



Failure Modes, Effects and Diagnostic Analysis

Project:

Rosemount 3051S HART Diagnostics Pressure Transmitter, option code DA2
Sensor Software revision 7 or 8

Company:

Rosemount, Inc.
Chanhassen, MN
USA

Contract Number: Q08/11-17

Report No.: ROS 08/11-17 R002

Version V1, Revision R2, June 11, 2010

John Grebe

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Rosemount 3051S HART Diagnostics Pressure Transmitter, option code DA2, Sensor Software revision 7 or 8. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. 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 3051S HART Diagnostics Pressure Transmitter. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 3051S HART Diagnostics Pressure Transmitter is a two-wire 4 – 20 mA smart device. 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. It utilizes the well proven Rosemount Supermodule in CAN mode feeding a Feature Board that performs advanced diagnostics. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. All other possible output variants are not covered by this report. The device can be equipped with or without display.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 3051S HART Diagnostics Pressure Transmitter.

Table 1 Version Overview

| | |
|---------------|--|
| Model 3051S_C | Rosemount 3051S HART Diagnostics Pressure Transmitter, Coplanar, Sensor Software revision 7 or 8 |
| Model 3051S_T | Rosemount 3051S HART Diagnostics Pressure Transmitter, In-Line, Sensor Software revision 7 or 8 |

The 3051S HART Diagnostics Pressure Transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The complete final element subsystem, of which the 3051S HART Diagnostics Pressure Transmitter is the final control element, will need to be evaluated to determine the Safe Failure Fraction.

The failure rates for the 3051S_C HART Diagnostic Pressure Transmitter, Coplanar configuration are listed in Table 2.

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

Table 2 Failure rates Model 3051S_C, Coplanar

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 6.2 | |
| Fail Dangerous Detected | 685.2 | |
| Fail Detected (detected by internal diagnostics) | 612.7 | |
| Fail High (detected by logic solver) | 21.6 | |
| Fail Low (detected by logic solver) | 50.9 | |
| Fail Dangerous Undetected | 31.2 | |
| Residual | 203.6 | |
| Annunciation Undetected | 30.4 | |

The failure rates for the 3051S_T HART Diagnostic Pressure Transmitter, In-Line configuration are listed in Table 3.

Table 3 Failure rates Model 3051S_T, In-Line

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 6.2 | |
| Fail Dangerous Detected | 681.2 | |
| Fail Detected (detected by internal diagnostics) | 608.7 | |
| Fail High (detected by logic solver) | 21.6 | |
| Fail Low (detected by logic solver) | 50.9 | |
| Fail Dangerous Undetected | 31.4 | |
| Residual | 188.6 | |
| Annunciation Undetected | 32.3 | |

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

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 4 lists the failure rates for the 3051S HART Diagnostics Pressure Transmitter according to IEC 61508.

Table 4 Failure rates according to IEC 61508

| Device | λ_{SD} | λ_{SU}^2 | λ_{DD} | λ_{DU} | SFF ³ |
|---------------|----------------|------------------|----------------|----------------|------------------|
| Model 3051S_C | 0 FIT | 240.2 FIT | 685.2FIT | 31.2 FIT | 96.7% |
| Model 3051S_T | 0 FIT | 227.0 FIT | 681.2 FIT | 31.4 FIT | 96.7% |

A user of the 3051S HART Diagnostics 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 4.4 along with all assumptions.

² It is important to realize that the Residual 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

³ Safe Failure Fraction needs to be calculated on (sub)system level



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 and Literature used | 7 |
| 2.4 Reference documents | 8 |
| 3 Product Description | 9 |
| 4 Failure Modes, Effects, and Diagnostic Analysis | 11 |
| 4.1 Failure Categories description | 11 |
| 4.2 Methodology – FMEDA, Failure Rates | 12 |
| 4.3 Assumptions | 13 |
| 4.4 Results | 14 |
| 5 Using the FMEDA Results | 16 |
| 5.1 Impulse line clogging | 16 |
| 5.2 PFD _{AVG} Calculation 3051S HART Diagnostics Pressure Transmitter | 16 |
| 6 Terms and Definitions | 18 |
| 7 Status of the Document | 19 |
| 7.1 Liability | 19 |
| 7.2 Releases | 19 |
| 7.3 Future Enhancements | 19 |
| 7.4 Release Signatures | 20 |
| Appendix A Lifetime of Critical Components | 21 |
| Appendix B Proof tests to reveal dangerous undetected faults | 22 |
| B.1 Simple Proof Test | 22 |
| B.2 Comprehensive Proof Test | 22 |
| Appendix C: Common Cause for redundant configurations | 24 |

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 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 per 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 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 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 in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 3051S HART Diagnostics 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 subsystem meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.



