



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

Electrical Position Indicator GEMÜ 12A0

Customer:

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG  
Niedernhall-Waldzimmern  
Germany

Contract No.: GEMÜ 25/06-071-R2

Report No.: GEMÜ 25/06-071 R001

Version V1, Revision R0; October 2025

Jan Hettenbach

## Management summary

This report summarizes the results of the hardware assessment carried out on the Electrical Position Indicator GEMÜ 12A0 with software version V.1.1.0.0 and hardware version as listed in the drawings referenced in section 2.5.1.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). An FMEDA is one of the steps taken to achieve functional safety assessment of a device or subsystem per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) and other safety metrics are calculated for the device or subsystem. For full assessment purposes all requirements of the applicable standards must be considered.

For safety applications, only the variants mentioned in Table 1 of the Electrical Position Indicator GEMÜ 12A0 are considered. All other possible variants and configurations are not covered by this report.

**Table 1: Overview of covered product variants**

Type	Field bus interface	Motion type	Design variant
12A0	IO-Link (IO)	Linear (L)	BG1
12A0	IO-Link (IO)	Linear (L)	BG2
12A0	IO-Link (IO)	Linear (L)	BG3
12A0	IO-Link (IO)	Rotary (R)	BG1
12A0	IO-Link (IO)	Rotary (R)	BG2
12A0	IO-Link (IO)	Rotary (R)	BG3

This analysis is performed on the 12A0 device variants BG1 [D1] / BG2 [D2] / BG3 [D3] in the motion type “rotary”. The “rotary” motion type needs an additional mounting adapter [D4].

From the perspective of functional safety, the “rotary” type of the 12A0 is the more critical variant, because the failure rates are slightly higher compared to the “linear” type, which doesn’t need the additional mounting adapter. Therefore, this analysis covers both motion types “linear” and “rotary” of the Electrical Position Indicator GEMÜ 12A0.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 3 <sup>1</sup>.

The Electrical Position Indicator GEMÜ 12A0 can be considered to be a Type B <sup>2</sup> element with a hardware fault tolerance of 0 according to IEC 61508.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 5.2.3.

The following table shows how the above stated requirements are fulfilled for the Electrical Position Indicator GEMÜ 12A0 with configuration of active high configured C/Q signal in case of closed valve.

---

<sup>1</sup> For details see Appendix 3.

<sup>2</sup> Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

**Table 2: Electrical Position Indicator GEMÜ 12A0 in motion type “rotary”  
(needs additional mounting adapter [D4]) – failure rates per IEC 61508:2010**

Failure category	<i>exida</i> Profile 3	
	Failure rates (in FIT)	
	without test	with test <sup>3</sup>
<b>Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>	<b>0</b>
<b>Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>96</b>	<b>96</b>
<b>Dangerous Detected (<math>\lambda_{DD}</math>), by external diagnostics</b>	<b>0</b>	<b>127</b>
<b>Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>141</b>	<b>14</b>
Annunciation Detected ( $\lambda_{AD}$ )	0	23
Annunciation Undetected ( $\lambda_{AU}$ )	26	3
No effect	57	57
No part	594	594
<b>Total failure rate (safety function)</b>	<b>237</b>	<b>237</b>
<b>SFF <sup>4</sup></b>	<b>40%</b>	<b>94%</b>
<b>DC</b>	<b>0%</b>	<b>90%</b>
<b>MTBF</b>	<b>812 years</b>	
<b>SIL AC <sup>5</sup></b>	<b>---</b>	<b>SIL 2</b>

The failure rates are valid for the useful life of the considered Electrical Position Indicator GEMÜ 12A0 in motion type “rotary” with additional mounting adapter (see Appendix 2) when operating as defined in the considered scenarios.

The motion type “linear” without the mounting adapter has about 0.5 % less DU failures.

<sup>3</sup> This analysis assumes that the connected safety logic solver carries out a temporal and logical plausibility check on the expected signal transitions. Further details are given in section 4.

