Failure Modes, Effects and Diagnostic Analysis

Project:
IR Gas Transmitter PIR 3000 with 4..20 mA current output

Customer:
Draeger Safety AG & Co. KGaA
Lübeck
Germany

Contract No.: Draeger Safety 09/05-26
Report No.: Draeger Safety 09/05-26 R015
Version V1, Revision R3; February 2010
Stephan Aschenbrenner, Alexander Dimov
Management summary

This report summarizes the results of the hardware assessment carried out on the IR Gas Transmitter PIR 3000 with 4..20 mA current output with software version 2.10.

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) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

The listed SN 29500 failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

The failure rates listed below do not include failures resulting from incorrect use of the IR Gas Transmitter PIR 3000 with 4..20 mA current output.

The IR Gas Transmitter PIR 3000 with 4..20 mA current output is considered to be a Type B¹ subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF shall be ≥ 90% for SIL 2 subsystems according to table 2 of IEC 61508-2.

It is important to realize that the “no effect” failures and the “annunciation” failures are included in the “safe” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the IR Gas Transmitter PIR 3000 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 table shows how the above stated requirements are fulfilled.

---
¹ Type B subsystem: “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.
Table 1: Summary PIR 3000 – IEC 61508 failure rates

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Failure rates (in FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SN29500</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Fail Safe Detected ($\lambda_{SD}$)</strong></td>
<td></td>
</tr>
<tr>
<td>Fail safe detected</td>
<td>0</td>
</tr>
<tr>
<td><strong>Fail Safe Undetected ($\lambda_{SU}$)</strong></td>
<td>202</td>
</tr>
<tr>
<td>Fail safe undetected</td>
<td>112</td>
</tr>
<tr>
<td>No effect</td>
<td>88</td>
</tr>
<tr>
<td>Annunciation undetected (95%)</td>
<td>2</td>
</tr>
<tr>
<td><strong>Fail Dangerous Detected ($\lambda_{DD}$)</strong></td>
<td>367</td>
</tr>
<tr>
<td>Fail detected (detected by internal diagnostics)</td>
<td>358</td>
</tr>
<tr>
<td>Fail high (detected by safety logic solver)</td>
<td>6</td>
</tr>
<tr>
<td>Annunciation detected</td>
<td>3</td>
</tr>
<tr>
<td><strong>Fail Dangerous Undetected ($\lambda_{DU}$)</strong></td>
<td>54</td>
</tr>
<tr>
<td>Fail dangerous undetected</td>
<td>54</td>
</tr>
<tr>
<td>Annunciation undetected (5%)</td>
<td>0</td>
</tr>
<tr>
<td>No part</td>
<td>48</td>
</tr>
<tr>
<td><strong>Total failure rate (safety function)</strong></td>
<td>623 FIT</td>
</tr>
<tr>
<td>SFF 3</td>
<td>91%</td>
</tr>
<tr>
<td>DCd</td>
<td>87%</td>
</tr>
<tr>
<td><strong>MTBF</strong></td>
<td>170 years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIL AC 4</th>
<th>SIL2</th>
</tr>
</thead>
</table>

A user of the IR Gas Transmitter PIR 3000 with 4..20 mA current output can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

The failure rates are valid for the useful life of the IR Gas Transmitter PIR 3000 with 4..20 mA current output (see Appendix 2).

