



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

Project:

Universal Transmitter 4114 with current output  
Universal Transmitter 4116 with current and relay output

Customer:

PR electronics A/S  
Rønde  
Denmark

Contract No.: PR Q24/12-098

Report No.: PR electronics 05/04-14 R003

Version V3, Revision R3; September, 2025

Armin Schulze, Stephan Aschenbrenner

## Management summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Universal Transmitter 4114 / 4116. Table 1 gives an overview of the considered product configurations.

A Failure Modes, Effects, and Diagnostic Analysis is one of the steps taken to achieve functional safety assessment of a device per IEC 61508 or ISO 13849. From the FMEDA, failure rates are determined and consequently the safety metrics for the corresponding standard can be calculated for a subsystem.

**Table 1: Overview of the considered product configuration**

| Product | Product description                                                      | Hardware Version | Software Version |            |
|---------|--------------------------------------------------------------------------|------------------|------------------|------------|
|         |                                                                          |                  | Input CPU        | Output CPU |
| 4114    | Universal transmitter, rail mounted with current output                  | PR4116-1-06      | 2.7              | 2.0        |
| 4116    | Universal transmitter, rail mounted with current output and relay output | PR4116-1-06      | 2.7              | 2.0        |

For safety applications only the described products with the described hardware and software versions of the Universal Transmitter 4114 / 4116 have been considered. Any other products and configurations are not covered by this report.

The Universal Transmitter 4114 / 4116 can be considered as a Type B <sup>1</sup> element with a hardware fault tolerance (HFT) of 0.

The failure modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N2] for Profile 1. They meet the *exida* criteria for Route 2<sub>H</sub> (see Appendix 4). Therefore, the Universal Transmitter 4114 / 4116 can be classified as a 2<sub>H</sub> device when the listed failure rates are used. The analysis resulted in a DC (Diagnostic Coverage) of over 60%.

The failure rates are valid for the useful life of the Universal Transmitter 4114 / 4116 (see Appendix 2) when operating as defined in the considered scenarios.

When 2<sub>H</sub> data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT = 0 for low demand mode applications or SIL 2 / SIL 3 at HFT = 1 for high and low demand mode applications.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the Universal Transmitter 4114 / 4116 with 4 ... 20 mA current output communicates detected faults by an alarm output current ≤ 3.6mA or ≥ 21mA.

Assuming that, the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

<sup>1</sup> Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

**Table 2: Summary for the Universal Transmitter 4114 / 4116 – Current output**

|                                                                      | <b>exida Profile 1 <sup>2</sup></b><br><b>IEC 61508 failure rates</b> |
|----------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Failure category</b>                                              | <b>Failure rates (in FIT)</b>                                         |
| <b>Safe Detected (<math>\lambda_{SD}</math>)</b>                     | <b>0</b>                                                              |
| <b>Safe Undetected (<math>\lambda_{SU}</math>)</b>                   | <b>0</b>                                                              |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>)</b>                | <b>401</b>                                                            |
| Fail detected (detected by internal diagnostics)                     | 196                                                                   |
| Fail Low (detected by safety logic solver)                           | 178                                                                   |
| Fail high (detected by safety logic solver)                          | 5                                                                     |
| Diagnostic faults, detected ( $\lambda_{DIAG\_D}$ ) <sup>3</sup>     | 22                                                                    |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>) <sup>4</sup></b> | <b>82</b>                                                             |
| <b>Total failure rate (safety function)</b>                          | <b>483</b>                                                            |
| <b>DC <sup>5</sup></b>                                               | <b>83 %</b>                                                           |

**Table 3: Safety metrics according to ISO 13849-1**

|                                                                             |                     |
|-----------------------------------------------------------------------------|---------------------|
| <b>MTTF<sub>D</sub> (years)</b>                                             | <b>236 (High)</b>   |
| <b>DC<sub>avg</sub></b>                                                     | <b>83 % (Low)</b>   |
| <b>Average frequency of a dangerous failure per hour (PFH) <sup>6</sup></b> | <b>8.23E-08 1/h</b> |
| <b>Performance Level (PL) <sup>7</sup></b>                                  | <b>d</b>            |

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

<sup>2</sup> For details see Appendix 3.

<sup>3</sup> As the system reaction on a detected diagnostic fault ( $\lambda_{DIAG\_D}$ ) is the same as on a dangerous detected fault ( $\lambda_{DD}$ ), a detected diagnostic fault can be considered as being a dangerous detected fault.

<sup>4</sup> The dangerous undetected faults  $\lambda_{DU}$  include 17.4 FIT transient faults (soft errors).

<sup>5</sup> According to the Route 2H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

<sup>6</sup> The PFH value of 8.23E-08 1/h is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

<sup>7</sup> The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF<sub>D</sub>, DC<sub>avg</sub> and PFH value of the device itself.

**Table 4: Summary for the Universal Transmitter 4116 – Relay output**

|                                                                      | <b>exida Profile 1<sup>8</sup></b><br><b>IEC 61508 failure rates</b> |
|----------------------------------------------------------------------|----------------------------------------------------------------------|
| <b>Failure category</b>                                              | <b>Failure rates (in FIT)</b>                                        |
| <b>Safe Detected (<math>\lambda_{SD}</math>)</b>                     | <b>0</b>                                                             |
| <b>Safe Undetected (<math>\lambda_{SU}</math>)</b>                   | <b>179</b>                                                           |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>)</b>                | <b>191</b>                                                           |
| Fail detected (detected by internal diagnostics)                     | 115                                                                  |
| Diagnostic faults, detected ( $\lambda_{DIAG\_D}$ ) <sup>9</sup>     | 76                                                                   |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>)<sup>10</sup></b> | <b>82</b>                                                            |
| <b>Total failure rate (safety function)</b>                          | <b>452</b>                                                           |
| <b>DC<sup>11</sup></b>                                               | <b>69 %</b>                                                          |

**Table 5: Safety metrics according to ISO 13849-1**

|                                                                             |                     |
|-----------------------------------------------------------------------------|---------------------|
| <b>MTTF<sub>D</sub> (years)</b>                                             | <b>418 (High)</b>   |
| <b>DC<sub>avg</sub></b>                                                     | <b>69 % (Low)</b>   |
| <b>Average frequency of a dangerous failure per hour (PFH)<sup>12</sup></b> | <b>8.22E-08 1/h</b> |
| <b>Performance Level (PL)<sup>13</sup></b>                                  | <b>d</b>            |

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

<sup>8</sup> For details see Appendix 3.

<sup>9</sup> As the system reaction on a detected diagnostic fault ( $\lambda_{DIAG\_D}$ ) is the same as on a dangerous detected fault ( $\lambda_{DD}$ ), a detected diagnostic fault can be considered as being a dangerous detected fault.

<sup>10</sup> The dangerous undetected faults  $\lambda_{DU}$  include 15.4 FIT transient faults (soft errors).