<sup>4</sup> The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>5</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	6
2 Project management.....	7
2.1 <i>exida</i> .....	7
2.2 Roles of the parties involved .....	7
2.3 Standards / Literature used .....	7
2.4 <i>exida</i> tools used.....	7
2.5 Reference documents .....	8
2.5.1 Documentation provided by the customer .....	8
2.5.2 Documentation generated by <i>exida</i> .....	8
3 Description of the analyzed element.....	9
4 Description of diagnostic possibilities.....	10
4.1 Temporal and logical plausibility check .....	10
4.2 Full Valve Stroke Testing (FVS) .....	10
5 Failure Modes, Effects, and Diagnostic Analysis .....	11
5.1 Description of the failure categories .....	11
5.2 Methodology – FMEDA, Failure rates.....	12
5.2.1 FMEDA.....	12
5.2.2 Failure rates.....	12
5.2.3 Assumptions.....	13
5.3 Results.....	14
5.3.1 Electrical Position Indicator GEMÜ 12A0 in motion type “rotary” .....	15
6 Terms and Definitions .....	16
7 Status of the document.....	17
7.1 Liability.....	17
7.2 Releases .....	17
7.3 Release signatures .....	17
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	18
Appendix 1.1: Proof test to detect dangerous undetected faults .....	18
Appendix 2: Impact of lifetime of critical components on the failure rate .....	19
Appendix 3: <i>exida</i> Environmental Profiles .....	20

## 1 Purpose and Scope

This document shall describe the results of the mechanical assessment carried out on the Electrical Position Indicator GEMÜ 12A0 with hardware version as listed in the drawings referenced in section 2.5.1 and software version V.1.1.0.0.

The FMEDA builds the basis for an evaluation whether an element including the described Electrical Position Indicator GEMÜ 12A0 meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

## 2 Project management

### 2.1 *exida*

*exida* is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity.

Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project-oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

### 2.2 Roles of the parties involved

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG      Manufacturer of the Electrical Position Indicator GEMÜ 12A0.

*exida*      Performed the hardware assessment.

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG contracted *exida* in June 2025 with the FMEDA of the above mentioned device.

### 2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components	<i>exida</i> LLC, Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components ISBN 978-1-934977-09-5
[N3]	Mechanical Component Reliability Handbook, 5th Edition, 2021	<i>exida</i> LLC, Mechanical Component Reliability Handbook, 5th Edition, 2021, ISBN 978-1-934977-10-1
[N4]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions
[N5]	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”

### 2.4 *exida* tools used

[T1]	SILcal X – 1.6.4 Build 1128	<i>exida</i> FMEDA Tool
------	-----------------------------	-------------------------

## 2.5 Reference documents

### 2.5.1 Documentation provided by the customer

[D1]	12A0IO0LB1P01IBL0_Elektr. Stellungsrückmelder-+- GE401647.pdf	Mechanical drawing 12A0 linear BG1 of 02.07.2025
[D2]	12A0_BG2_Elektr. Stellungsrückmelder-+- GE401267.pdf	Mechanical drawing 12A0 linear BG2 of 19.09.2022
[D3]	12A0_BG3_DRAFT_Elektr. Stellungsrückmelder-+- GE200810.pdf	Mechanical drawing 12A0 linear BG3 of 16.07.2025
[D4]	12A0IO0RB2P01IBL0 GM01_Elektr. Stellungsrückmelder-+- DRW081817_-.pdf	Mechanical drawing 12A0 rotary adapter of 21.06.2024 The rotary adapter can be combined with 12A0 linear BG1 [D1] / BG2 [D2] / BG3 [D3]
[D5]	7-0299- 0353_Basic_BG2_250520.pdf	Schematic diagram of basic board V2 of 24.07.2025
[D6]	7-0257-0395_V2.xlsx	BOM of basic board
[D7]	7-0299-0368_AL_IO- Link_EVO1_V2_250205.PDF	Schematic diagram of IO link board V2 of 18.11.2024
[D8]	7-0257-0412_V1.xlsx	BOM of IO link board

