



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

Project:

Electrical Position Indicator GEMÜ 1235

Customer:

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

Contract No.: GEMÜ 13/08-046

Report No.: GEMÜ 13/08-046 R004

Version V1, Revision R0; July 2014

Stephan Aschenbrenner

## Management summary

This report summarizes the results of the hardware assessment carried out on the Electrical Position Indicator GEMÜ 1235 with software version V1.0.0.4 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). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

For safety applications only the described Electrical Position Indicator GEMÜ 1235 has been considered. All other possible variants and configurations are not covered by this report.

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG and *exida* together did a quantitative analysis of the Electrical Position Indicator GEMÜ 1235 to calculate the failure rates using *exida*'s component database (see [N3]) for the different components. 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 1235 can be considered to be a Type B<sup>2</sup> element with a hardware fault tolerance of 0.

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 worst-case configurations of the considered Electrical Position Indicator GEMÜ 1235. The indicated failure rates include only the failure rates of one switch / sensor as only one switch / sensor is part of the considered safety function.

---

<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 1: Electrical Position Indicator GEMÜ 1235 – 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>113</b>             | <b>113</b>             |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>), by external diagnostics</b> | <b>0</b>               | <b>62</b>              |
| Dangerous Detected ( $\lambda_{dd}$ )                                          | 0                      | 43                     |
| Annunciation Detected ( $\lambda_{AD}$ )                                       | 0                      | 19                     |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>)</b>                        | <b>48</b>              | <b>5</b>               |
| Annunciation Undetected ( $\lambda_{AU}$ )                                     | 21                     | 2                      |
| No effect                                                                      | 146                    | 146                    |
| No part                                                                        | 2                      | 2                      |
| <b>Total failure rate (safety function)</b>                                    | <b>161</b>             | <b>180</b>             |
| <b>SFF <sup>4</sup></b>                                                        | <b>70%</b>             | <b>97%</b>             |
| <b>DC</b>                                                                      | <b>0%</b>              | <b>93%</b>             |
| <b>MTBF</b>                                                                    | <b>346 years</b>       |                        |
| <b>SIL AC <sup>5</sup></b>                                                     | <b>SIL 1</b>           | <b>SIL 2</b>           |

The failure rates are valid for the useful life of the considered Electrical Position Indicator GEMÜ 1235 (see Appendix 2) when operating as defined in the considered scenarios.

<sup>3</sup> This analysis assumes that the connected safety PLC carries out a temporal and logical plausibility check on the expected signal transitions. Further details are given in section 4.1.

<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 .....                                                                | 5  |
| 2 Project management.....                                                                | 6  |
| 2.1 <i>exida</i> .....                                                                   | 6  |
| 2.2 Roles of the parties involved .....                                                  | 6  |
| 2.3 Standards / Literature used .....                                                    | 6  |
| 2.4 <i>exida</i> tools used.....                                                         | 6  |
| 2.5 Reference documents .....                                                            | 7  |
| 2.5.1 Documentation provided by the customer .....                                       | 7  |
| 2.5.2 Documentation generated by <i>exida</i> .....                                      | 7  |
| 3 Description of the analyzed element.....                                               | 8  |
| 4 Description of diagnostic possibilities.....                                           | 9  |
| 4.1 Temporal and logical plausibility check .....                                        | 9  |
| 4.2 Full Valve Stroke Testing (FVST) .....                                               | 9  |
| 5 Failure Modes, Effects, and Diagnostic Analysis .....                                  | 10 |
| 5.1 Description of the failure categories .....                                          | 10 |
| 5.2 Methodology – FMEDA, Failure rates.....                                              | 11 |
| 5.2.1 FMEDA.....                                                                         | 11 |
| 5.2.2 Failure rates.....                                                                 | 11 |
| 5.2.3 Assumptions.....                                                                   | 12 |
| 5.3 Results.....                                                                         | 13 |
| 5.3.1 Electrical Position Indicator GEMÜ 1235 .....                                      | 14 |
| 6 Using the FMEDA results.....                                                           | 15 |
| 6.1 Example PFD <sub>AVG</sub> / PFH calculation.....                                    | 15 |
| 7 Terms and Definitions.....                                                             | 16 |
| 8 Status of the document.....                                                            | 17 |
| 8.1 Liability.....                                                                       | 17 |
| 8.2 Releases .....                                                                       | 17 |
| 8.3 Release Signatures.....                                                              | 17 |
| Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test .. | 18 |
| Appendix 1.1: Proof tests 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 1235 with software version V1.0.0.4 and hardware version as listed in the drawings referenced in section 2.5.1.