<sup>11</sup> According to the Route 2H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

<sup>12</sup> The PFH value of 8.22E-08 1/h is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

<sup>13</sup> The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF<sub>D</sub>, DC<sub>avg</sub> and PFH value of the device itself.

## 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 Product Description.....                                                               | 9  |
| 4 Failure Modes, Effects, and Diagnostic Analysis.....                                   | 11 |
| 4.1 Failure categories description .....                                                 | 11 |
| 4.2 Methodology – FMEDA, Failure rates .....                                             | 13 |
| 4.2.1 FMEDA .....                                                                        | 13 |
| 4.2.2 Failure rates .....                                                                | 13 |
| 4.2.3 Assumptions .....                                                                  | 14 |
| 4.3 FMEDA Results .....                                                                  | 15 |
| 4.3.1 Universal Transmitter 4114 / 4116 – Current output .....                           | 16 |
| 4.3.2 Universal transmitter 4116 – Relay output.....                                     | 18 |
| 4.4 Architectural Constraints .....                                                      | 20 |
| 5 Using the FMEDA results.....                                                           | 21 |
| 5.1 Example PFD <sub>AVG</sub> / PFH calculation .....                                   | 22 |
| 6 Terms and Definitions .....                                                            | 24 |
| 7 Status of the document .....                                                           | 25 |
| 7.1 Liability .....                                                                      | 25 |
| 7.2 Releases.....                                                                        | 26 |
| 7.3 Release Signatures .....                                                             | 26 |
| Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test... | 27 |
| Appendix 1.1: Possible proof tests to detect dangerous undetected faults .....           | 27 |
| Appendix 2: Impact of lifetime of critical components on the failure rate.....           | 28 |
| Appendix 3: <i>exida</i> Environmental Profiles .....                                    | 29 |
| Appendix 4: <i>exida</i> Route 2 <sub>H</sub> Criteria .....                             | 30 |
| Appendix 5: Using the FMEDA results.....                                                 | 31 |
| Appendix 5.1: Universal Transmitter 4114 / 4116 with thermocouple .....                  | 31 |
| Appendix 5.2: Universal Transmitter 4114 / 4116 with RTD .....                           | 33 |

## 1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Universal Transmitter 4114 / 4116 with hardware version PR4116-1-06 and software versions 2.7 (Input CPU) and 2.0 (Output CPU).

The FMEDA builds the basis for an evaluation whether a sensor / logic / final-element subsystem, including the product, meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) / Probability of dangerous Failure per hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 or ISO 13849.

It **does not** consider any calculations necessary for proving intrinsic safety or an evaluation of the correct device behavior in general. This FMEDA **does not** replace a full assessment according to IEC 61508 or ISO 13849.

## 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 or ISO 13849.

### 2.2 Roles of the parties involved

PR electronics A/S

Manufacturer of the  
Universal Transmitter 4114 / 4116.  
PR electronics A/S performed the original FMEDA for  
the devices under consideration.

*exida*

Reviewed the original FMEDA from PR electronics A/S  
and transferred it to the latest SILcal X format. *exida* also  
updated the related FMEDA report to the *exida* CRD  
Route 2<sub>H</sub> compliant failure rate data.

PR electronics A/S contracted *exida* in March 2025 with the update of the hardware assessment  
of the above mentioned devices.

### 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<br>Electrical/Electronic/Programmable Electronic<br>Safety-Related Systems                                             |
| [N2] | ISO 13849-1:2023                                                                                   | Safety of machinery<br>— Safety-related parts of control systems — Part 1:<br>General principles for design                                 |
| [N3] | Component Reliability<br>Database Handbook, 5th<br>Edition, 2021<br>Vol. 1 – Electrical Components | <i>exida</i> LLC, Component Reliability Database<br>Handbook, 5th Edition, 2021<br>Vol. 1 – Electrical Components<br>ISBN 978-1-934977-09-5 |

### 2.4 *exida* tools used

|      |                    |                       |
|------|--------------------|-----------------------|
| [T1] | SILcal X 1.6.4     | FMEDA Tool            |
| [T2] | exSILentia V4.14.3 | SIL Verification Tool |

## 2.5 Reference documents

### 2.5.1 Documentation provided by the customer

|      |                                              |                                                                                    |
|------|----------------------------------------------|------------------------------------------------------------------------------------|
| [D1] | 4116-1-05E-PDF.pdf<br>Rev. E of 26.06.17     | Schematic drawing                                                                  |
| [D2] | 4116SMD_2080.xlsx<br>of 17.03.23             | List of components (BOM) for<br>Universal Transmitter 4116                         |
| [D3] | 4114SMD_2032.xlsx<br>of 06.01.23             | List of components (BOM) for<br>Universal Transmitter 4114                         |
| [D4] | 4116 input modes failures.xls<br>of 27.10.05 | Overview of failure modes for multiple sensor<br>interface                         |
| [D5] | 4116-rev5 V6 R0.5.xls<br>of 21.10.05         | FMEDA results file for Universal Transmitter<br>4114 / 4116 for the current output |
| [D6] | 4116 FMEDA relay V1R0.xls<br>of 12.03.09     | FMEDA results file for<br>Universal Transmitter 4116 relay output                  |

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] | PR_4116_current_output_V2R2.xlsx<br>V2R2 of 25.04.25 | FMEDA results file for the current output<br>based on [D5] with Route 2 <sub>H</sub> compliant failure<br>rate data used from the <i>exida</i> CRD [N3].<br>Valid for Universal Transmitter 4114 / 4116. |
| [R2] | PR_4116_RE1_V2R2.xlsx<br>V2R2 of 25.04.25            | FMEDA results file for the relay output based<br>on [D6] with Route 2 <sub>H</sub> compliant failure rate<br>data used from the <i>exida</i> CRD [N3]. Valid for<br>the Universal Transmitter 4116.      |

### 3 Product Description

The Universal Transmitter 4114 / 4116 is an isolated two-wire 4 ... 20 mA device used in many different industries for both control and safety applications. The device contains an additional relay output. Combined with e.g. a temperature sensing device, the Universal Transmitter 4114 / 4116 becomes a temperature sensor assembly.