2 Project Management

2.1 *exida*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle 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

| | |
|-----------------|---|
| Rosemount, Inc. | Manufacturer of the 3051S HART Diagnostics Pressure Transmitter |
| <i>exida</i> | Performed the hardware assessment according to Option 1 (see Section 1) |

Rosemount, Inc. contracted *exida* in May 2009 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

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

| | | |
|------|---|--|
| [N1] | IEC 61508-2: 2000 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |
| [N2] | Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008 | <i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6 |
| [N3] | Safety Equipment Reliability Handbook, 3rd Edition, 2007 | <i>exida</i> L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7 |
| [N4] | Goble, W.M. 1998 | Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods |
| [N5] | IEC 60654-1:1993-02, second edition | Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition |
| [N6] | Goble, W.M. and Cheddie, H., 2005 | Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISA, ISBN 1-55617-909-X |

2.4 Reference documents

2.4.1 Documentation provided by Rosemount, Inc.

| | | |
|------|---|--|
| [D1] | 3051S_hdpt_sirs.doc | Safety Integrity Requirements Specification, 3051S HART Diagnostics Pressure Transmitter Phase 2, Revision B.1 |
| [D2] | 3051S_hdpt_srs.doc | Software Requirements Specification, 3051S Hart Diagnostic Pressure Transmitter Phase 2, Revision G.6 |
| [D3] | 03151-3610AA.pdf | Schematic, Feature Bd, HART Diagnostic, Drawing No. 03151-36100010, Rev. AA |
| [D4] | 03151-4214 transient Terminal Block.pdf | Schematic, Transient Terminal Block, Drawing No. 03051-4214, Rev. AA |
| [D5] | 03151-4211 standard Terminal Block.pdf | Schematic, Terminal Block – Standard, Drawing No. 03051-4211, Rev. AB |

2.4.2 Documentation generated by *exida*

| | | |
|------|---|---|
| [R1] | Rosemount Phase 2 HART Diagnostic Feature Board 05262010.efm | Failure Modes, Effects, and Diagnostic Analysis – 3051S HART Diagnostics Pressure Transmitter |
| [R2] | CAN Mode SM Coplanar II 3051S ROM 6_7.xls | Failure Modes, Effects, and Diagnostic Analysis – 3051S HART Diagnostics Pressure Transmitter |
| [R3] | CAN Mode SM Inline 3051T ROM6_7.xls | Failure Modes, Effects, and Diagnostic Analysis – 3051S HART Diagnostics Pressure Transmitter |
| [R4] | Summary Sheet - Phase 2 3051S HART Diagnostic Pressure Transmitter 05262010.xls | Failure Modes, Effects, and Diagnostic Analysis - Summary – 3051S HART Diagnostics Pressure Transmitter |
| [R5] | ROS 08-11-17 R002 V1 R2 FMEDA Model 3051S HART ROM 6_7.doc, 06/11/2010 | FMEDA report, 3051S HART Diagnostics Pressure Transmitter (this report) |

3 Product Description

The Rosemount 3051S HART Diagnostics Pressure Transmitter, option code DA2 is a two-wire 4 – 20 mA smart device used in multiple industries for both control and safety applications. The transmitter consists of a standard well proven Rosemount Supermodule in combination with a Hart Diagnostic Pressure Transmitter (HDPT) Feature Board that performs advanced process diagnostics. It 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. No other output variants are covered by this report.

Figure 1 provides an overview of the 3051S HART Diagnostics Pressure Transmitter and the boundary of the FMEDA.