The FMEDA builds the basis for an evaluation whether an element including the described Electrical Position Indicator GEMÜ 1235 meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) / Probability of dangerous Failure per Hour (PFH) 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 and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG      Manufacturer of the Electrical Position Indicator GEMÜ 1235.

*exida*      Performed the hardware assessment.

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG contracted *exida* in January 2013 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] | Electrical Component Reliability Handbook, 3rd Edition, 2012 | <i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0              |
| [N3] | Mechanical Component Reliability Handbook, 3rd Edition, 2012 | <i>exida</i> LLC, Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7              |
| [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 V8.0.11                 | FMEDA Tool            |
| [T2] | exSILentia Ultimate V3.2.1.896 | SIL Verification Tool |

## 2.5 Reference documents

### 2.5.1 Documentation provided by the customer

|      |                                                                  |                                                                                                  |
|------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| [D1] | db_1235_1236_V_3E_3S_4E_4S_gb.pdf                                | Technical data sheet „Electrical Position Indicator Device Version 3E,3S,4E,4S“ 01/2013 88353395 |
| [D2] | 7-0299-0178_ae34474.pdf                                          | Circuit diagram “1235 STELLUNGSRUECKMELDER STANDARD MIT I/O LINK“ 7-0299-0178 of 21.11.2011      |
| [D3] | 1235000Z3EM125030G10_ELEKTR.STELLUNGSANZEIGE_AUF_ZU_00436489.PDF | Mechanical drawing „ELEKTR. STELLUNGSANZEIGE AUF/ZU“ 1235000Z3EM125030G10 of 23.07.2010          |
| [D4] | 7-0010-0474_OBERTEIL_00400193.PDF                                | Mechanical drawing „OBERTEIL“ 7-0010-0474 of 05.07.2011                                          |
| [D5] | 7-0025-0505_UNTERTEIL_301164.PDF                                 | Mechanical drawing „UNTERTEIL“ 7-0025-0505 of 31.01.2008                                         |
| [D6] | 7-2070-0022_BETAETIGUNGSSPINDEL_363545.PDF                       | Mechanical drawing „BETAETIGUNGSSPINDEL“ 7-2070-0022 of 11.05.2009                               |
| [D7] | 7-0070-0317_00158694.PDF                                         | Mechanical drawing „BETAETIGUNGSSPINDEL 4222“ 7-0070-0317 of 18.05.2010                          |
| [D8] | 7-0305-0330_Druckfeder.pdf                                       | Mechanical drawing „Druckfeder“ 7-0305-0330 of 29.02.2000                                        |

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.