**Figure 1 Universal Transmitter 4114 / 4116**

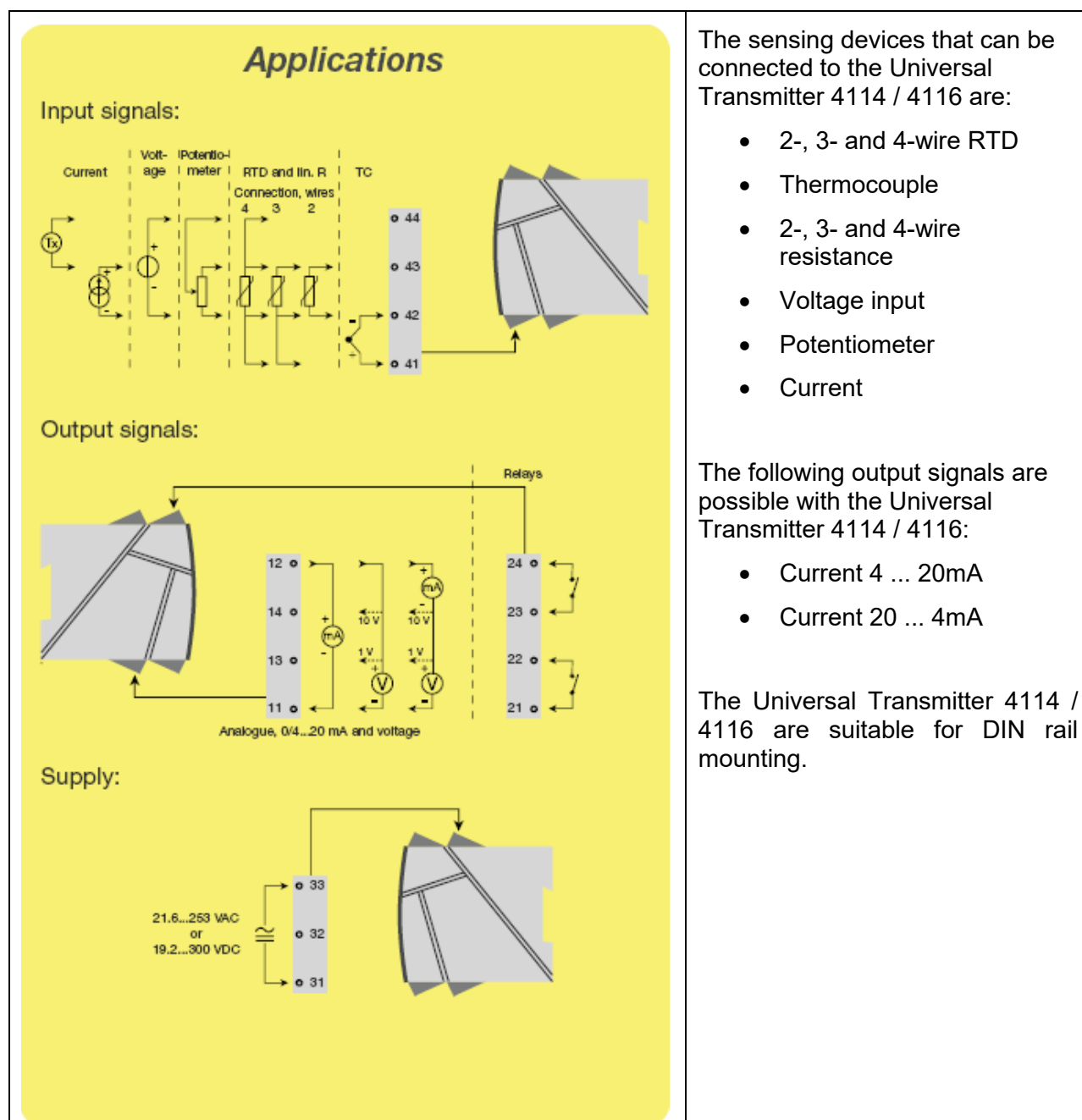
The Universal Transmitter 4114 / 4116 are configured with the interface unit 45xx which is plugged into the front of the device.

The Universal Transmitter 4114 / 4116 is classified as a Type B <sup>14</sup> element according to IEC 61508, having a hardware fault tolerance of 0.

<sup>14</sup> Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

The universal transmitter operates with a 2-wire output and with separate wires for the supply voltage. The supply voltage can be from 19.2V to 300V DC or from 21.6V to 253V AC.

This is also indicated in the following figure.



**Figure 2: Input configurations with Universal Transmitter 4114 / 4116**

The FMEDA has been performed considering the worst-case input sensor configuration.

## 4 Failure Modes, Effects, and Diagnostic Analysis

The original Failure Modes, Effects, and Diagnostic Analysis was done by **PR electronics A/S** and is documented in [D5] and [D6]. *exida* updated the failure rates from that report to the *exida* CRD (see [N3]) and created the FMEDAs documented in [R1] and [R2]. The analysis presented in this chapter is based on [R1] and [R2].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. This was then indicated in the FMEDA effects with a (TEST).

This resulted in failures that can be classified according to the following failure categories.

### 4.1 Failure categories description

In order to judge the failure behavior of the Universal Transmitter 4114 / 4116, the following definitions for the failure of the product were considered.

#### Fail-Safe State

|                       |                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------|
| Current output (Aout) | The fail-safe state is defined as the output reaching the user defined threshold value. |
| Relay output          | Relay is de-energized.                                                                  |

|                           |                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fail Safe                 | Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.                                                                                                                                                 |
| Fail Dangerous            | Failure that corrupts the measured value by more than 2% of full span (0.32mA) and therefore has the potential to not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).                                      |
| Fail Dangerous Undetected | Failure that is dangerous and that is not being diagnosed by internal diagnostics.                                                                                                                                                                        |
| Fail Dangerous Detected   | Failure that is dangerous but is detected by internal diagnostics and causes the output signal to go to the predefined alarm state.                                                                                                                       |
| Fail High                 | A fail high failure is defined as a failure that causes the output signal to go to the over-range or high alarm output current (> 21mA).                                                                                                                  |
| Fail Low                  | A fail low failure is defined as a failure that causes the output signal to go to the under-range or low alarm output current (< 3.6mA).                                                                                                                  |
| 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 and does not corrupt the measured value by more than 2% of full span (0.32mA).                                    |
| Diagnostic faults         | 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). Diagnostic faults are divided into diagnostic detected (DIAG_D) and diagnostic undetected (DIAG_U) failures. |

No Part                      Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the DC, this failure mode is not taken into account. It is also not part of the total failure rate.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment, the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The diagnostic faults are provided for those who wish to do reliability modeling more detailed than required by IEC 61508.

## 4.2 Methodology – FMEDA, Failure rates

### 4.2.1 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 under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions 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.

### 4.2.2 Failure rates

The failure modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N3] for environmental profile 1 (see Appendix 3). The rates were chosen in a way that is appropriate for safety integrity level verification calculations and the intended applications. 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 or ISO 13849 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.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power or physical abuse.

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 the failure rate applicability to any particular environment.

Accurate plant specific data may be used to check validity of the failure rate data. 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.

