
# Failure Modes, Effects and Diagnostic Analysis

Project:

**Yamatake Corporation ST 3000 Series 900 Smart Pressure Transmitter**

Customer:

Yamatake Corporation
Koza-gun, Kanagawa-ken
Japan

Contract No.: Yamatake Q06/07-35
Report No.: Yamatake 06-07-35 R002
Version V1, Revision R2, September 6, 2006
Chris O'Brien

## Management summary

This report summarizes the results of the hardware assessment of the ST 3000 Series 900 Smart Pressure Transmitter. 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 ST 3000 Pressure Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The ST 3000 Pressure Transmitter is a two-wire 4 – 20 mA smart device used to measure process pressure. The ST 3000 Pressure Transmitter 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 ST 3000 Pressure Transmitter is classified as a Type B[1] 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%[2] (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 failure rates for the ST 3000 Series 900 Smart Pressure Transmitter are listed in Table 1.

**Table 1 Failure rates ST 3000 Pressure Transmitter**

| Failure category | | Failure rate (in FIT) | |
|---|---|---|---|
| Fail Dangerous Detected | | | 380 |
| | Fail Detected (detected by internal diagnostics) | 336 | |
| | Fail High (detected by the logic solver) | 11 | |
| | Fail Low (detected by the logic solver) | 33 | |
| Fail Dangerous Undetected | | | 141 |
| No Effect | | | 99 |
| Annunciation Undetected | | | 5 |

Table 2 lists the failure rates for the ST 3000 Pressure Transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents. It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

[1] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

[2] Provided that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics.

**Table 2 Failure rates according to IEC 61508**

| Device | $\lambda_{sd}$ | $\lambda_{su}$[3] | $\lambda_{dd}$ | $\lambda_{du}$ | SFF |
|---|---|---|---|---|---|
| ST 3000 Pressure Transmitter | 0 FIT | 104 FIT | 380 FIT | 141 FIT | 77.4% |

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

A user of the ST 3000 Series 900 Smart Pressure Transmitter 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 along with all assumptions.

[3] 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**

# 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 the Failure Modes, Effects and Diagnostic Analysis carried out on the ST 3000 Series 900 Smart Pressure Transmitter. 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 (or logic / final element subsystem) 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

| | |
|---|---|
| Yamatake Corporation | Manufacturer of the ST 3000 Pressure Transmitter |
| *exida* | Performed the hardware assessment per Option 1 (see Section 1) |

Yamatake Corporation contracted *exida* in July 2006 for the FMEDA of the ST 3000 Pressure Transmitter.

## 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] | exida 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 | exida 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 Yamatake Corporation

| | | |
|---|---|---|
| [D1] | SS2-STJ100-0100 Rev 7.pdf, 10/2003 | Specification Sheet, ST 3000 Series 900 Smart Pressure Transmitter |
| [D2] | HW Block Diagragms.ppt | Hardware Block Diagram |
| [D3] | IeAput.pdf, 9/24/04 | Main circuit schematic |
| [D4] | LCD.pdf, 9/24/04 | LCD schematic |
| [D5] | Output.pdf, 9/24/04 | Output schematic |
| [D6] | Terminal.pdf, 7/2/03 | Terminal schematic |
| [D7] | Zero span adjust.pdf, 9/24/04 | Zero – span schematic |
| [D8] | Parts List.pdf | Parts List |