---

2 It is assumed that complete practical fault insertion tests can confirm the assumptions made in the FMEDA.

3 The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

4 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.
# Table of Contents

Management summary .................................................................................................... 2  
1 Purpose and Scope ................................................................................................... 5  
2 Project management .................................................................................................. 6  
   2.1 exida .................................................................................................................. 6  
   2.2 Roles of the parties involved ............................................................................... 6  
   2.3 Standards / Literature used ............................................................................... 6  
   2.4 Reference documents ....................................................................................... 7  
      2.4.1 Documentation provided by the customer ............................................... 7  
      2.4.2 Documentation generated by the customer together with exida ............... 7  
3 Description of the analyzed subsystems ................................................................. 8  
   3.1 Principle of operation ....................................................................................... 8  
4 Failure Modes, Effects, and Diagnostic Analysis ....................................................... 9  
   4.1 Description of the failure categories .................................................................. 9  
   4.2 Methodology – FMEDA, Failure rates ................................................................ 10  
      4.2.1 FMEDA ..................................................................................................... 10  
      4.2.2 Failure rates ............................................................................................. 10  
      4.2.3 Assumptions ............................................................................................. 11  
   4.3 Results .............................................................................................................. 11  
      4.3.1 IR Gas Transmitter PIR 3000 with 4..20 mA current output ..................... 12  
5 Using the FMEDA results .................................................................................... 13  
   5.1 Example PFDAVG calculation ........................................................................... 13  
6 Terms and Definitions ............................................................................................ 14  
7 Status of the document ......................................................................................... 15  
   7.1 Liability ........................................................................................................... 15  
   7.2 Releases ........................................................................................................... 15  
   7.3 Release Signatures ........................................................................................... 15  
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test .. 16  
Appendix 1.1: Possible proof tests to detect dangerous undetected faults ............... 16  
Appendix 2: Impact of lifetime of critical components on the failure rate ............... 17
1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

**Option 1: Hardware assessment according to IEC 61508**

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

**Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511**

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

**Option 3: Full assessment according to IEC 61508**

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

**This assessment shall be done according to option 1.**

This document shall describe the results of the hardware assessment carried out on the IR Gas Transmitter PIR 3000 with 4..20 mA current output with software version 2.10.

The information in this report can be used to evaluate whether a sensor subsystem, including infrared gas transmitter PIR 3000 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. 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 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 partnership company with offices around the world. exida offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis 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

Draeger Safety AG & Co. KGaA Manufacturer of the IR Gas Transmitter PIR 3000 with 4..20 mA current output.

exida Performed the hardware assessment according to option 1 (see section 1) and reviewed the FMEDA provided by the customer.

Draeger Safety AG & Co. KGaA contracted exida in July 2009 with the FMEDA review of the above mentioned device.

2.3 Standards / Literature used

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

|------|-----------------|------------------------------------------------------------------------------------------|
2.4 Reference documents

2.4.1 Documentation provided by the customer

<table>
<thead>
<tr>
<th>No.</th>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D2]</td>
<td>D1750600.pdf</td>
<td>Layouts, parts lists and circuit diagram “IR-sensor (DSIR)”, 8318264 status 3 of 13.09.05</td>
</tr>
<tr>
<td>[D3]</td>
<td>D1770800.pdf</td>
<td>Layouts, parts lists and circuit diagram “Adapter (DSIR)”, 8318284 status 4 of 07.03.05</td>
</tr>
<tr>
<td>[D4]</td>
<td>D1750600.bxt / D1750601.bxt D1750602.bxt / D1770800.bxt</td>
<td>Parts list (Transmitter / Pellistor / IR-sensor / adaptive board)</td>
</tr>
</tbody>
</table>

2.4.2 Documentation generated by the customer together with exida

<table>
<thead>
<tr>
<th>No.</th>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1]</td>
<td>DSIR FMEDA 09-05-11 Transmitter.xls of July 2, 2009</td>
<td></td>
</tr>
</tbody>
</table>
3 Description of the analyzed subsystems

3.1 Principle of operation

The IR Gas Transmitter PIR 3000 with 4..20 mA current output is a gas transmitter designed to determine the concentration of gases and vapors in the ambient air. The principle of measurement is based on the concentration-dependent absorption of infrared radiation in measured gases.

The monitored ambient air diffuses through sintered material into the flameproof housing of a measuring cuvette. The broadband light emitted by the radiator passes through the gas in the cuvette and is reflected by the cuvette walls from where it is directed towards the inlet window of a dual element detector. One channel of the detector measures the gas-dependent light transmission of the cuvette (measuring channel), the other channel is used as reference.

The ratio between measuring and reference signal is used to determine the gas concentration in the cuvette. The cuvette is heated to avoid condensation of the atmosphere's moisture content. Internal electronics and software are used to calculate the concentration.

The gas transmitter is preconfigured for the gases methane, propane and ethylene. The operating range respectively comprises 0 to 100% LEL (lower explosion limit).

An analog, 4 to 20 mA output signal is used as measuring value output.

A gas sensitivity drift is very unlikely due to the infrared-optical principle of measurement and in addition, the zero point stability is enhanced by an automatic tracking system.