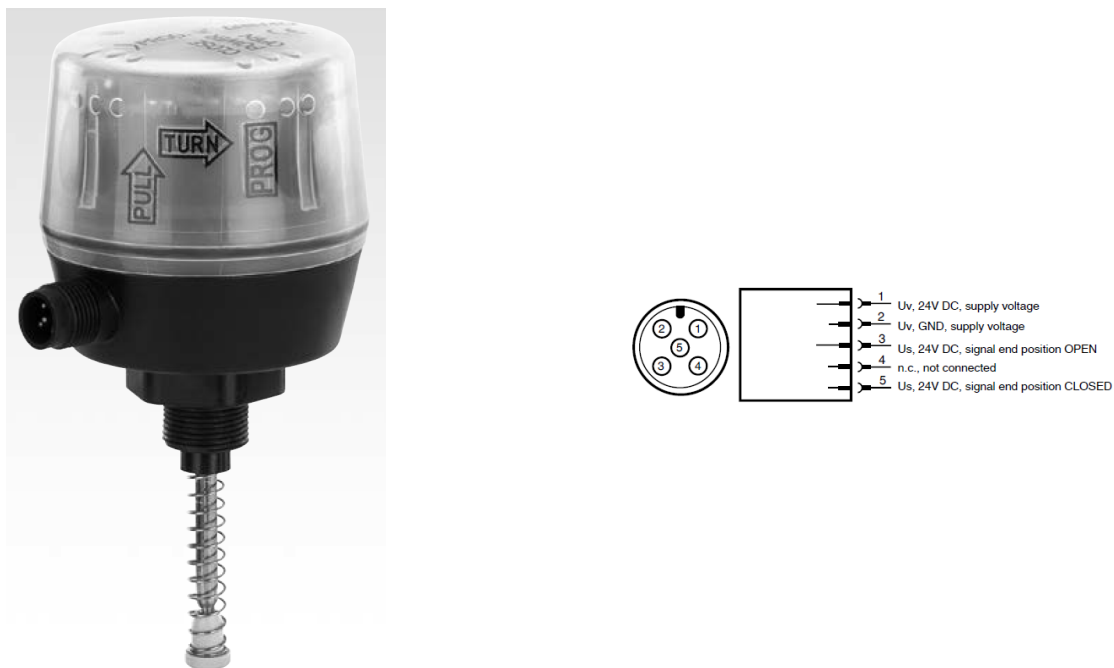
### 2.5.2 Documentation generated by *exida*

|      |                                               |
|------|-----------------------------------------------|
| [R1] | FMEDA_V8_1235_V1R0.efm of 09.07.2014          |
| [R2] | FMEDA_V8_1235_withTest_V1R0.efm of 09.07.2014 |

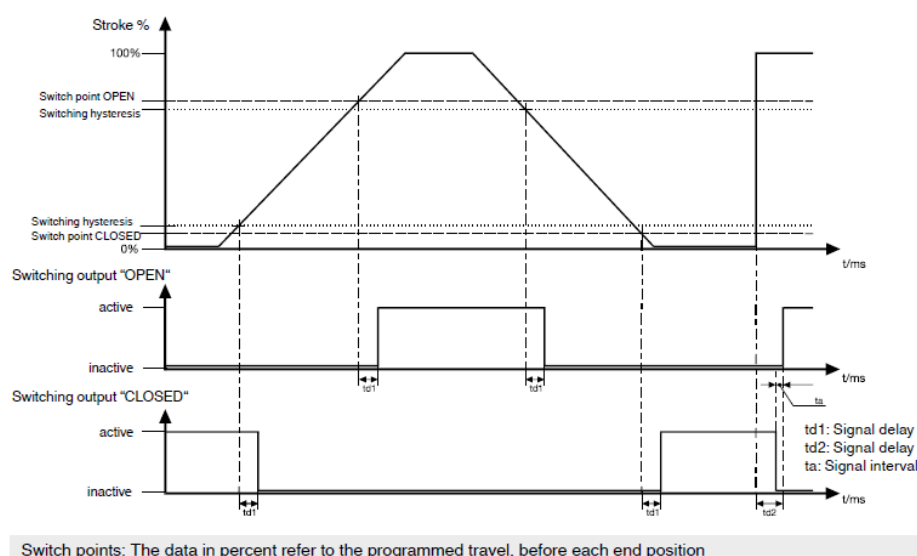
### 3 Description of the analyzed element

The Electrical Position Indicator GEMÜ 1235 can be considered to be a Type B element with a hardware fault tolerance of 0.