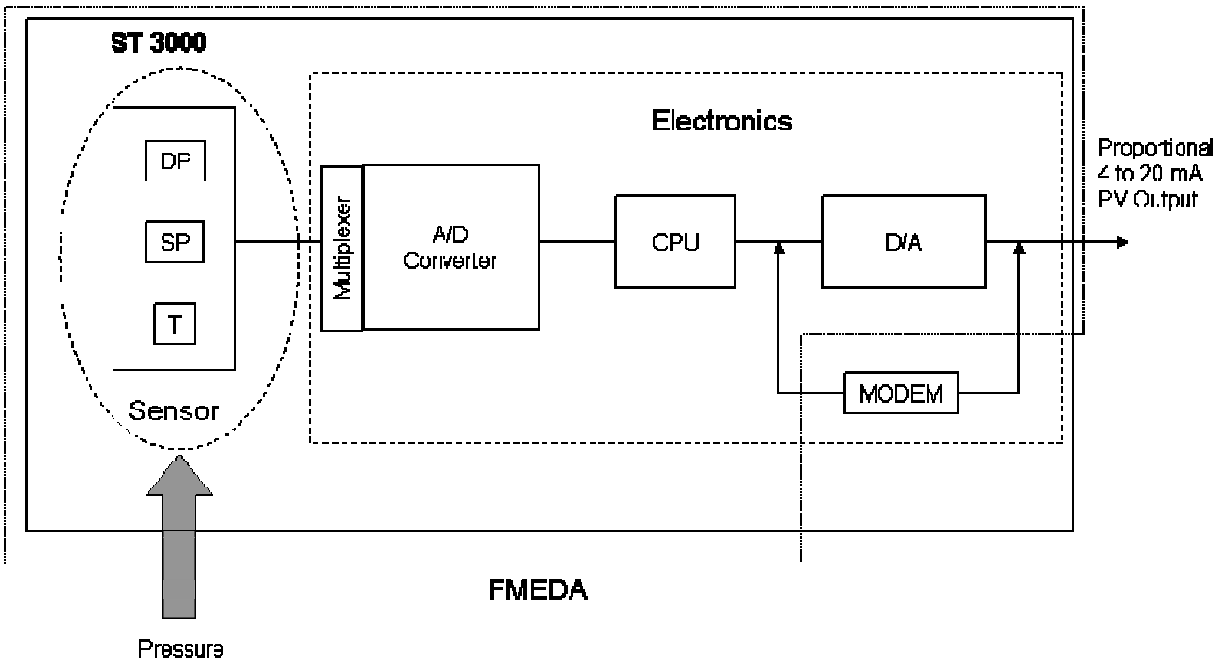
### 2.4.2 Documentation generated by *exida*

| | | |
|---|---|---|
| [R1] | Yamatake 06-07-35 R001 V1 R1 FMEDA Pressure Transmitter, 09/05/2006 | FMEDA report, ST 3000 Series 900 Smart Pressure Transmitter (this report) |
| [R2] | Yamatake PT FMEDA Summary – with proof test.xls, 9/05/06 | Failure Modes, Effects, and Diagnostic Analysis – ST 3000 Pressure Transmitter Summary |
| [R3] | Yamatake PT EMI Termination – with proof test.xls, 9/05/06 | Failure Modes, Effects, and Diagnostic Analysis – ST 3000 Pressure Transmitter Termination Board |
| [R4] | Yamatake PT Main Board – with proof test.xls, 9/05/06 | Failure Modes, Effects, and Diagnostic Analysis – ST 3000 Series 900 Smart Pressure Transmitter Main Board |
| [R5] | Yamatake PT Sensor Section – with proof test.xls, 9/05/06 | Failure Modes, Effects, and Diagnostic Analysis – ST 3000 Series 900 Smart Pressure Transmitter Sensor Assembly |

# 3 Product Description

The Yamatake Corporation ST 3000 Series 900 Smart Pressure Transmitter is a two-wire, 4 – 20 mA smart device used in many different industries for both control and safety applications. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low 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. All other output variants are not covered by this report. The different devices can be equipped with or without display. A graphical representation of the transmitter is shown in the following figure.




The ST 3000 Pressure Transmitter is classified as a Type B[4] device according to IEC 61508, having a hardware fault tolerance of 0.

The pressure transmitter can be connected to the process using an impulse line, depending on the application the clogging of the impulse lines needs to be accounted for.