Figure 1: Principle of operation
4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by Draeger Safety AG & Co. KGaA. and reviewed by exida. The results are documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the IR Gas Transmitter PIR 3000 with 4..20 mA current output, the following definitions for the failure of the product were considered.

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail-Safe State</td>
<td>The fail-safe state is defined as the output being below 1.2 mA.</td>
</tr>
<tr>
<td>Fail Safe</td>
<td>Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.</td>
</tr>
<tr>
<td>Fail Dangerous</td>
<td>Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or decreases the output current by more than 20% of full scale.</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>Failure that is dangerous and that is not being diagnosed by internal diagnostics.</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>Failure that is dangerous but is detected by internal diagnostics and causes the output signal to go to the predefined alarm state.</td>
</tr>
<tr>
<td>Fail High</td>
<td>A fail high failure (H) is defined as a failure that causes the output signal to go to the over-range current (&gt; 20.5 mA) or to the high alarm output current (&gt; 20.5 mA).</td>
</tr>
<tr>
<td>No Effect</td>
<td>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 decrease the measured value by more than 20% of full scale. For the calculation of the SFF it is treated like a safe undetected failure.</td>
</tr>
<tr>
<td>Annunciation</td>
<td>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. For the calculation of the SFF they are treated to 5% as a “Dangerous Undetected” failure and to 95% as a “No Effect” failure.</td>
</tr>
<tr>
<td>No Part</td>
<td>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 SFF this failure mode is not taken into account. It is also not part of the total failure rate.</td>
</tr>
</tbody>
</table>

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508:2000.

The “No Effect” and “Annunciation Undetected” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508:2000 the “No Effect” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.
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 rate data used in this FMEDA are the basic failure rates from the Siemens standard SN 29500. 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 IEC 60654-1 class C (sheltered location). 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 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 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 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.
4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the IR Gas Transmitter PIR 3000 with 4..20 mA current output.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- Materials are compatible with process conditions.
- The measurement/application limits are considered.
- The device is installed per manufacturer’s instructions.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- 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 device is locked against unintended operation/modification.
- The worst-case internal fault detection time is 24 hours.
- The device is operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- The 4..20 mA output signal is fed to a SIL 2 compliant analog input board of a safety PLC.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with temperature limits within the manufacturer’s rating and an average temperature over a long period of time of 40°C (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed. Humidity levels are assumed within manufacturer’s rating.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- General necessary gas detection tests have successfully been passed.

4.3 Results

For the calculation of the Safe Failure Fraction (SFF) and $\lambda_{\text{total}}$ the following has to be noted:

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

$\text{SFF} = 1 - \frac{\lambda_{DU}}{\lambda_{\text{total}}}$

$\text{DCD} = \frac{\lambda_{DD}}{(\lambda_{DD} + \lambda_{DU})}$

$\text{MTBF} = \text{MTTF} + \text{MTTR} = (1 / (\lambda_{\text{total}} + \lambda_{\text{no part}})) + 24 \text{ h}$
4.3.1 IR Gas Transmitter PIR 3000 with 4..20 mA current output

The FMEDA carried out on IR Gas Transmitter PIR 3000 with 4..20 mA current output leads under the assumptions described in section 4.2.3 to the following failure rates:

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Failure rates (in FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Detected ($\lambda_{SD}$)</td>
<td></td>
</tr>
<tr>
<td>Fail safe detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Safe Undetected ($\lambda_{SU}$)</td>
<td></td>
</tr>
<tr>
<td>Fail safe undetected</td>
<td>112</td>
</tr>
<tr>
<td>No effect</td>
<td>88</td>
</tr>
<tr>
<td>Annunciation undetected (95%)</td>
<td>2</td>
</tr>
<tr>
<td>Fail Dangerous Detected ($\lambda_{DD}$)</td>
<td>367</td>
</tr>
<tr>
<td>Fail detected (detected by internal diagnostics)</td>
<td>358</td>
</tr>
<tr>
<td>Fail high (detected by safety logic solver)</td>
<td>6</td>
</tr>
<tr>
<td>Annunciation detected</td>
<td>3</td>
</tr>
<tr>
<td>Fail Dangerous Undetected ($\lambda_{DU}$)</td>
<td>54</td>
</tr>
<tr>
<td>Fail dangerous undetected</td>
<td>54</td>
</tr>
<tr>
<td>Annunciation undetected (5%)</td>
<td>0</td>
</tr>
<tr>
<td>No part</td>
<td>48</td>
</tr>
</tbody>
</table>