The Electrical Position Indicator GEMÜ 1235 is a programmable, electrical position indicator for linear actuators. It has 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. An integrated IO-Link interface offers additional parameterization and diagnostic facilities. The housing cover is made of corrosion resistant plastic and the housing base is PVDF. The protection class is IP 67.



**Figure 1: Electrical Position Indicator GEMÜ 1235 and connection diagram**



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

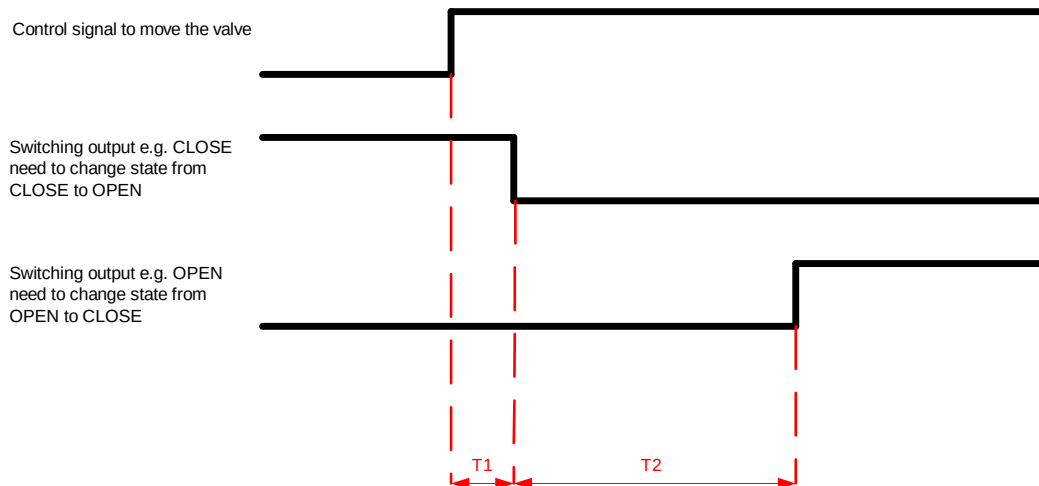


## 4 Description of diagnostic possibilities

### 4.1 Temporal and logical plausibility check

The failure rates which are listed “with test” require that the connected safety PLC 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



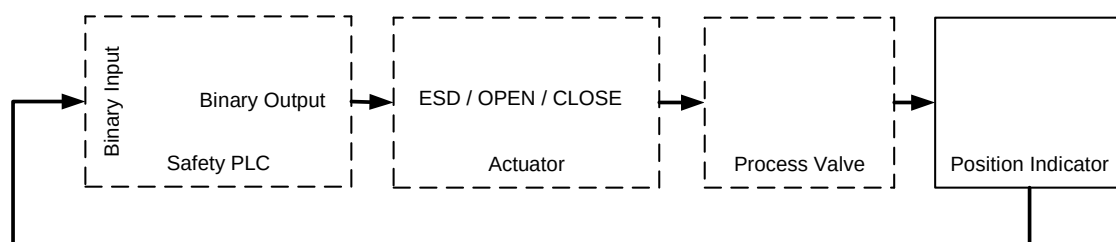
**Figure 3: Time diagram**

After the safety 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 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 [R2].

### 5.1 Description of the failure categories

In order to judge the failure behavior of the Electrical Position Indicator GEMÜ 1235, the following definitions for the failure of the products were considered.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fail-Safe State      | The fail-safe state is defined as "High" (24V) signal at Pin 5 (device version 3S) when potentiometer setting < configured threshold value (default 12%) <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) 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,</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> As long as no limit switch signal is provided it needs to be assumed that the monitored valve is not yet closed / opened which need to be considered as safe. An unintended limit switch signal would be dangerous.