[4] 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 [R5]. 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 ST 3000 Pressure Transmitter, the following definitions for the failure of the product were considered by Yamatake Corporation.

| | |
|---|---|
| Fail-Safe State | The fail-safe state is defined as state where the output exceeds the user defined threshold. |
| 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 which cause the output signal to go to the predefined alarm state (open circuit, 0mA). |
| Fail Safe Undetected | Failure that deviates the output toward the fail-safe state but is undetected by internal diagnostics. |
| Fail Safe Detected | Failure that deviates the output toward the fail-safe state but is detected by internal diagnostics which cause the output signal to go to the predefined alarm state (open circuit, 0mA). |
| Fail High | Failure that forces the output signal to go to the maximum output current (> 20.4mA). |
| Fail Low | Failure that forces the output signal to go to the minimum output current (< 4mA). |
| Fail Detected | Failure that causes the output to go to the predefined alarm state and that is detected by a connected logic solver. |
| Fail No Effect | Failure of a component that is part of the safety function but that has no effect on the safety function. |
| Annunciation Undetected | 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) and that is not detected by internal diagnostics. |

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.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected 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 by exida in this FMEDA is from the exida proprietary component failure rate database derived using the 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 ST 3000 Pressure Transmitter.

- 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 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.

- 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 40ºC. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

## 4.4 Behavior of the safety logic solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value goes below a predefined low set value. A current < 3.6 mA (Fail Low) is below the specified trip point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 21.5 mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by the connected logic solver. The PLC Detection Behavior in Table 3 represents the under-range and over-range detection capability of the connected logic solver.

**Table 3 Application Example**

| Application | PLC Detection Behavior | $\lambda_{low}$ | $\lambda_{high}$ |
|---|---|---|---|
| Low trip | <4 mA | $= \lambda^{sd}$ | $= \lambda^{du}$ |
| Low trip | >20 mA | $= \lambda^{su}$ | $= \lambda^{dd}$ |
| Low trip | <4 mA and >20 mA | $= \lambda^{sd}$ | $= \lambda^{dd}$ |
| Low trip | - | $= \lambda^{su}$ | $= \lambda^{du}$ |
| | | | |
| High trip | <4 mA | $= \lambda^{dd}$ | $= \lambda^{su}$ |
| High trip | >20 mA | $= \lambda^{du}$ | $= \lambda^{sd}$ |
| High trip | <4 mA and >20 mA | $= \lambda^{dd}$ | $= \lambda^{sd}$ |
| High trip | - | $= \lambda^{du}$ | $= \lambda^{su}$ |

In this analysis it is assumed that the logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

## 4.5 Results

The FMEDA described in [R1] – [R5] carried out by exida on the ST 3000 Pressure Transmitter and under the assumptions described in section 4.3 leads to the following failure rates.

Table 4 lists the failure rates for the ST 3000 Pressure Transmitter.

**Table 4 Failure rates ST 3000 Pressure Transmitter**

| Failure category | | Failure rate (in FIT) | |
|---|---|---|---|
| Fail Dangerous Detected | | | 380 |
| | Fail Detected (detected by internal diagnostics) | 336 | |
| | Fail High (detected by the logic solver) | 11 | |
| | Fail Low (detected by the logic solver) | 33 | |
| Fail Dangerous Undetected | | | 141 |
| No Effect | | | 99 |
| Annunciation Undetected | | | 5 |

The failure rates that are derived from the FMEDA for the ST 3000 Pressure Transmitter are in a format different from the IEC 61508 format. Table 5 lists the failure rates for ST 3000 Pressure Transmitter 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 ST 3000 Pressure Transmitter 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 and Annunciation Undetected 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 5 Failure rates according to IEC 61508**

| Device | $\lambda_{sd}$ | $\lambda_{su}$ [5] | $\lambda_{dd}$ | $\lambda_{du}$ | SFF |
|---|---|---|---|---|---|
| ST 3000 Pressure Transmitter | 0 FIT | 104 FIT | 380 FIT | 141 FIT | 77.4% |

The architectural constraint type for ST 3000 Pressure Transmitter 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] 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

# 5 Using the FMEDA results

## 5.1 Example $PFD_{AVG}$ calculation for ST 3000 Pressure Transmitter

An example average Probability of Failure on Demand ($PFD_{AVG}$) calculation is performed for a single (1oo1) ST 3000 Series 900 Smart Pressure Transmitter. The failure rate data used in this calculation is displayed in section 4.

The resulting $PFD_{AVG}$ values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the $PFD_{AVG}$ value for a single ST 3000 Pressure Transmitter with a proof test interval of 12 months equals 6.21E-04.

