

## GEMÜ 4242

Combi switchbox with integrated pilot valve

EN

### SIL Safety Manual



IO-Link



further information  
webcode: GW-4242



All rights including copyrights or industrial property rights are expressly reserved.

Keep the document for future reference.

© GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG  
12.09.2019

---

## Contents

<b>1</b>	<b>General information</b>	<b>4</b>
1.1	Definition of terms	4
1.2	Abbreviations	5
<b>2</b>	<b>Standards / Literature used</b>	<b>5</b>
<b>3</b>	<b>Functional description</b>	<b>5</b>
3.1	Safety function	5
<b>4</b>	<b>Description of diagnostic possibilities</b>	<b>6</b>
4.1	Temporal and logical plausibility check	6
4.2	Full Valve Stroke Testing (FVST)	6
<b>5</b>	<b>Assumptions</b>	<b>7</b>
<b>6</b>	<b>SIL manufacturer's declaration GEMÜ 4242</b>	<b>8</b>
	Functional safety in accordance with IEC 61508 and IEC 61511	000
	Texts	000

## 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_4242_IO-Link_de_gb	88393655

### 1.1 Definition of terms

#### Fail-Safe State

The fail-safe state is defined as a High (24 V DC) signal at pin 4 (device version 24 V IO-Link), 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 that is not being diagnosed by external diagnostics (DU).

#### Dangerous Detected

Failure that is dangerous but is detected by 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 ( $DC = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$ )

### FIT

Failure in Time: Failure rate ( $1 \times 10^{-9}$  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<sub>AVG</sub>

Average Probability of Failure on Demand

### PVST

Partial Valve Stroke Test

### SFF

Safe Failure Fraction

### 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 4242 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 stainless steel, aluminium or PPS (polyphenylene sulfide). The protection class is IP 67.

The GEMÜ 4242 electrical position indicator can be considered to be a Type B element with a hardware fault tolerance of 0.

### 3.1 Safety function

The fail-safe state is defined as a High (24 V DC) signal at pin 4 (device version 24 V IO-Link), 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.

#### Normal state

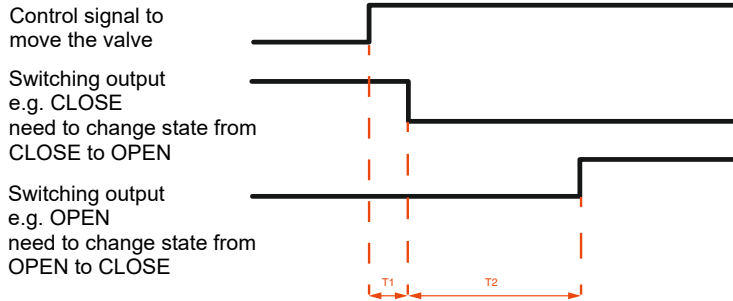


Fig. 1: Time diagram

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 ten times faster than the expected demand rate. For SIL 2 safety functions the Full Valve Stroke Testing (FVST) is at least SIL 1 compliant.

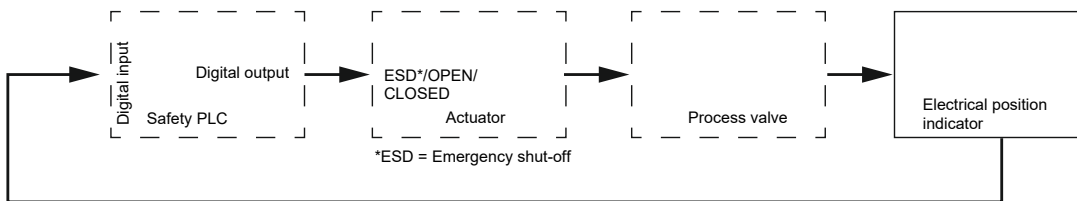


Fig. 2: Possible test set-up

## 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 variants 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 ten times faster than the expected demand rate.
- For SIL 2 safety functions the Full Valve Stroke Testing (FVST) is 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 4242 combi switchbox is only used in conjunction with linear actuators (CLOSED / OPEN position, no intermediate position).

**6 SIL manufacturer's declaration GEMÜ 4242**

# Manufacturer's declaration

## 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 18/02-073 R006).

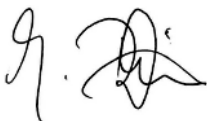
**Product description:** Electrical position indicator GEMÜ 4242  
**Device type:** B  
**Valid software version:** V1.0.1.2  
**Safety function:** The fail-safe state is defined as a High (24 V DC) signal at pin 4 (device version 24 V IO-Link), if the current position of the integrated travel sensor 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):** 232 years

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

	Failure rates (in FIT*)	
	Without test	With test
<b>Safety function:</b>	300	356
<b>SIL (Safety Integrity Level):</b>	1	2
<b><math>\lambda_{DU}</math> (Dangerous undetected):</b>	153	16
<b><math>\lambda_{DD}</math> (Dangerous detected):</b>	0	193
<b><math>\lambda_{SU}</math> (Safe undetected):</b>	147	147
<b><math>\lambda_{SD}</math> (Safe detected):</b>	0	0
<b>SFF (Safe Failure Fraction):</b>	49 %	95 %
<b>DC (Diagnostic Coverage of dangerous failures):</b>	0 %	92 %

\* FIT = Failure In Time ( $1 \times 10^{-9}$  failures per hour)

Ingelfingen-Criesbach, 2019-09-12



Joachim Brien  
 Head of Technical Department





GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG  
Fritz-Müller-Straße 6-8, 74653 Ingelfingen-Criesbach,  
Germany  
Phone +49 (0)7940 123-0 · info@gemue.de  
www.gemu-group.com

Subject to alteration

09.2019