## 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 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 1235.

- 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 integrated IO-Link interface is not used for any safety function but only for parameterization and diagnostic facilities.
- 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 1235 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 version is 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 Electrical Position Indicator GEMÜ 1235 is only used on linear actuators (position CLOSE / OPEN, no intermittent position).

### 5.3 Results

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

$$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

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

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 plus dangerous detected failures and safe 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 1235 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 1235

The FMEDA carried out on the Electrical Position Indicator GEMÜ 1235 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 2: Electrical Position Indicator GEMÜ 1235 – failure rates per IEC 61508:2010**

| Failure category                                                               | <i>exida</i> Profile 3 |                        |
|--------------------------------------------------------------------------------|------------------------|------------------------|
|                                                                                | Failure rates (in FIT) |                        |
|                                                                                | without test           | with test <sup>7</sup> |
| <b>Safe Detected (<math>\lambda_{SD}</math>)</b>                               | <b>0</b>               | <b>0</b>               |
| <b>Safe Undetected (<math>\lambda_{SU}</math>)</b>                             | <b>113</b>             | <b>113</b>             |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>), by external diagnostics</b> | <b>0</b>               | <b>62</b>              |
| Dangerous Detected ( $\lambda_{dd}$ )                                          | 0                      | 43                     |
| Annunciation Detected ( $\lambda_{AD}$ )                                       | 0                      | 19                     |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>)</b>                        | <b>48</b>              | <b>5</b>               |
| Annunciation Undetected ( $\lambda_{AU}$ )                                     | 21                     | 2                      |
| No effect                                                                      | 146                    | 146                    |
| No part                                                                        | 2                      | 2                      |
| <b>Total failure rate (safety function)</b>                                    | <b>161</b>             | <b>180</b>             |
| <b>SFF <sup>8</sup></b>                                                        | <b>70%</b>             | <b>97%</b>             |
| <b>DC</b>                                                                      | <b>0%</b>              | <b>93%</b>             |
| <b>MTBF</b>                                                                    | <b>346 years</b>       |                        |
| <b>SIL AC <sup>9</sup></b>                                                     | <b>SIL 1</b>           | <b>SIL 2</b>           |

<sup>7</sup> This analysis assumes that the connected safety PLC carries out a temporal and logical plausibility check on the expected signal transitions. Further details are given in section 4.1.

<sup>8</sup> The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>9</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 Using the FMEDA results

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose. The following section describes how to apply the results of the FMEDA.

### 6.1 Example $PFD_{AVG}$ / PFH calculation

The following results must be considered in combination with  $PFD_{AVG}$  / PFH values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

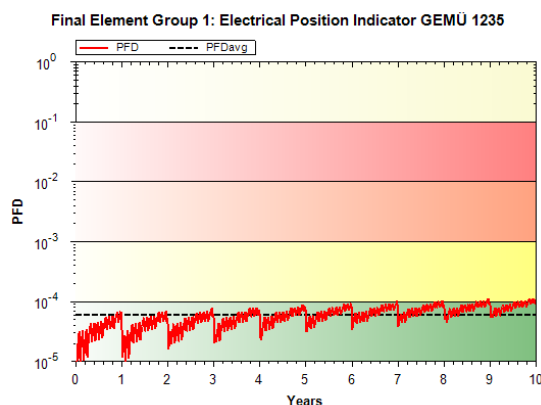
An average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is performed for a single (1001) Electrical Position Indicator GEMÜ 1235 with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 5.3.1. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 3 lists the results for different proof test intervals considering an average proof test coverage of 90% (see Appendix 1.1).