### 4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Universal Transmitter 4114 / 4116:

- Failure-rates are constant, wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed by manufacturers instructions.
- Failures during parameterization are not considered.
- Environmental conditions according to *exida* profile 1 as defined in Appendix 3.
- 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 internal fault detection time is 38 seconds. Therefore, a demand for the safety function in high demand mode is only possible every 3800 seconds, which corresponds to 63 minutes.
- Both modules are suitable for high demand mode of operation with a maximum demand rate of 1.5 hours.
- The safety function is carried out via 1 input and 1 output channel.
- Only the described output versions are used for safety applications.
- The related current output is used and programmed to provide 4 ... 20 mA or 20 ... 4 mA
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore, these failures have been classified as dangerous detected failures.
- When using the relay output for a safety function, and the analog output range is configured to S4-20 or S20-4 (4-20/20-4 mA with safety read-back), the output should be short-circuited or connected to a proper analog input.
- External power supply failure rates are not included.
- No inductive load.
- The relay output is protected by a fuse which initiates at 2A to avoid contact welding (this assumes that 2A is less than 60% of the rated current for the relay).
- The maximum allowed switching frequency for the relay output is 3 Hz. The user must calculate the product lifetime with respect to the relay lifetime. The relay lifetime is 100 000 switching times.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Short circuit and lead breakage detection are activated.
- Soft Error Rates (SER) were considered for relative neutron flux of 4.5 corresponding to 1,600 meters above sea.

### 4.3 FMEDA Results

For the calculations the following has to be noted:

$$\lambda_{\text{total}}^{(15)} = \lambda_{\text{SD}} + \lambda_{\text{SU}} + \lambda_{\text{DD}} + \lambda_{\text{DIAG\_D}} + \lambda_{\text{DU}}$$

#### IEC 61508:

$$\text{DC}^{(15)} = (\lambda_{\text{DD}} + \lambda_{\text{DIAG\_D}}) / (\lambda_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DIAG\_D}})$$

#### ISO 13849-1:

$$\text{MTTF}_D [\text{years}] = 1 / (\lambda_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DIAG\_D}}) * 24 * 365$$

$$\text{PFH} = \lambda_{\text{DU}}$$

$$\text{DC}_{\text{avg}}^{(15)} = (\lambda_{\text{DD}} + \lambda_{\text{DIAG\_D}}) / (\lambda_{\text{DD}} + \lambda_{\text{DU}} + \lambda_{\text{DIAG\_D}})$$

---

<sup>15</sup> As the system reaction on a detected diagnostic fault ( $\lambda_{\text{DIAG\_D}}$ ) is the same as on a dangerous detected fault ( $\lambda_{\text{DD}}$ ), a detected diagnostic fault can be considered as being a dangerous detected fault.

### 4.3.1 Universal Transmitter 4114 / 4116 – Current output

The FMEDA carried out on the Universal Transmitter 4114 / 4116, under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

| <i>exida</i> Profile 1 <sup>16</sup>                                  |                        |
|-----------------------------------------------------------------------|------------------------|
| Failure category                                                      | Failure rates (in FIT) |
| <b>Safe Detected (<math>\lambda_{SD}</math>)</b>                      | <b>0</b>               |
| <b>Safe Undetected (<math>\lambda_{SU}</math>)</b>                    | <b>0</b>               |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>)</b>                 | <b>401</b>             |
| Fail detected (detected by internal diagnostics)                      | 196                    |
| Fail low (detected by safety logic solver)                            | 178                    |
| Fail high (detected by safety logic solver)                           | 5                      |
| Diagnostic faults, detected ( $\lambda_{DIAG\_D}$ ) <sup>17</sup>     | 22                     |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>) <sup>18</sup></b> | <b>82</b>              |

|                                                       |     |
|-------------------------------------------------------|-----|
| Diagnostic faults, undetected ( $\lambda_{DIAG\_U}$ ) | 13  |
| No effect ( $\lambda_{\#}$ )                          | 163 |
| No part ( $\lambda_{-}$ )                             | 226 |

|                                             |            |
|---------------------------------------------|------------|
| <b>Total failure rate (safety function)</b> | <b>483</b> |
|---------------------------------------------|------------|

|                         |             |
|-------------------------|-------------|
| <b>DC <sup>19</sup></b> | <b>83 %</b> |
|-------------------------|-------------|

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

<sup>16</sup> For details see Appendix 3.

<sup>17</sup> As the system reaction on a detected diagnostic fault ( $\lambda_{DIAG\_D}$ ) is the same as on a dangerous detected fault ( $\lambda_{DD}$ ), a detected diagnostic fault can be considered as being a dangerous detected fault.

<sup>18</sup> The dangerous undetected faults  $\lambda_{DU}$  include 17.4 FIT transient faults (soft errors).

<sup>19</sup> According to the Route 2<sub>H</sub> approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

## Safety metrics according to ISO 13849-1

|                           |            |
|---------------------------|------------|
| MTTF <sub>D</sub> (years) | 236 (High) |
|---------------------------|------------|

|                                                                       |              |
|-----------------------------------------------------------------------|--------------|
| DC <sub>avg</sub>                                                     | 83 % (Low)   |
| Average frequency of a dangerous failure per hour (PFH) <sup>20</sup> | 8.23E-08 1/h |
| Performance Level (PL) <sup>21</sup>                                  | d            |

<sup>20</sup> The PFH value of 8.23E-08 1/h is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

<sup>21</sup> The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF<sub>D</sub>, DC<sub>avg</sub> and PFH value of the device itself.

### 4.3.2 Universal transmitter 4116 – Relay output

The FMEDA carried out on the Universal Transmitter 4116, under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

| <b>exida Profile 1 <sup>22</sup></b>                                  |                               |
|-----------------------------------------------------------------------|-------------------------------|
| <b>Failure category</b>                                               | <b>Failure rates (in FIT)</b> |
| <b>Safe Detected (<math>\lambda_{SD}</math>)</b>                      | <b>0</b>                      |
| <b>Safe Undetected (<math>\lambda_{SU}</math>)</b>                    | <b>179</b>                    |
| <b>Dangerous Detected (<math>\lambda_{DD}</math>)</b>                 | <b>191</b>                    |
| Fail detected (detected by internal diagnostics)                      | 115                           |
| Diagnostic faults, detected ( $\lambda_{DIAG\_D}$ ) <sup>23</sup>     | 76                            |
| <b>Dangerous Undetected (<math>\lambda_{DU}</math>) <sup>24</sup></b> | <b>82</b>                     |
| Diagnostic faults, undetected ( $\lambda_{DIAG\_U}$ )                 | 25                            |
| No effect ( $\lambda_{\#}$ )                                          | 150                           |
| No part ( $\lambda_{-}$ )                                             | 256                           |
| <b>Total failure rate (safety function)</b>                           | <b>452</b>                    |
| <b>DC <sup>25</sup></b>                                               | <b>69 %</b>                   |

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

<sup>22</sup> For details see Appendix 3.

<sup>23</sup> As the system reaction on a detected diagnostic fault ( $\lambda_{DIAG\_D}$ ) is the same as on a dangerous detected fault ( $\lambda_{DD}$ ), a detected diagnostic fault can be considered as being a dangerous detected fault.

