



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

Project:

**Detcon DM-700 Toxic Gas/Oxygen Deficiency Sensor**

Customer:

**Detcon**

The Woodlands, TX  
USA

Contract No.: DC 06/08-04

Report No.: DC 06/08-04 R004

Version V1, Revision R2, January 5, 2012

Rudolf Chalupa

## Management summary

This report summarizes the results of the hardware assessment of the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor. The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification of a device per IEC 61508. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the DM-700, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The DM-700 is a three-wire 4 – 20 mA smart device to detect toxic or oxygen gas hazards. It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The DM-700 is classified as a Type B<sup>1</sup> device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the transmitter has a safe failure fraction between 60% and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1 as a single device. The transmitter has a safe failure fraction > 90% and can be used up to SIL2 as a single device if the 2 application restrictions listed in Section 3 of this report are met.

The failure rates for the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor are listed in Table 1 and Table 2.

**Table 1 Failure rates DM-700 with Oxygen Sensor – no restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	242
Fail Dangerous Detected	4006
Fail Detected (detected by internal diagnostics)	3933
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	1314
No Effect	217

<sup>1</sup> Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

**Table 2 Failure rates DM-700 with Toxic Gas Sensor – no restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	237
Fail Dangerous Detected	3387
Fail Detected (detected by internal diagnostics)	3314
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	1943
No Effect	228

In additions to the above failure rates, the following data are valid for applications restricted to the applications described in section 3 of this document. The failure rates for the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor are listed in Table 3 and Table 4.

**Table 3 Failure rates DM-700 with Oxygen Sensor –application restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	242
Fail Dangerous Detected	4768
Fail Detected (detected by internal diagnostics)	4695
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	553
No Effect	217

**Table 4 Failure rates DM-700 with Toxic Gas Sensor – application restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	237
Fail Dangerous Detected	4940
Fail Detected (detected by internal diagnostics)	4867
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	391
No Effect	228

Table 5 and Table 6 list the failure rates for the DM-700 according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.



**Table 5 Failure rates according to IEC 61508 – no restrictions**

Device	$\lambda_{sd}$	$\lambda_{su}^2$	$\lambda_{dd}$	$\lambda_{du}$	SFF
DM-700 with Oxygen Sensor	0 FIT	459 FIT	4006 FIT	1314 FIT	77.3%
DM-700 with Toxic Gas Sensor	0 FIT	465 FIT	3387 FIT	1943 FIT	66.5%

**Table 6 Failure rates according to IEC 61508 – application restrictions**

Device	$\lambda_{sd}$	$\lambda_{su}^3$	$\lambda_{dd}$	$\lambda_{du}$	SFF
DM-700 with Oxygen Sensor	0 FIT	459 FIT	4768 FIT	553 FIT	90.4%
DM-700 with Toxic Gas Sensor	0 FIT	465 FIT	4940 FIT	391 FIT	93.3%

These failure rates are valid for the useful lifetime of the product, see Appendix A: Lifetime of critical components.

A user of the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor 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). A full table of failure rates is presented in section 4.4 along with all assumptions.

---

<sup>2</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

<sup>3</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

## 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 Reference documents .....	8
2.4.1 Documentation provided by Detcon .....	8
2.4.2 Documentation generated by <i>exida</i> .....	8
3 Product Description.....	10
4 Failure Modes, Effects, and Diagnostics Analysis .....	11
4.1 Description of the failure categories .....	11
4.2 Methodology – FMEDA, Failure rates.....	11
4.2.1 FMEDA.....	11
4.2.2 Failure rates.....	12
4.3 Assumptions .....	12
4.4 Results.....	14
5 Using the FMEDA results.....	17
5.1 Example PFD <sub>AVG</sub> calculation for DM-700.....	17
6 Terms and Definitions .....	19
7 Status of the document .....	20
7.1 Liability .....	20
7.2 Releases.....	20
7.3 Future Enhancements.....	20
7.4 Release Signatures.....	20
Appendix A: Lifetime of critical components .....	21
Appendix B Proof test to reveal dangerous undetected faults .....	22
B.1 Suggested proof test .....	22

# 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 EN 954-1. 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 for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and 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 is an assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. 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. In addition, this option includes an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and may help justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices when combined with plant specific proven-in-use records.