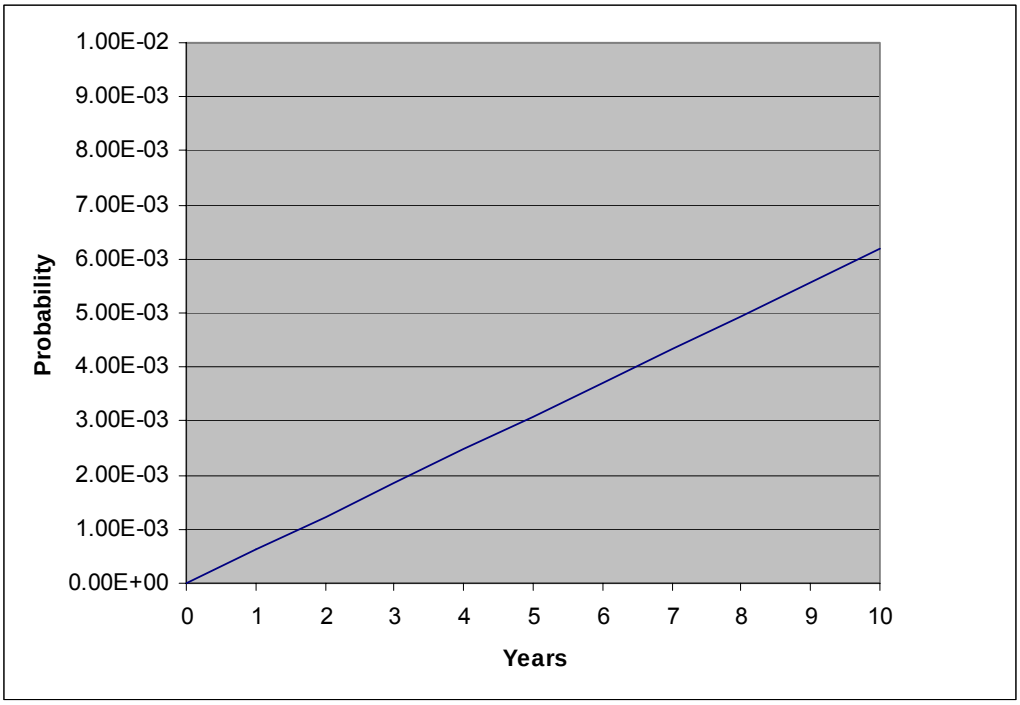



**Figure 1 $PFD_{AVG}(t)$ ST 3000 Pressure Transmitter**

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 ≥ $10^{-2}$ and < $10^{-1}$. This means that for a SIL 1 application, the $PFD_{AVG}$ for a 12 month Proof Test Interval of the ST 3000 Pressure Transmitter is equal to 0.6% 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 ($1x10^{-9}$ 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 one per year and 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: | R1 | |
| Version History: | V0, R1: | Draft; September 5, 2006 |
| | V1, R1: | Release; September 5, 2006 |
| | V1, R2: | Update to client name; September 6, 2006 |
| Authors: | Chris O'Brien | |
| Review: | V0, R1: | Bill Goble |
| Release status: | Released | |

## 7.3 Future Enhancements

At request of client.

## 7.4 Release Signatures

Dr. William M. Goble, Principal Partner

Chris O'Brien

## 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[6] 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 7 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 7 Useful lifetime of electrolytic components contributing to $\lambda_{du}$**

| Type | Useful life at 40°C |
|---|---|
| Capacitor – Solid tantalum | Approx. 500,000 Hours[7] |

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

[6] 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.

[7] The operating temperature has a direct impact on this time. Therefore a small increase in the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.

# 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 8. This test will detect approximately 88% of possible DU failures in the ST 3000 Pressure Transmitter.

**Table 8 Steps for Proof Test**

| Step | Action |
|---|---|
| 1. | Bypass the safety PLC or take other appropriate action to avoid a false trip. |
| 2. | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3. | Use HART communications to read primary pressure and secondary temperature information and verify the reasonability of these values against independent data. |
| 4. | Use HART communications to set the analog output to 3.6 mA and verify. |
| 5. | Use HART communications to set the analog output to 21.6 mA and verify. |
| 6. | Return unit to normal operation |
| 7. | Remove the bypass from the safety PLC or otherwise restore normal operation. |