<sup>24</sup> The dangerous undetected faults  $\lambda_{DU}$  include 15.4 FIT transient faults (soft errors).

<sup>25</sup> According to the Route 2<sub>H</sub> approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

## Safety metrics according to ISO 13849-1

|                           |            |
|---------------------------|------------|
| MTTF <sub>D</sub> (years) | 418 (High) |
|---------------------------|------------|

|                                                                       |              |
|-----------------------------------------------------------------------|--------------|
| DC <sub>avg</sub>                                                     | 69 % (Low)   |
| Average frequency of a dangerous failure per hour (PFH) <sup>26</sup> | 8.22E-08 1/h |
| Performance Level (PL) <sup>27</sup>                                  | d            |

<sup>26</sup> The PFH value of 8.22E-08 1/h is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

<sup>27</sup> The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF<sub>D</sub>, DC<sub>avg</sub> and PFH value of the device itself.

#### 4.4 Architectural Constraints

The architectural constraint type for the Universal Transmitter 4114 / 4116 is B. The hardware fault tolerance of the device is 0.

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 (SFF) 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 FMEDA analysis uses the 2<sub>H</sub> approach with the 2<sub>H</sub> qualified failure rates from the *exida* component reliability database [N3] (see also Appendix 4). To apply the 2<sub>H</sub> approach on a Type B device, the diagnostic coverage has to be at least 60%. Table 6 shows the FMEDA results for the diagnostic coverage for the analyzed safety outputs.

**Table 6: Diagnostic coverage for safety outputs**

| Device                            | Safety output  | Diagnostic coverage in % |
|-----------------------------------|----------------|--------------------------|
| Universal Transmitter 4114 / 4116 | Current output | 83                       |
| Universal Transmitter 4116        | Relay output   | 69                       |

The analysis shows that the current output of the Universal Transmitter 4114 / 4116 and the relay output of Universal Transmitter 4116 has a diagnostic coverage over 60%. For the current output, it is important that the logic solver is programmed to detect over-scale and under-scale outputs. Under this assumption, both safety outputs meet the hardware architectural constraints for up to SIL 2 as a single device.

When 2<sub>H</sub> data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL 2 / SIL 3 at HFT=1 for high and low demand mode applications.

As the Universal Transmitter 4114 / 4116 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

## 5 Using the FMEDA results

Using the failure rate data given in section 4.3 and the failure rate data for the associated element devices, an average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation can be performed for the entire Safety Instrumented Function (SIF).

Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

To perform an average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a  $PFD_{AVG}$  by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is best accomplished with *exida's* exSILentia tool.

The failure rates for all the devices of the Safety Instrumented Function and the corresponding proof test coverages are required to perform the  $PFD_{AVG}$  calculation. The proof test coverage of the suggested proof test for the Universal Transmitter 4114 / 4116 is listed in Appendix 1.1. This has to be combined with the dangerous failure rates after proof test for other devices to establish the proof test coverage for the entire Safety Instrumented Function.

When performing testing at regular intervals, the Universal Transmitter 4114 / 4116 contribute less to the overall  $PFD_{AVG}$  of the safety instrumented function.

The following section gives a simplified example on how to apply the results of the FMEDA.

## 5.1 Example PFD<sub>AVG</sub> / PFH calculation

An average Probability of Failure on Demand (PFD<sub>AVG</sub>) calculation is performed for a single (1oo1D) Universal Transmitter 4114 / 4116 with *exida's* exSILentia tool for both safety outputs. The failure rate data used in this calculation are given in section 4.3.

A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 7 lists the results for different proof test intervals considering an average proof test coverage of 99% from proof test 2 (see Appendix 1.1).

**Table 7: Universal Transmitter 4114 / 4116 – PFD<sub>AVG</sub> / PFH values**

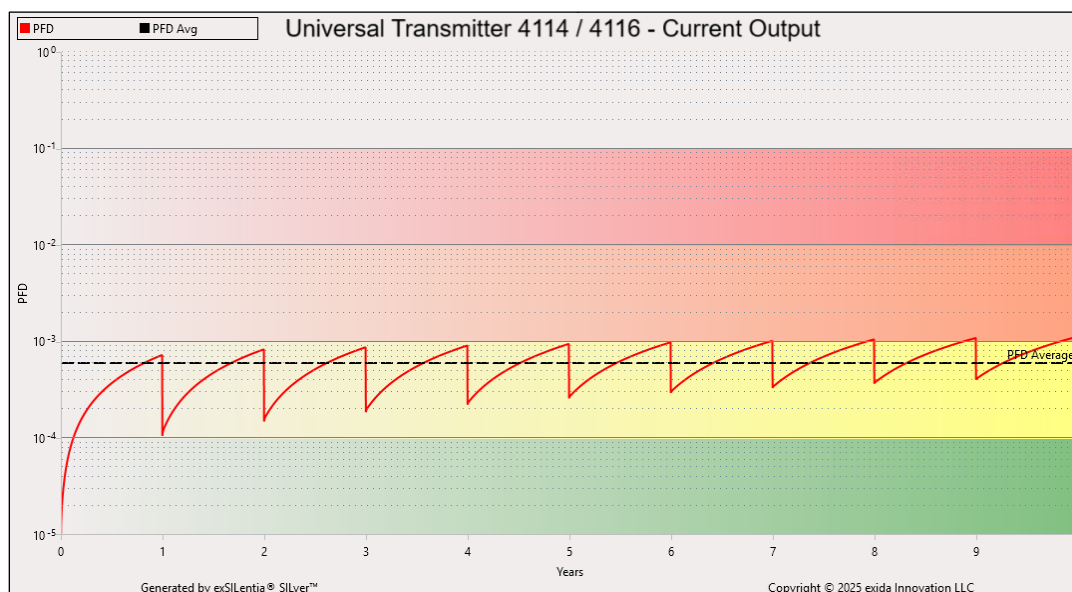
| Products    | Safety output  | PFH           | T[Proof]                       |                                |
|-------------|----------------|---------------|--------------------------------|--------------------------------|
|             |                |               | 1 year                         | 4 years                        |
| 4114 / 4116 | Current output | 8.23 E-08 1/h | PFD <sub>AVG</sub> = 6.00 E-04 | PFD <sub>AVG</sub> = 1.59 E-03 |
| 4116        | Relay output   | 8.22 E-08 1/h | PFD <sub>AVG</sub> = 5.94 E-04 | PFD <sub>AVG</sub> = 1.59 E-03 |

For SIL2 the overall PFD<sub>AVG</sub> shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h.