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

### 2.5.2 Documentation generated by *exida*

[R1]	12A0_Pos_GEMUE_electronic.3fmx	
[R2]	12A0_Pos_GEMUE_Mech.3fmx	
[R3]	12A0_Pos_GEMUE_electronik_mechanic.3fmx	
[R4]	12A0_Pos_GEMUE_electronik_mechanic_with_adapter.xlsx	Printout V1R0
[R5]	12A0_Pos_GEMUE_electronik_mechanic-with-external- DIAG_with_adapter.xlsx	Printout V1R0



### 3 Description of the analyzed element

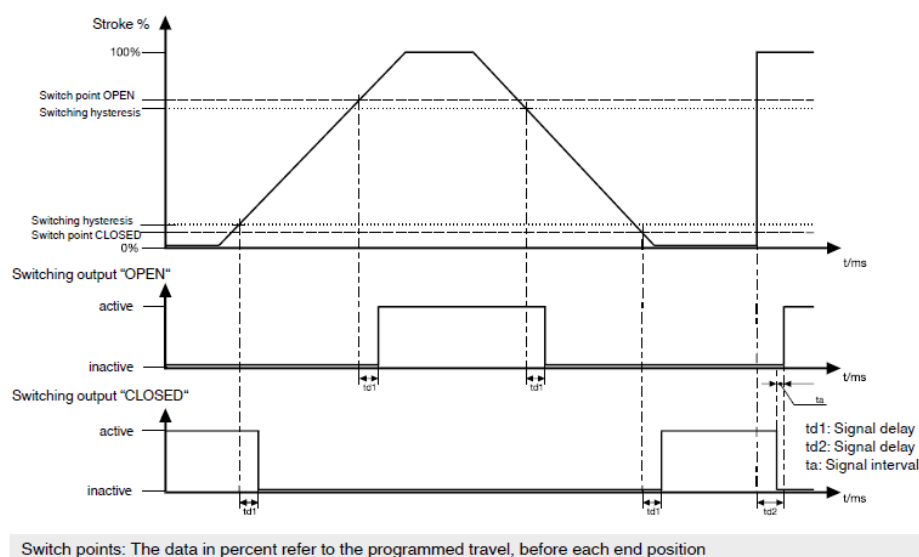
The Electrical Position Indicators GEMÜ 12A0 can be considered to be Type B elements with a hardware fault tolerance of 0.

The Electrical Position Indicators GEMÜ 12A0 are programmable, electrical position indicators for linear and rotary actuators. They have a microprocessor controlled intelligent position sensor with an integrated analog travel sensor system. The non-safety-related optical position feedback is via high visibility LEDs. Also, some non-safety-related environmental sensors are included, e.g. to monitor pressure or temperature.

The integrated IO-Link interface provides the C/Q output signal, which is considered as the safety-related output signal. Only the configuration valve closed = C/Q signal "HIGH" is considered as a safety-related configuration. The housing cover and base is made of polycarbonate.