Total failure rate (safety function) 623 FIT

<table>
<thead>
<tr>
<th>SFF $^5$</th>
<th>91%</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC$_D$</td>
<td>87%</td>
</tr>
<tr>
<td>MTBF</td>
<td>170 years</td>
</tr>
</tbody>
</table>

SIL AC $^6$ SIL2

---

$^5$ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

$^6$ 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.
5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

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

5.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) IR Gas Transmitter PIR 3000 with 4..20 mA current output considering a proof test coverage of 95% (see Appendix 1.1) and a useful lifetime of 10 years. The failure rate data used in this calculation are displayed in section 4.3.1. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 2.

For SIL2 applications, the PFD_{AVG} value needs to be < 1.00E-02.

Table 2: PFD_{AVG} values

<table>
<thead>
<tr>
<th>T[Proof] = 1 year</th>
<th>T[Proof] = 2 years</th>
<th>T[Proof] = 5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFD_{AVG} = 3,52E-04</td>
<td>PFD_{AVG} = 5,76E-04</td>
<td>PFD_{AVG} = 1,25E-03</td>
</tr>
</tbody>
</table>

For the IR Gas Transmitter PIR 3000 with 4..20 mA current output this means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 3.5% of the allowed range.

Figure 2 shows the time dependent curve of PFD_{AVG}.
6 Terms and Definitions

DCD  Diagnostic Coverage of dangerous failures (DCD = λ_dd / (λ_dd + λ_du))
FIT  Failure In Time (1x10^-9 failures per hour)
FMEDA Failure Modes, Effects, and Diagnostic Analysis
HFT  Hardware Fault Tolerance
Low demand mode Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
MTTR  Mean Time To Restoration
PFDavg Average Probability of Failure on Demand
SFF Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF  Safety Instrumented Function
SIL  Safety Integrity Level
Type B subsystem “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof] Proof Test Interval
7 Status of the document

7.1 Liability

exida prepares FMEDA 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:  
V1R3: Editorial changes; February 19, 2010  
V1R2: Editorial changes; February 9, 2010  
V1R1: Additional external review comments incorporated; January 11, 2010  
V1R0: Review comments incorporated; December 4, 2009  
V0R1: Initial version; September 28, 2009

Authors: Stephan Aschenbrenner, Alexander Dimov

Review:  
V0R1: Rachel Amkreutz (exida); October 13, 2009  
Thomas Wiedemann (Draeger Safety); December 1, 2009

Release status: Released to Draeger Safety AG & Co. KGaA

7.3 Release Signatures

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

Rachel Amkreutz, Safety Engineer
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 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: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 3.

Table 3 Suggested proof test

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bypass the safety PLC or take other appropriate action to avoid a false trip (i.e inhibit alarms). Ensure that the functional safety is kept by other measures, such as organizational measures or safe shut-down procedures.</td>
</tr>
<tr>
<td>2</td>
<td>Apply (an) adequate gas concentration(s) above the desired alarm threshold(s), in order to go above the alarm current output(s) and verify that the analog current(s) reach(es) that value(s).</td>
</tr>
<tr>
<td>3</td>
<td>Perform a two-point calibration of the transmitter (zero-point and span calibration), if necessary.</td>
</tr>
<tr>
<td>4</td>
<td>Interrupt the signal loop to ensure fault condition alarm.</td>
</tr>
<tr>
<td>5</td>
<td>Restore the loop to full operation.</td>
</tr>
<tr>
<td>6</td>
<td>Remove the bypass from the safety PLC or otherwise restore to normal operation.</td>
</tr>
</tbody>
</table>

This test will detect more than 95% of possible "du" failures in the IR Gas Transmitter PIR 3000 with 4..20 mA current output.
Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 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 4.2.3) this only applies provided that the useful lifetime 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 – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD\textsubscript{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 4 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD\textsubscript{AVG} calculation and what their estimated useful lifetime is.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Useful life at 40°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor part</td>
<td>According to Draeger’s Specification</td>
<td></td>
</tr>
</tbody>
</table>

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

---

7 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.