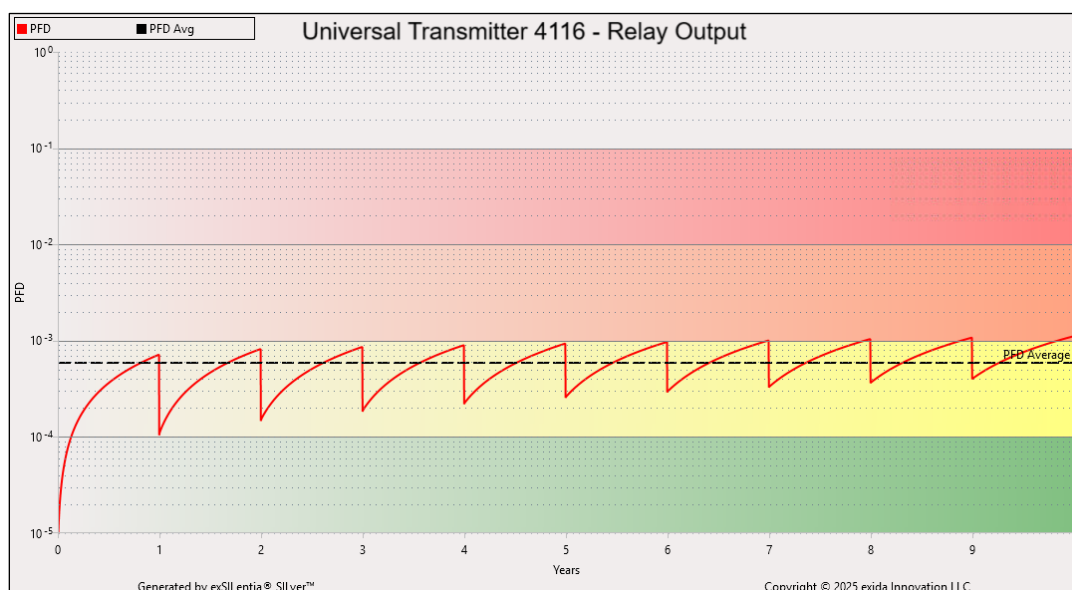
As the Universal Transmitter 4114 / 4116 is contributing to the entire safety function, it should only consume a certain percentage of the allowed range. Assuming 35% of this range as a reasonable budget, they should be better than or equal to a PFD<sub>AVG</sub> value of 3.50E-03 or a PFH value of 3.50E-07 1/h, respectively.

The calculated PFD<sub>AVG</sub> / PFH values for both safety outputs are within the allowed range for SIL 2 according to table 2 of IEC 61508-1:2010 and do fulfill the assumption to not claim more than 35% of the allowed range, i.e. to be better than or equal to 3.50E-03 or 3.50E-07 1/h, respectively.

The resulting PFD(t) / PFD<sub>AVG</sub> graph generated with exSILentia for a proof test interval of one year is displayed in Figure 3.



**Figure 3: PFD(t) / PFD<sub>AVG</sub> for current output**



**Figure 4: PFD(t) / PFD<sub>AVG</sub> for relay output**

## 6 Terms and Definitions

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internal Diagnostics   | Tests performed internally by the device or, if specified, externally by another device without manual intervention.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Fault tolerance        | Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DC / DC <sub>avg</sub> | Diagnostic Coverage of dangerous failures (in %)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 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.                                                                                                                                                                                                                                                                                                                                                                                 |
| MTTF <sub>D</sub>      | Mean Time To dangerous Failure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| PFD <sub>AVG</sub>     | Average Probability of Failure on Demand                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| PFH                    | Probability of dangerous Failure per Hour                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| PL                     | Performance Level<br>ISO 13849-1: Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.                                                                                                                                                                                                                                                                                                                                                                                         |
| SFF                    | Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.                                                                                                                                                                                                                                                                                                                                                           |
| SIF                    | Safety Instrumented Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SIL                    | Safety Integrity Level<br>IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.<br>IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest. |
| SIS                    | Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).                                                                                                                                                                                                                                                                                                                                                                                        |
| Type B element         | “Complex” element (using complex components such as 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: | V3R3:   | Updated environmental notes in chapter <i>Assumptions</i> . The environmental conditions for profile 1 defined in Appendix 3 are decisive; September 12, 2025 |
|                  | V3R2:   | Changed display name from “4501” to “45xx” as requested by PR electronics A/S; April 30, 2025                                                                 |
|                  | V3R1:   | Implemented review comments by <i>exida</i> and PR electronics A/S, included also the DIAG_D failures to calculate the DD failure rate; April 25, 2025        |
|                  | V3R0:   | Updated to IEC 61508:2010, Route 2H, also updated FMEDA report to current format; April 23, 2025                                                              |
|                  | V2R4:   | Changed assumption regarding current output when relay output is used                                                                                         |
|                  | V2R3:   | Editorial changes; April 1, 2009                                                                                                                              |
|                  | V2R2:   | Updates after review by PR electronics A/S; March 25, 2009                                                                                                    |
|                  | V2R1:   | Updated after internal <i>exida</i> review; March 25, 2009                                                                                                    |
|                  | V2R0:   | Added FMEDA analysis result for using the Universal Transmitter 4116 relay outputs in a safety function; March 20, 2009                                       |
|                  | V1R1.3: | Failure rate distribution for sensor assembly corrected; January 19, 2007                                                                                     |
|                  | V1R1.2: | Updates after review by PR electronics A/s and Stephan Aschenbrenner; January 23, 2006                                                                        |
|                  | V1R1.1: | Minor updates after review; January 09, 2006                                                                                                                  |
|                  | V1R0.0: | Updated after review; January 09, 2006                                                                                                                        |
|                  | V0R1.0: | Initial version; January 03, 2006                                                                                                                             |

Authors: Mats Gunnmarker, Jürgen Hochhaus, Armin Schulze

|         |         |                                                                                                  |
|---------|---------|--------------------------------------------------------------------------------------------------|
| Review: | V3R0:   | Stephan Aschenbrenner ( <i>exida</i> ); April 23, 2025<br>PR electronics A/S; April 24, 2009     |
|         | V2R1:   | PR electronics A/S; March 25, 2009                                                               |
|         | V2R0:   | Stephan Aschenbrenner ( <i>exida</i> ); March 23, 2009                                           |
|         | V1R1.1: | PR electronics A/S; January 17, 2006<br>Stephan Aschenbrenner ( <i>exida</i> ); January 19, 2006 |
|         | V1R1.0: | Stephan Aschenbrenner ( <i>exida</i> ); January 9, 2006                                          |
|         | V0R1.0: | Rachel Amkreutz ( <i>exida</i> ); January 6, 2006                                                |

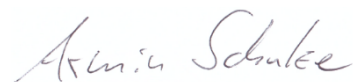
Release status: Released to PR electronics A/S

## 7.3 Release Signatures



---

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



---

Dipl.-Ing. (Univ.) Armin Schulze, 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 1.1: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 8.