**Table 3: Electrical Position Indicator GEMÜ 1235 –  $PFD_{AVG}$  / PFH values**

| PFH                | without test           |                        | with test <sup>10</sup> |                        |
|--------------------|------------------------|------------------------|-------------------------|------------------------|
|                    | T[Proof]               |                        | T[Proof]                |                        |
|                    | 1 year                 | 2 years                | 1 year                  | 2 years                |
| PFH = 4.80E-08 1/h | $PFD_{AVG} = 3.99E-04$ | $PFD_{AVG} = 5.88E-04$ | $PFD_{AVG} = 6.00E-05$  | $PFD_{AVG} = 7.60E-05$ |

For SIL2 the overall  $PFD_{AVG}$  shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h. As the Electrical Position Indicator GEMÜ 1235 is contributing to the entire safety function it should only consume a certain percentage of the allowed range. Assuming 25% of this range as a reasonable budget it should be better than or equal to 2.50E-03 or 2.50E-07 1/h, respectively. The calculated  $PFD_{AVG}$  / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 25% of the allowed range, i.e. to be better than or equal to 2.50E-03 or 2.50E-07 1/h, respectively.

The resulting  $PFD_{AVG}$  graph with test generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 5.



**Figure 5:  $PFD_{AVG}(t)$  for Electrical Position Indicator GEMÜ 1235 with test**

<sup>10</sup> This analysis assumes that the connected safety PLC carries out a temporal and logical plausibility check on the expected signal transitions. Further details are given in section 4.1.

## 7 Terms and Definitions

|                       |                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Automatic Diagnostics | Tests performed on line 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                                                                                                                                            |
| HFT                   | Hardware Fault Tolerance<br>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. |
| 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                                                                                                                                                  |
| 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                                                                                                                                                                        |



## 8 Status of the document

### 8.1 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.

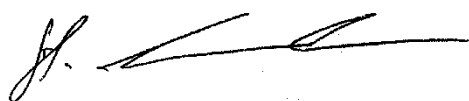
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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.

### 8.2 Releases

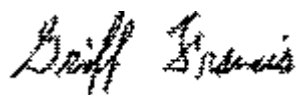
Version History: V1R0: Review comments incorporated; July 14, 2014  
V0R1: Initial version; July 9, 2014  
Authors: Stephan Aschenbrenner  
Review: V0R1: Marcus Ripsam (GEMÜ); July 11, 2014  
Griff Francis (*exida*); July 11, 2014  
Release status: Released to GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG

### 8.3 Release Signatures



---

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner



---

Griff Francis, Senior Safety Engineer

## 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 tests 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 1235 to detect a desired position and verify that the desired position is correctly indicated.                      |
| 4    | Force the Electrical Position Indicator GEMÜ 1235 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 the  $PFD_{AVG}$  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 the  $PFD_{AVG}$  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/<br>Climate Controlled | Low Power Field Mounted<br><br>no self-heating | General Field Mounted<br><br>self-heating | Subsea            | Offshore                     | N/A                 |
| <b>Description (Mechanical)</b>                                           | Cabinet mounted/<br>Climate Controlled | General Field Mounted                          | General Field Mounted                     | Subsea            | Offshore                     | Process Wetted      |
| <b>IEC 60654-1 Profile</b>                                                | B2                                     | C3<br>also applicable for D1                   | C3<br>also applicable for D1              | N/A               | C3<br>also applicable for D1 | N/A                 |
| <b>Average Ambient Temperature</b>                                        | 30C                                    | 25C                                            | 25C                                       | 5C                | 25C                          | 25C                 |
| <b>Average Internal Temperature</b>                                       | 60C                                    | 30C                                            | 45C                                       | 5C                | 45C                          | Process Fluid Temp. |
| <b>Daily Temperature Excursion (pk-pk)</b>                                | 5C                                     | 25C                                            | 25C                                       | 0C                | 25C                          | N/A                 |
| <b>Seasonal Temperature Excursion (winter average vs. summer average)</b> | 5C                                     | 40C                                            | 40C                                       | 2C                | 40C                          | 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 60068-2-6

<sup>14</sup> Vibration rating per IEC 60770-1

<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 6100-4-3

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