**Figure 1: Examples for Electrical Position Indicators GEMÜ 12A0**



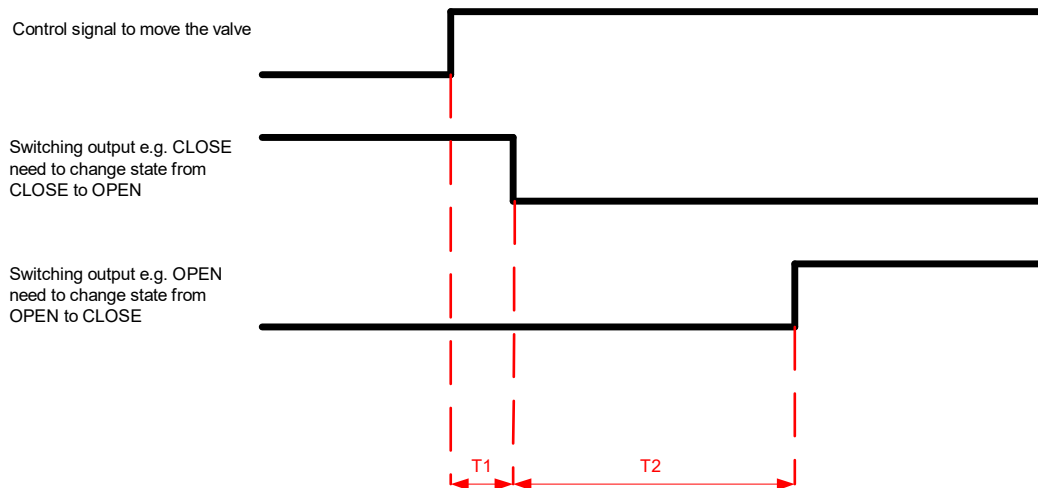
**Figure 2: Switching characteristic of output signals**

## 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 logic solver carries out a temporal and logical plausibility check on the expected signal transitions. An expected time / transition diagram is shown in Figure 3.

#### Normal state



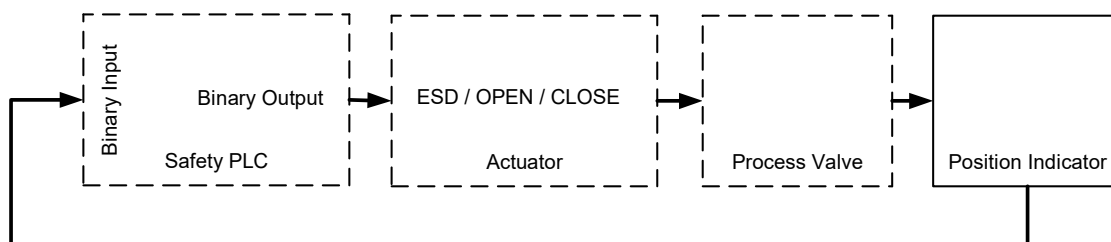
**Figure 3: Time diagram**

After the safety logic solver 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 (FVS)

Full Stroke Testing (FST) is similar in concept to a PST (partial stroke testing), 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. A possible test set-up is shown in Figure 4.

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.



**Figure 4: Possible test set-up**

Partial stroke testing methods are further described in [N5].

## 5 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG and is documented in [R1] to [R5].

### 5.1 Description of the failure categories

In order to judge the failure behavior of the Electrical Position Indicator GEMÜ 12A0, the following definitions for the failures of the product were considered:

Fail-Safe State	The fail-safe state is defined as the valve is in closed position, but the device indicates an “open” valve. In that case, the position output signal at C/Q Pin 4 indicates “LOW” (0V) <sup>6</sup> .
Safe	<p>A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:</p> <ul style="list-style-type: none"> <li>a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,</li> <li>b) 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.</li> </ul>
Dangerous	<p>A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:</p> <ul style="list-style-type: none"> <li>a) The position output signal at C/Q Pin 4 shows permanently closed valve; or,</li> <li>b) decreases the probability that the safety function operates correctly when required.</li> </ul>
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.

<sup>6</sup> The additional I/Q signal (Pin 2) is only used for diagnostic in combination with the C/Q Pin. The I/Q Pin is showing HIGH signal in case of an “open” valve.