## 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 EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

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

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor. From this, failure rates, Safe Failure Fraction (SFF) and example  $PFD_{AVG}$  values are calculated.

The information in this report can be used to evaluate whether a sensor subsystem, including the DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor, meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508.

## 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 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed 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

Detcon                      Manufacturer of the DM-700

*exida*                        Performed the hardware assessment per Option 1 (see Section 1)

Detcon contracted *exida* in August 2006 for the FMEDA of the DM-700.

### 2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	<i>exida</i> Mechanical Components, Rev 06-06	Mechanical components failure rate and failure modes database
[N5]	SN 29500	Failure rates of components
[N6]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N7]	Telcordia (Bellcore) Failure rate database and models	Statistical compilation of failure rate data over a wide range of applications along with models for estimating failure rates as a function of the application.
[N8]	Safety Equipment Reliability Handbook, 2003	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N9]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods
[N10]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

## 2.4 Reference documents

### 2.4.1 Documentation provided by Detcon

[D1]	DM-700_IM_R11Print.pdf, May 5, 2006	Manual, DM-700 Toxic Gas/O2 Deficiency Sensor, Document # 3207, Revision 1.1
[D2]	003077-002.pdf, August 12, 2005	Series 700 Main Processor Schematic Diagram, Revision 002
[D3]	440-003087-001.pdf, May 16.2006	Series 700 Transient Protection Schematic Diagram, Revision 1
[D4]	005089-001.pdf, Apr. 4.2006	Schematic Diagram, EC Smart Sensor, Revision 001
[D5]	003082-001.pdf, Nov. 11, 2005	Schematic Diagram (untitled), Revision 001
[D6]	003083-000.pdf, Nov. 3, 2005	Schematic Diagram, EC Sensor Interface, Revision 000

### 2.4.2 Documentation generated by *exida*

[R1]	DC 06-08-04 R004 V1 R2 DM-700.doc, 01/05/2012	FMEDA report, DM-700 Toxic Gas/O2 Deficiency Sensor (this report)
[R2]	700_Processor_FMEDA.xls, 9/13/2006	Failure Modes, Effects, and Diagnostic Analysis –Series 700 Processor Board
[R3]	700_Protection_FMEDA.xls, 8/8/2006	Failure Modes, Effects, and Diagnostic Analysis –Series 700 Transient Protection Board
[R4]	Detcon_DM-700_Toxic_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (Toxic Cartridge)
[R5]	Detcon_DM-700_Toxic_Restricted_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (Toxic Cartridge) – restricted application
[R6]	Detcon_DM-700_Bias_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (Biased Toxic Cartridge)
[R7]	Detcon_DM-700_Bias_Restricted_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (Biased Toxic Cartridge) – restricted application
[R8]	Detcon_DM-700_O2_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (O2 Cartridge)
[R9]	Detcon_DM-700_O2_Restricted_FME DA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Smart Sensor (O2 Cartridge) – restricted application

[R10]	Detcon_DM-700_IF_FMEDA.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis – DM-700 Sensor Interface Assembly
[R11]	Detcon_DM-700_Summary.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis - Summary – DM-700 Toxic Gas/O2 Deficiency Sensor
[R12]	Detcon_DM-700_Restricted_Summary.xls, Oct. 2, 2006	Failure Modes, Effects, and Diagnostic Analysis - Summary – DM-700 Toxic Gas/O2 Deficiency Sensor – restricted application

### 3 Product Description

The Detcon DM-700 Toxic Gas/Oxygen Deficiency Sensor is a gas detection system that provides continuous monitoring of gas concentration. A variety of sensor assemblies is available for various gases – see [D1] for details. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable.

The system contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. Faults and status conditions are indicated using the 4-20 mA analog signal output, see [D1].