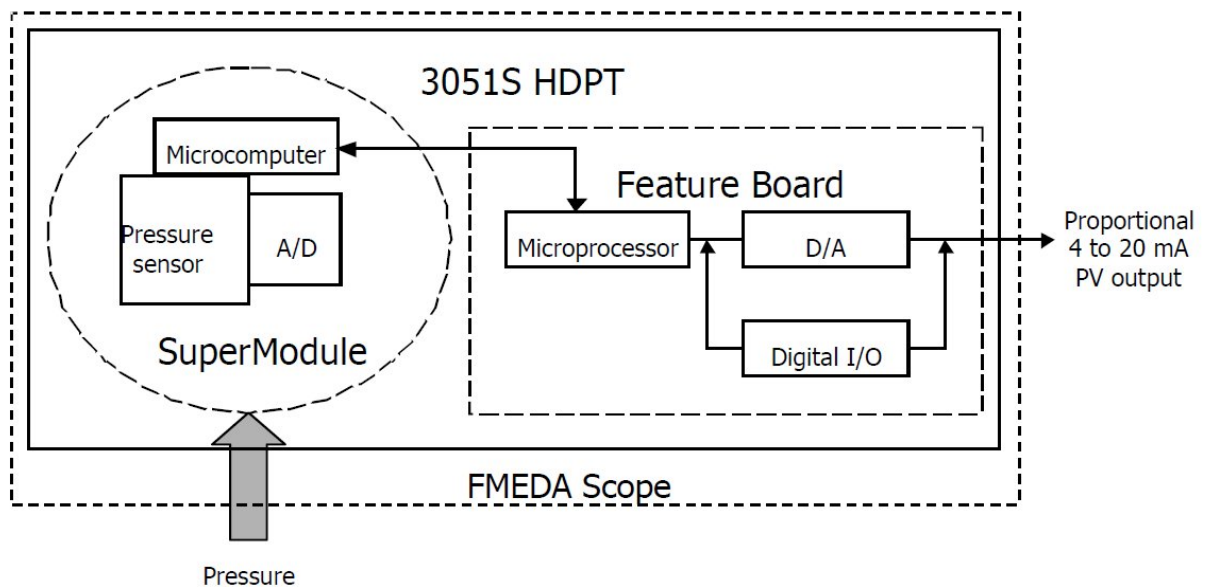


Figure 1 3051S HART Diagnostics Pressure Transmitter, Parts included in the FMEDA - transmitter

The FMEDA has been performed for two different configurations of the 3051S HDPT Pressure Transmitter, i.e. Coplanar, and In-Line configuration. Table 5 gives an overview of the different versions that were considered in the FMEDA of the 3051S HART Diagnostics Pressure Transmitter.

Table 5 Version Overview

| | |
|---------------|--|
| Model 3051S_C | Rosemount 3051S HART Diagnostics Pressure Transmitter, Coplanar, Sensor Software revision 7 or 8 |
| Model 3051S_T | Rosemount 3051S HART Diagnostics Pressure Transmitter, In-Line, Sensor Software revision 7 or 8 |



The 3051S HART Diagnostics Pressure Transmitter is classified as a Type B⁴ device according to IEC 61508, having a hardware fault tolerance of 0.

The 3051S HDPT Pressure Transmitter can be connected to the process using an impulse line, depending on the application the clogging of the impulse line needs to be accounted for, see section 5.1.

⁴ Type B device: “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 Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Rosemount, Inc. and is documented in [D1] through [D5].

4.1 Failure Categories description

In order to judge the failure behavior of the 3051S HART Diagnostics Pressure Transmitter, the following definitions for the failure of the device were considered.

| | |
|---------------------------|---|
| Fail-Safe State | State where the output exceeds the user defined threshold |
| Fail Safe | Failure that causes the device to go to the defined fail-safe state without a demand from the process. |
| Fail Detected | Failure that causes the output signal to go to the predefined alarm state. |
| Fail Dangerous | Failure that deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale |
| Fail Dangerous Undetected | Failure that is dangerous and that is not being diagnosed by automatic diagnostics |
| Fail Dangerous Detected | Failure that is dangerous but is detected by automatic diagnostics which cause the output signal to go to the predefined alarm state. |
| Fail High | Failure that causes the output signal to go to the over-range or high alarm output current (≥ 21.75 mA) |
| Fail Low | Failure that causes the output signal to go to the under-range or low alarm output current (≤ 3.75 mA) |
| Residual | 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 IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2000, the Residual 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.

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

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

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 in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) 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 Electrical and Mechanical Component Reliability Handbook which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 2, see Table 6. 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.