## 5.2 Methodology – FMEDA, Failure rates

### 5.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### 5.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from a proprietary electrical and mechanical component failure rate database derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to *exida* Profile 3. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions, the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

### 5.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Electrical Position Indicator GEMÜ 12A0.

- 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.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The correct parameterization 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 Electrical Position Indicator GEMÜ 12A0 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 device variants mentioned in Table 1 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 hundred 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 C/Q output position signal at Pin 4 is configured as HIGH active, which means that in case of a closed valve the C/Q output signal goes to HIGH. Other possible configurations of C/Q signal are not considered.
- The I/Q output is only used for diagnosis to detect an open valve.
- Failure rates shown in the *with test* column (Table 2 and Table 3) are only valid if the connected safety logic solver performs a temporal and logical plausibility check of the expected signal transitions as described in section 4, "Description of diagnostic possibilities".
- The Electrical Position Indicator GEMÜ 12A0 is used on linear or quarter-turn actuators (position CLOSE / OPEN, no intermittent position).

### 5.3 Results

$$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$$

$$\lambda_{total} = \lambda_{SAFE} + \lambda_{DD} + \lambda_{DU}$$

$$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{AU})) + 24\ h$$

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1<sub>H</sub> approach according to 7.4.4.2 of IEC 61508-2 or the 2<sub>H</sub> approach according to 7.4.4.3 of IEC 61508-2.

The 1<sub>H</sub> approach involves calculating the Safe Failure Fraction for the entire element.

The 2<sub>H</sub> approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-2.

This assessment supports the 1<sub>H</sub> approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe failures plus dangerous detected failures and safe failures plus dangerous failures. This ratio is represented by the following equation:

$$SFF = (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg) / (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg + \Sigma\lambda_{DU}\ avg)$$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$$

Where:

$\lambda_S$  = Fail Safe

$\lambda_{DD}$  = Fail Dangerous Detected

$\lambda_{DU}$  = Fail Dangerous Undetected

As the Electrical Position Indicator GEMÜ 12A0 is only one part of an element, the architectural constraints should be determined for the entire final element.

### 5.3.1 Electrical Position Indicator GEMÜ 12A0 in motion type “rotary”

The FMEDA carried out on the Electrical Position Indicator GEMÜ 12A0 under the assumptions described in section 5.2.3 and the definitions given in section 5.1 and 5.3 leads to the following failure rates:

**Table 3: Electrical Position Indicator GEMÜ 12A0 in motion type “rotary”  
(needs additional mounting adapter [D4])<sup>7</sup> – failure rates per IEC 61508:2010**

Failure category	<i>exida</i> Profile 3	
	Failure rates (in FIT)	
	without test	with test <sup>8</sup>
<b>Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>	<b>0</b>
<b>Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>96</b>	<b>96</b>
<b>Dangerous Detected (<math>\lambda_{DD}</math>), by external diagnostics</b>	<b>0</b>	<b>127</b>
<b>Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>141</b>	<b>14</b>
Annunciation Detected ( $\lambda_{AD}$ )	0	23
Annunciation Undetected ( $\lambda_{AU}$ )	26	3
No effect	57	57
No part	594	594
<b>Total failure rate (safety function)</b>	<b>237</b>	<b>237</b>
<b>SFF<sup>9</sup></b>	<b>40%</b>	<b>94%</b>
<b>DC</b>	<b>0%</b>	<b>90%</b>
<b>MTBF</b>	<b>812 years</b>	
<b>SIL AC<sup>10</sup></b>	<b>---</b>	<b>SIL 2</b>

<sup>7</sup> Versions without mounting adapter have about 0.5 % less DU failures than versions with mounting adapter.

<sup>8</sup> This analysis assumes that the connected safety logic solver carries out a temporal and logical plausibility check on the expected signal transitions. Further details are given in section 4.

<sup>9</sup> The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>10</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

## 6 Terms and Definitions

Automatic Diagnostics	Tests are performed online, either internally by the device or, if specified, externally by another device without manual intervention.
DC	Diagnostic Coverage of dangerous failures ( $DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$ )
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
FST	Full stroke testing
HFT	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.
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.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
$PFD_{AVG}$	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
PST	Partial stroke testing
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B element	"Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval



## 7 Status of the document

### 7.1 Liability

*exida* prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

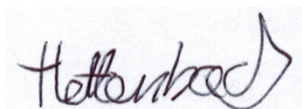
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three-year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, and the exact results are critical to the SIL verification, you may wish to contact the product vendor to verify the current validity of the results.