**Table 8: Suggested proof test**

| Step | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Bypass the safety PLC or take other appropriate action to avoid a false trip.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2    | <p>(<b>Current output</b> usage) Use the 45xx to command the transmitter (with EN:SIM) to go to the high alarm current output and verify that the analog current reaches that value, or,</p> <p>(<b>Relay output</b> usage) Use the 45xx to command the transmitter (with EN:SIM) to go to the high alarm current output and verify that the relay is de-energized</p> <p>This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.</p> |
| 3    | <p>(<b>Current output</b> usage) Use the 45xx to command the transmitter (with EN:SIM) to go to the low alarm current output and verify that the analog current reaches that value, or,</p> <p>(<b>Relay output</b> usage) Use the 45xx to command the transmitter (with EN:SIM) to go to the low alarm current output and verify that the relay is de-energized</p> <p>This tests for possible quiescent current related failures</p>                                                                                                        |
| 4    | Restore the loop to full operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 5    | Remove the bypass from the safety PLC or otherwise restore normal operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

This test will detect approximately 50% of possible “DU” failures in the transmitter and approximately 90% of the simple sensing element “DU” failures.

Proof test 2 consists of the following steps, as described in Table 9:

**Table 9: Suggested proof test**

| Step | Action                                                                        |
|------|-------------------------------------------------------------------------------|
| 1    | Bypass the safety PLC or take other appropriate action to avoid a false trip. |
| 2    | Perform Proof Test 1.                                                         |
| 3    | Perform a two-point calibration of the transmitter.                           |
| 4    | Restore the loop to full operation.                                           |
| 5    | Remove the bypass from the safety PLC or otherwise restore normal operation.  |

This test will detect approximately 99% of possible DU failures in the transmitter and approximately 99% of the simple sensing element “DU” failures.

## 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 determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2) this only applies provided that the useful lifetime<sup>28</sup> of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the probability 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.

It is the responsibility of the end user to maintain and operate the Universal Transmitter 4114 / 4116 per manufacturer's instructions.

Note 3 in IEC 61508-2 states that experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

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

Table 10 shows the electronic parts with reduced lifetime used in the Universal Transmitter 4114 / 4116 contributing to the dangerous failure rate and therefore to the  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 10 Useful lifetime of electronic parts contributing to  $\lambda_{du}$**

| Type                                                                    | Name | Schematic          | Useful lifetime <sup>28</sup>      |
|-------------------------------------------------------------------------|------|--------------------|------------------------------------|
| Capacitor (electrolytic) - Aluminum electrolytic, non solid electrolyte | C8   | 4116-1-05E-PDF.pdf | Approx. 90 000 hours <sup>29</sup> |
| Relay                                                                   | RE1  | 4116-1-05E-PDF.pdf | Approx. 100 000 switching cycles   |

<sup>28</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.

<sup>29</sup> The operating temperature has a direct impact on this time. Therefore, already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperature follows "The doubling 10°C rule" where life is doubled for each 10°C reduction in the operating temperature.

### 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>                                        | 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>30</sup></b>                                              | 0-95% Non-Condensing                   | 0-100% Condensing                              | 0-100% Condensing                         | 0-100% Condensing | 0-100% Condensing            | N/A                 |
| <b>Shock<sup>31</sup></b>                                                 | 10 g                                   | 15 g                                           | 15 g                                      | 15 g              | 15 g                         | N/A                 |
| <b>Vibration<sup>32</sup></b>                                             | 2 g                                    | 3 g                                            | 3 g                                       | 3 g               | 3 g                          | N/A                 |
| <b>Chemical Corrosion<sup>33</sup></b>                                    | G2                                     | G3                                             | G3                                        | G3                | G3                           | Compatible Material |
| <b>Surge<sup>34</sup></b>                                                 |                                        |                                                |                                           |                   |                              | N/A                 |
| Line-Line                                                                 | 0.5 kV                                 | 0.5 kV                                         | 0.5 kV                                    | 0.5 kV            | 0.5 kV                       |                     |
| Line-Ground                                                               | 1 kV                                   | 1 kV                                           | 1 kV                                      | 1 kV              | 1 kV                         |                     |
| <b>EMI Susceptibility<sup>35</sup></b>                                    |                                        |                                                |                                           |                   |                              | N/A                 |
| 80MHz to 1.4 GHz                                                          | 10V /m                                 | 10V /m                                         | 10V /m                                    | 10V /m            | 10V /m                       |                     |
| 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>36</sup></b>                                             | 6kV                                    | 6kV                                            | 6kV                                       | 6kV               | 6kV                          | N/A                 |

<sup>30</sup> Humidity rating per IEC 60068-2-3

<sup>31</sup> Shock rating per IEC 60068-2-27

<sup>32</sup> Vibration rating per IEC 60068-2-6

<sup>33</sup> Chemical Corrosion rating per ISA 71.04

<sup>34</sup> Surge rating per IEC 61000-4-5

<sup>35</sup> EMI Susceptibility rating per IEC 6100-4-3

<sup>36</sup> ESD (Air) rating per IEC 61000-4-2

## Appendix 4: *exida* Route 2<sub>H</sub> Criteria

IEC 61508:2010 2<sup>nd</sup> edition describes the Route 2<sub>H</sub> alternative to Route 1<sub>H</sub> architectural constraints.

The standard states:

"based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to

- the amount of field feedback; and
- the exercise of **expert judgment**; and when needed
- the undertake of specific tests,

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

*exida* has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508:2010 2<sup>nd</sup> edition does not give detailed criteria for Route 2<sub>H</sub>, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" versus "systematic" are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.

## Appendix 5: Using the FMEDA results

The Universal Transmitter 4114 / 4116 together with a temperature sensing device becomes a temperature sensor assembly. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered.

### Appendix 5.1: Universal Transmitter 4114 / 4116 with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 11 and Table 12 when thermocouples are supplied with the Universal Transmitter 4114 / 4116. The drift failure mode is primarily due to T/C aging.