The DM-700 is classified as a Type B<sup>4</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

In addition to the data for unrestricted application, a set of data is provided for applications conforming to the following restrictions:

1. For toxic gas sensors, combustible or toxic gas is not constantly present (e.g. for long periods of more than 24 hours).
2. For oxygen sensors, deviations from normal atmospheric concentration are being monitored and the logic solver is configured to alarm on an excess as well as a shortage of oxygen.

These application restrictions are required to detect the additional failure mode of baseline drift in the electrochemical cell.

---

<sup>4</sup> Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by exida and is documented in [R1] through [R12]. This resulted in failures that can be classified according to the following failure categories.

### 4.1 Description of the failure categories

In order to judge the failure behavior of the DM-700, the following definitions for the failure of the product were considered by Detcon.

Fail-Safe State	The fail-safe state is defined as state where the output exceeds the user defined threshold.
Fail Safe Undetected	Failure that deviates the output toward the fail-safe state but is undetected by internal diagnostics.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 10% of span away from the 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 or a connected logic solver.
Fail High	Failure that causes the output signal to go to the maximum output current ( $> 20.4\text{mA}$ )
Fail Low	Failure that causes the output signal to go to the minimum output current ( $< 4\text{mA}$ )
Fail Detected	Failure that causes the output signal to go to the predefined alarm state ( $0\text{mA}$ ).
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High, a Fail Low, or Fail Detected failure can either 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.

### 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 by exida in this FMEDA is from the exida proprietary component failure rate database derived using the IEC 62380 standard, Telcordia failure rate database/models, the SN29500 failure rate database and other sources. 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. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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.

#### 4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the DM-700.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The transmitter is used in a low-demand application such that drift beyond the safety margin will result in a negative reading or a false trip.
- The application program in the safety logic solver is configured to detect under-range (Fail Low), over-range (Fail High) and Fail Detected failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs and the diagnostic coverage provided by the online diagnostics.
- Transmitter is installed per the instructions and the requirements of the application.
- For applications utilizing the oxygen sensor, the dangerous state is defined as insufficient oxygen.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:

- IEC 60654-1, Class C with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40°C. 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 must be assumed.
- External power supply failure rates are not included.
- Recommended calibration intervals and replacement schedules of the sensor cartridge are observed and used to implement frequent proof testing of the device.
- For those tables listed as application restricted, the additional conditions listed in Section 3 apply.

#### 4.4 Results

The FMEDA described in [R1] - [R12] carried out by exida on the DM-700 and under the assumptions described in section 4.3 leads to the following failure rates. Table 7, Table 8, Table 9, and Table 10 list the failure rates for the DM-700.

**Table 7 Failure rates DM-700 with Oxygen Sensor – no restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	242
Fail Dangerous Detected	4006
Fail Detected (detected by internal diagnostics)	3933
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	1314
No Effect	217

**Table 8 Failure rates DM-700 with Oxygen Sensor –application restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	242
Fail Dangerous Detected	4768
Fail Detected (detected by internal diagnostics)	4695
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	553
No Effect	217

**Table 9 Failure rates DM-700 with Toxic Gas Sensor – no restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	237
Fail Dangerous Detected	3387
Fail Detected (detected by internal diagnostics)	3314
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	1943
No Effect	228

**Table 10 Failure rates DM-700 with Toxic Gas Sensor – application restrictions**

Failure category	Failure rate (in FIT)
Fail Safe Undetected	237
Fail Dangerous Detected	4940
Fail Detected (detected by internal diagnostics)	4867
Fail High (detected by the logic solver)	27
Fail Low (detected by the logic solver)	46
Fail Dangerous Undetected	391
No Effect	228

The failure rates that are derived from the FMEDA for the DM-700 are in a format different from the IEC 61508 format. Table 11 and Table 12 list the failure rates for DM-700 according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the DM-700 should be calculated. The SFF is the fraction of the overall failure rate of a subsystem that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formula for SFF:

$$SFF = 1 - \lambda_{du} / \lambda_{total}$$

Note that according to IEC61508 definition the No Effect failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

