safety Instrumented Systems Applications”

3 Functional description

The GEMÜ 1235 electrical position indicator is a programmable, electrical position indicator for linear actuators. It has a microprocessor controlled intelligent position sensor with an integrated analogue travel sensor system. The non safety-related optical position feedback is via high visibility LEDs. An integrated IO-Link interface offers additional parameterisation and diagnostic functions. The housing cover is made of corrosion resistant plastic and the housing base is PVDF. The protection class is IP 67.

The GEMÜ 1235 electrical position indicator can be considered to be a Type B element with a hardware fault tolerance of 0.

3.1 Safety function

The safety function is defined as a High (24 V DC) signal at pin 5 (device version 3S/4S) and at pin 4 (device version 3E/4E), if the current position of the integrated travel sensor is smaller than the switch point CLOSED (default setting 12 %).

4 Description of diagnostic possibilities

4.1 Temporal and logical plausibility check

The failure rates which are listed "with test" require that the connected safety PLC carries out a temporal and logical plausibility check on the expected signal transitions. An expected time / transition diagram is shown in Figure 1.

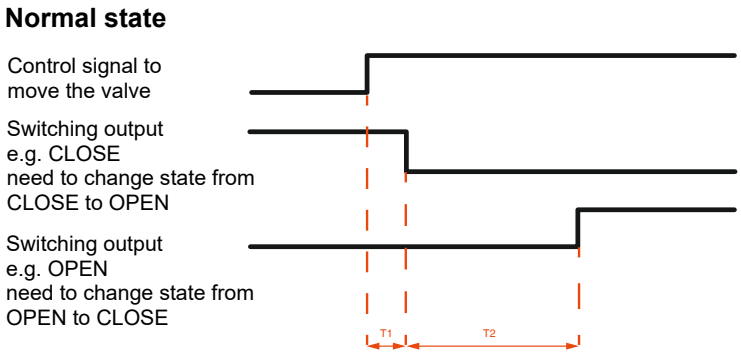

Fig. 1: Time diagram

After the safety PLC sent a control signal to the valve to move e.g. from OPEN to CLOSE it needs to monitor that one of the switching outputs changes its state from CLOSE to OPEN (or vice versa depending on the set-up) and that the other switching output changes its state from OPEN to CLOSE (or vice versa depending on the set-up) after a given time of T1 + T2.

4.2 Full Valve Stroke Testing (FVST)

Full Valve Stroke Testing (FVST) is similar in concept to a PVST, with the variation that the process 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. The purpose of FVST is to provide a diagnostic check of the SIF function including the limit switch box. A possible test set-up is shown in Figure 2.

Full Valve Stroke Testing is performed at a rate at least one hundred times faster than the expected demand rate. For SIL 2 safety functions, the Full Valve Stroke Testing (FVST) must be at least SIL 1 compliant.

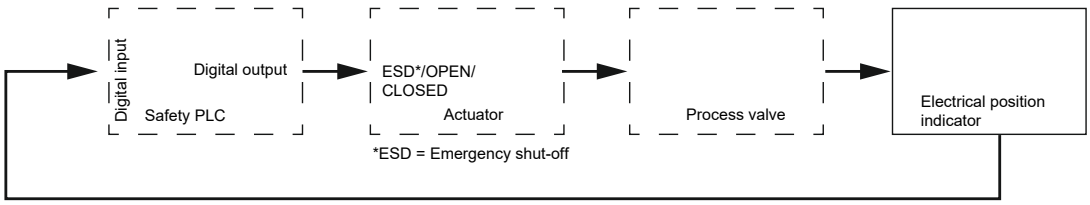

Fig. 2: Possible test set-up

5 Assumptions

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- The integrated IO-Link interface is not used for any safety function but only for parameterisation and diagnostic facilities.
- The correct parameterisation is verified by the user.
- Materials are compatible with process conditions.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- The device is installed per the manufacturer's instructions.
- 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.
- 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.
- Testing is performed at a rate at least one hundred times faster than the expected demand rate.
- For SIL 2 safety functions, the Full Valve Stroke Testing (FVST) must be at least SIL 1 compliant.
- The failure rates that assume a test require that the connected safety PLC carries out a temporal and logical plausibility check on the expected signal transitions.
- The GEMÜ 1235 electrical position indicator is only used in conjunction with linear actuators (CLOSED/OPEN position, no intermediate position).
- The safety controller is an essential part for the functional safety of the system. It controls the valve actuator. The feedback from the electrical position indicator and its failure rate can be used as the basis for an overall evaluation up to SIL 1. Drawing up and validating this evaluation is the task of the system integrator.
- When combined with Full Valve Stroke Testing, SIL 2 can be achieved.
- A closed valve should always be assumed to be the safe state, which is indicated as High (24 V) by the electrical position indicator. This means that failure of the supply voltage can be recognized as a fault.

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 SIL failure rate calculation GEMÜ 1235

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 R004).

Product description:	GEMÜ electrical position indicator 1235
Device type:	B
Valid software version:	V1.0.0.4
Safety function:	The safety function is defined as a High (24 V DC) signal at pin 5 (device version 3S/4S) and at pin 4 (device version 3E/4E), if the current position of the integrated travel sensor is smaller than the switch point CLOSED (default setting 12%).
HFT (Hardware Fault Tolerance):	0
MTTR (Mean Time To Restoration):	24 hours
MTBF (Mean Time Between Failures):	346 years

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

	Failure rates (in FIT*)	
	Without test	With test
Safety function:	161	180
SIL (Safety Integrity Level): [1)]	1	2
λ_{DU} (Dangerous undetected):	48	5
λ_{DD} (Dangerous detected):	0	62
λ_{SU} (Safe undetected):	113	113
λ_{SD} (Safe detected):	0	0
SFF (Safe Failure Fraction):	70 %	97 %
DC (Diagnostic Coverage of dangerous failures):	0 %	93 %

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