**Table 11: Typical failure rates for thermocouples (with extension wire)**

| <i>Thermocouple Failure Mode Distribution</i> | <i>Low Stress</i> | <i>High Stress</i> |
|-----------------------------------------------|-------------------|--------------------|
| Open Circuit                                  | 180 FIT           | 720 FIT            |
| Short Circuit                                 | 10 FIT            | 40 FIT             |
| Drift                                         | 10 FIT            | 40 FIT             |

**Table 12: Typical failure rates for thermocouples (close coupled)**

| <i>Thermocouple Failure Mode Distribution</i> | <i>Low Stress</i> | <i>High Stress</i> |
|-----------------------------------------------|-------------------|--------------------|
| Open Circuit                                  | 95 FIT            | 380 FIT            |
| Short Circuit                                 | 4 FIT             | 16 FIT             |
| Drift                                         | 1 FIT             | 4 FIT              |

**Table 13: Thermocouple fault classification according to Universal Transmitter 4114 / 4116 diagnostic capability**

| <b>Failure mode</b> | <b>Classification</b> |
|---------------------|-----------------------|
| Open circuit        | Dangerous detected    |
| Short circuit       | Dangerous undetected  |
| Drift               | Dangerous undetected  |

A complete temperature sensor assembly consisting of the Universal Transmitter 4114 / 4116 and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Assuming that the Universal Transmitter 4114 / 4116 will go to the pre-defined alarm state on detected failures of the thermocouple, the failure rate contribution for the thermocouple is:

**Table 14: Thermocouple (with extension wire)**

| Low stress environment (extension wire)                           | High stress environment (extension wire)                          |
|-------------------------------------------------------------------|-------------------------------------------------------------------|
| $\lambda_{DD} = 180 \text{ FIT}$                                  | $\lambda_{DD} = 720 \text{ FIT}$                                  |
| $\lambda_{DU} = 10 \text{ FIT} + 10 \text{ FIT} = 20 \text{ FIT}$ | $\lambda_{DU} = 40 \text{ FIT} + 40 \text{ FIT} = 80 \text{ FIT}$ |

**Table 15: Thermocouple (close coupled)**

| Low stress environment (close coupled)                         | High stress environment (close coupled)                          |
|----------------------------------------------------------------|------------------------------------------------------------------|
| $\lambda_{DD} = 95 \text{ FIT}$                                | $\lambda_{DD} = 380 \text{ FIT}$                                 |
| $\lambda_{DU} = 4 \text{ FIT} + 1 \text{ FIT} = 5 \text{ FIT}$ | $\lambda_{DU} = 16 \text{ FIT} + 4 \text{ FIT} = 20 \text{ FIT}$ |

## Appendix 5.2: Universal Transmitter 4114 / 4116 with RTD

The failure mode distribution for an RTD depends on the application with the key variables being stress level, presence (or not) of extension wire and wire configuration (2-wire/3-wire or 4-wire).

The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions are shown in Table 16 to Table 19.

**Table 16 Typical failure rates for 4-Wire RTDs (with extension wire)**

| <b>RTD Failure Mode Distribution</b> | <b>Low Stress</b> | <b>High Stress</b> |
|--------------------------------------|-------------------|--------------------|
| Open Circuit                         | 164 FIT           | 656 FIT            |
| Short Circuit                        | 8 FIT             | 32 FIT             |
| Drift                                | 28 FIT            | 112 FIT            |

**Table 17 Typical failure rates for 4-Wire RTDs (close coupled)**

| <b>RTD Failure Mode Distribution</b> | <b>Low Stress</b> | <b>High Stress</b> |
|--------------------------------------|-------------------|--------------------|
| Open Circuit                         | 41.5 FIT          | 166 FIT            |
| Short Circuit                        | 2.5 FIT           | 10 FIT             |
| Drift                                | 6 FIT             | 24 FIT             |

**Table 18 Typical failure rates for 2/3-Wire RTDs (with extension wire)**

| <b>RTD Failure Mode Distribution</b> | <b>Low Stress</b> | <b>High Stress</b> |
|--------------------------------------|-------------------|--------------------|
| Open Circuit                         | 75 FIT            | 299.5 FIT          |
| Short Circuit                        | 2 FIT             | 7.7 FIT            |
| Drift                                | 19 FIT            | 76.8 FIT           |

**Table 19 Typical failure rates for 2/3-Wire RTDs (close coupled)**

| <b>RTD Failure Mode Distribution</b> | <b>Low Stress</b> | <b>High Stress</b> |
|--------------------------------------|-------------------|--------------------|
| Open Circuit                         | 38 FIT            | 151.7 FIT          |
| Short Circuit                        | 1.4 FIT           | 5.7 FIT            |
| Drift                                | 8.6 FIT           | 34.6 FIT           |

**Table 20: RTD fault classification according to Universal Transmitter 4114 / 4116 diagnostic capability**

| <b>Failure mode</b> | <b>Classification</b> |
|---------------------|-----------------------|
| Open circuit        | Dangerous detected    |
| Short circuit       | Dangerous detected    |
| Drift (2/3-Wire)    | Dangerous undetected  |
| Drift (4-Wire)      | Dangerous undetected  |

A complete temperature sensor assembly consisting of the Universal Transmitter 4114 / 4116 and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Assuming that the Universal Transmitter 4114 / 4116 will go to the pre-defined alarm state on a detected failure of the RTD, the failure rate contribution for the RTD is:

**4-wire RTD with extension wire:**

| Low stress environment                                             | High stress environment                                             |
|--------------------------------------------------------------------|---------------------------------------------------------------------|
| $\lambda_{DD} = 164 \text{ FIT} + 8 \text{ FIT} = 172 \text{ FIT}$ | $\lambda_{DD} = 656 \text{ FIT} + 32 \text{ FIT} = 688 \text{ FIT}$ |
| $\lambda_{DU} = 28 \text{ FIT}$                                    | $\lambda_{DU} = 112 \text{ FIT}$                                    |

**4-wire RTD close coupled:**

| Low stress environment                                               | High stress environment                                             |
|----------------------------------------------------------------------|---------------------------------------------------------------------|
| $\lambda_{DD} = 41.5 \text{ FIT} + 2.5 \text{ FIT} = 44 \text{ FIT}$ | $\lambda_{DD} = 166 \text{ FIT} + 10 \text{ FIT} = 176 \text{ FIT}$ |
| $\lambda_{DU} = 6 \text{ FIT}$                                       | $\lambda_{DU} = 24 \text{ FIT}$                                     |

**2/3-wire RTD with extension wire:**

| Low stress environment                                           | High stress environment                                                  |
|------------------------------------------------------------------|--------------------------------------------------------------------------|
| $\lambda_{DD} = 75 \text{ FIT} + 2 \text{ FIT} = 77 \text{ FIT}$ | $\lambda_{DD} = 299.5 \text{ FIT} + 7.7 \text{ FIT} = 307.2 \text{ FIT}$ |
| $\lambda_{DU} = 19 \text{ FIT}$                                  | $\lambda_{DU} = 76.8 \text{ FIT}$                                        |

**2/3-wire RTD close coupled:**

| Low stress environment                                               | High stress environment                                                  |
|----------------------------------------------------------------------|--------------------------------------------------------------------------|
| $\lambda_{DD} = 38 \text{ FIT} + 1.4 \text{ FIT} = 39.4 \text{ FIT}$ | $\lambda_{DD} = 151.7 \text{ FIT} + 5.7 \text{ FIT} = 157.4 \text{ FIT}$ |
| $\lambda_{DU} = 8.6 \text{ FIT}$                                     | $\lambda_{DU} = 34.6 \text{ FIT}$                                        |