**Table 11 Failure rates according to IEC 61508 – no restrictions**

Device	$\lambda_{sd}$	$\lambda_{su}^5$	$\lambda_{dd}$	$\lambda_{du}$	SFF
DM-700 with Oxygen Sensor	0 FIT	459 FIT	4006 FIT	1314 FIT	77.3%
DM-700 with Toxic Gas Sensor	0 FIT	465 FIT	3387 FIT	1943 FIT	66.5%

**Table 12 Failure rates according to IEC 61508 – application restrictions**

Device	$\lambda_{sd}$	$\lambda_{su}^6$	$\lambda_{dd}$	$\lambda_{du}$	SFF
DM-700 with Oxygen Sensor	0 FIT	459 FIT	4768 FIT	553 FIT	90.4%
DM-700 with Toxic Gas Sensor	0 FIT	465 FIT	4940 FIT	391 FIT	93.3%

<sup>5</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

<sup>6</sup> It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

The architectural constraint type for DM-700 is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

## 5 Using the FMEDA results

### 5.1 Example $PFD_{AVG}$ calculation for DM-700

An example average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is performed for a single (1oo1) DM-700 Toxic Gas/O<sub>2</sub> Deficiency Sensor. The failure rate data used in this calculation is displayed in section 4.4.

The resulting  $PFD_{AVG}$  values for a variety of proof test intervals are displayed in Figure 1. As shown in Figure 1 the  $PFD_{AVG}$  value for a single DM-700 with oxygen sensor (no restrictions) with a proof test interval of 6 months equals  $2.89E-03$ . The  $PFD_{AVG}$  value for a single DM-700 with toxic gas sensor (no restrictions) with a proof test interval of 6 months equals  $4.27E-03$ . The  $PFD_{AVG}$  value for a single DM-700 with oxygen sensor (restricted application) with a proof test interval of 6 months equals  $1.23E-03$ . The  $PFD_{AVG}$  value for a single DM-700 with toxic gas sensor (restricted application) with a proof test interval of 6 months equals  $8.76E-04$ .