### 7.2 Releases

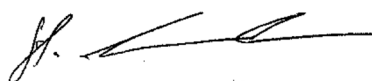
Version History:	V1R0: Editorial changes after customer feedback and internal review; October 27, 2025
	V0R1: Initial version; September 16, 2025
Authors:	Jan Hettenbach
Review:	V0R1 Stephan Aschenbrenner ( <i>exida</i> ), Philipp Göker (GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG )
Release status:	Released to GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG

### 7.3 Release signatures



---

Dipl. -Ing. (Univ.) Jan Hettenbach



---

Dipl.-Ing. (Univ.) Stephan Aschenbrenner

## Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 f) of IEC 61508-2, proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual, as it contains important safety related information.

### Appendix 1.1: Proof test to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 4.

**Table 4 Steps for Proof Test**

Step	Action
1	Take appropriate action to avoid a false trip
2	Inspect the device for any visible damage, corrosion or contamination.
3	Force the Electrical Position Indicator GEMÜ 12A0 to detect a desired position and verify that the desired position is correctly indicated.
4	Force the Electrical Position Indicator GEMÜ 12A0 to detect a desired position at the opposite side and verify that the desired position is correctly indicated.
5	Restore the loop to full operation
6	Restore normal operation

This test will detect 90% of possible “du” failures when no test has been carried out before and 90% of possible “du” failures when a test is periodically carried out.

## Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 5.2.3) this only applies provided that the useful lifetime<sup>11</sup> of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that a  $PFD_{AVG}$  calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

Table 5 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to a  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 5: Useful lifetime of components with reduced useful lifetime contributing to  $\lambda_{du}$**

Type	Useful life
Mechanical parts	Approximately 10 years

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

<sup>11</sup> Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

### Appendix 3: *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
<b>Description (Electrical)</b>	Cabinet mounted/ Climate Controlled	Low Power Field Mounted  no self-heating	General Field Mounted  self-heating	Subsea	Offshore	N/A
<b>Description (Mechanical)</b>	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
<b>IEC 60654-1 Profile</b>	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
<b>Average Ambient Temperature</b>	30°C	25°C	25°C	5°C	25°C	25°C
<b>Average Internal Temperature</b>	60°C	30°C	45°C	5°C	45°C	Process Fluid Temp.
<b>Daily Temperature Excursion (pk-pk)</b>	5°C	25°C	25°C	0°C	25°C	N/A
<b>Seasonal Temperature Excursion (winter average vs. summer average)</b>	5°C	40°C	40°C	2°C	40°C	N/A
<b>Exposed to Elements/Weather Conditions</b>	No	Yes	Yes	Yes	Yes	Yes
<b>Humidity <sup>12</sup></b>	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
<b>Shock <sup>13</sup></b>	10 g	15 g	15 g	15 g	15 g	N/A
<b>Vibration <sup>14</sup></b>	2 g	3 g	3 g	3 g	3 g	N/A
<b>Chemical Corrosion <sup>15</sup></b>	G2	G3	G3	G3	G3	Compatible Material
<b>Surge <sup>16</sup></b>						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
<b>EMI Susceptibility <sup>17</sup></b>						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
<b>ESD (Air) <sup>18</sup></b>	6kV	6kV	6kV	6kV	6kV	N/A

<sup>12</sup> Humidity rating per IEC 60068-2-3

<sup>13</sup> Shock rating per IEC 60068-2-27

<sup>14</sup> Vibration rating per IEC 60068-2-6

<sup>15</sup> Chemical Corrosion rating per ISA 71.04

<sup>16</sup> Surge rating per IEC 61000-4-5

<sup>17</sup> EMI Susceptibility rating per IEC 61000-4-3

<sup>18</sup> ESD (Air) rating per IEC 61000-4-2