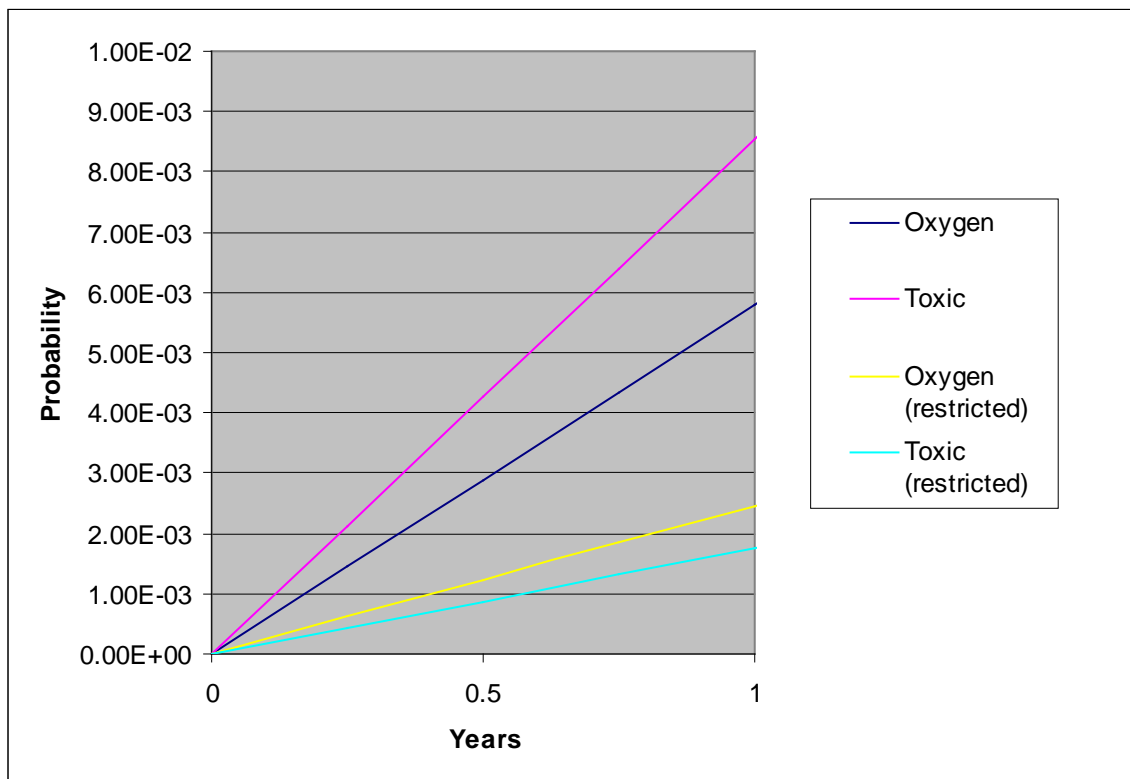


Figure 1  $PFD_{AVG}(t)$  DM-700

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF), considering the appropriate parameters such as proof test interval.

For SIL 1 applications, the  $PFD_{AVG}$  value needs to be  $\geq 10^{-2}$  and  $< 10^{-1}$ . This means that for a SIL 1 application, the  $PFD_{AVG}$  for a 6-month Proof Test Interval of the DM-700 with oxygen sensor (no restrictions) is equal to 2.9% of the range. The  $PFD_{AVG}$  for a 6-month Proof Test Interval of the DM-700 with toxic gas sensor (no restrictions) is equal to 4.3% of the range.

For SIL 2 applications, the  $PFD_{AVG}$  value needs to be  $\geq 10^{-3}$  and  $< 10^{-2}$ . This means that for a SIL 2 application, the  $PFD_{AVG}$  for a 6-month Proof Test Interval of the DM-700 with oxygen sensor (with application restrictions) is equal to 12.3% of the range. The  $PFD_{AVG}$  for a 6-month Proof Test Interval of the DM-700 with toxic gas sensor (with application restrictions) is equal to 8.8% of the range.

These 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).

## 6 Terms and Definitions

FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect 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 twice the proof test frequency.
$PFD_{AVG}$	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
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 A component	“Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

## 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.

### 7.2 Releases

Version: V1

Revision: R2

Version History: V1, R2 Clarified application restrictions, January 5, 2012  
V1, R1: Updated per review; released; October 3, 2006  
V0, R2 Added application restricted data, October 2, 2006  
V0, R1: Draft; September 28, 2006

Authors: Rudolf Chalupa

Review: V0, R2: William Goble & Greg Sauk, *exida*, October 2, 2006

Release status: Released

### 7.3 Future Enhancements

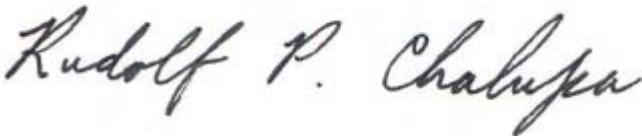
At request of client.

### 7.4 Release Signatures



---

Dr. William M. Goble, Principal Partner



---

Rudolf Chalupa, Safety Engineer

## Appendix A: Lifetime of critical components

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 4.3) this only applies provided that the useful lifetime<sup>7</sup> of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore 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  $PFD_{AVG}$  calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 13 shows which components are contributing to the dangerous undetected failure rate and therefore to the  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 13 Useful lifetime of electrolytic components contributing to  $\lambda_{du}$**

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours
Oxygen and toxic sensors	1 to 3 years – see [D1] Table 1

As there are no aluminum electrolytic capacitors used, the tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The tantalum electrolytic capacitors that are used in the DM-700 have an estimated useful lifetime of about 50 years.

Note, however, that the sensor has a much shorter life span than the electronics in the transmitter enclosure. The sensor should be replaced at an interval no longer than the expected life indicated in the manual.

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

---

<sup>7</sup> Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

## Appendix B Proof test to reveal dangerous undetected faults

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.

### B.1 Suggested proof test

A suggested proof test is described in Table 14. This test will detect approximately 99% of possible DU failures in the DM-700.

**Table 14 Steps for Proof Test**

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Calibrate the sensor per Section 3.4 of the Instruction Manual.
3.	Restore the loop to full operation.
4.	Remove the bypass from the safety PLC or otherwise restore normal operation.