Table 6 exida Environmental Profiles

| EXIDA ENVIRONMENTAL PROFILE | GENERAL DESCRIPTION | PROFILE PER IEC 60654-1 | AMBIENT TEMPERATURE [°C] | | TEMP CYCLE [°C / 365 DAYS] |
|---|---|-------------------------|--------------------------|-------------------|----------------------------|
| | | | AVERAGE (EXTERNAL) | MEAN (INSIDE BOX) | |
| 1 Cabinet Mounted Equipment | Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings | B2 | 30 | 60 | 5 |
| 2 Low Power /Mechanical Field Products | Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings | C3 | 25 | 30 | 25 |
| 3 General Field Equipment | General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings | C3 | 25 | 45 | 25 |
| 4 Unprotected Mechanical Field Products | Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation. | D1 | 25 | 30 | 35 |

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

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 3051S HART Diagnostics Pressure Transmitter.

- Only a single component failure will fail the entire 3051S HART Diagnostics Pressure Transmitter
- 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 stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 with temperature limits within the manufacturer’s rating. Other environmental characteristics are assumed to be within manufacturer’s rating.
- 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
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions
- The device is installed per manufacturer’s instructions
- External power supply failure rates are not included
- Worst-case internal fault detection time is 30 seconds

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 3051S HART Diagnostics Pressure Transmitter FMEDA.

The failure rates for the 3051S_C HART Diagnostic Pressure Transmitter, Coplanar configuration are listed in Table 7.

Table 7 Failure rates Model 3051S_C, Coplanar

| Failure Category | Failure Rate (FIT) |
|--|--------------------|
| Fail Safe Undetected | 6.2 |
| Fail Dangerous Detected | 685.2 |
| Fail Detected (detected by internal diagnostics) | 612.7 |
| Fail High (detected by logic solver) | 21.6 |
| Fail Low (detected by logic solver) | 50.9 |
| Fail Dangerous Undetected | 31.2 |
| Residual | 203.6 |
| Annunciation Undetected | 30.4 |

The failure rates for the 3051S_T HART Diagnostic Pressure Transmitter, In-Line configuration are listed in Table 8.

Table 8 Failure rates Model 3051S_T, In-Line

| Failure Category | Failure Rate (FIT) |
|--|--------------------|
| Fail Safe Undetected | 6.2 |
| Fail Dangerous Detected | 681.2 |
| Fail Detected (detected by internal diagnostics) | 608.7 |
| Fail High (detected by logic solver) | 21.6 |
| Fail Low (detected by logic solver) | 50.9 |
| Fail Dangerous Undetected | 31.4 |
| Residual | 188.6 |
| Annunciation Undetected | 32.3 |

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

Table 9 lists the failure rates for the 3051S HART Diagnostics Pressure Transmitter according to IEC 61508. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF: $SFF = 1 - \lambda_{DU} / \lambda_{TOTAL}$

Table 9 Failure rates according to IEC 61508

| Device | λ_{SD} | λ_{SU}^5 | λ_{DD} | λ_{DU} | SFF ⁶ |
|---------------|----------------|------------------|----------------|----------------|------------------|
| Model 3051S_C | 0 FIT | 240.2 FIT | 685.2FIT | 31.2 FIT | 96.7% |
| Model 3051S_T | 0 FIT | 227.0 FIT | 681.2 FIT | 31.4 FIT | 96.7% |

The architectural constraint type for the 3051S HART Diagnostics Pressure Transmitter is B. The hardware fault tolerance of the device is 0. 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 Residual 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

⁶ Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 Impulse line clogging

The transmitter can be connected to the process using impulse lines; depending on the application, the analysis needs to account for clogging of the impulse lines. The 3051S HART Diagnostics Pressure Transmitter failure rates that are displayed in section 4.4 are failure rates that reflect the situation where the transmitter is used in clean service. Clean service indicates that failure rates due to clogging of the impulse line are not counted. For applications other than clean service, the user must estimate the failure rates for the clogged impulse line and add this failure rate to the 3051S HART Diagnostics Pressure Transmitter failure rates.

5.2 PFD_{AVG} Calculation 3051S HART Diagnostics Pressure Transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) 3051S HART Diagnostics Pressure Transmitter for models 3501S_C and 3051S_T. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. For the proof tests the comprehensive proof test coverage of 87% has been assumed, see Appendix A.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 2. As shown in the graph the PFD_{AVG} value for a single 3051S HART Diagnostics Pressure Transmitter Model 3051S_C, with a proof test interval of 1 year equals 3.13E-04. The PFD_{AVG} value for a single 3051S HART Diagnostics Pressure Transmitter Model 3051S_T, with a proof test interval of 1 year equals 3.15E-04.

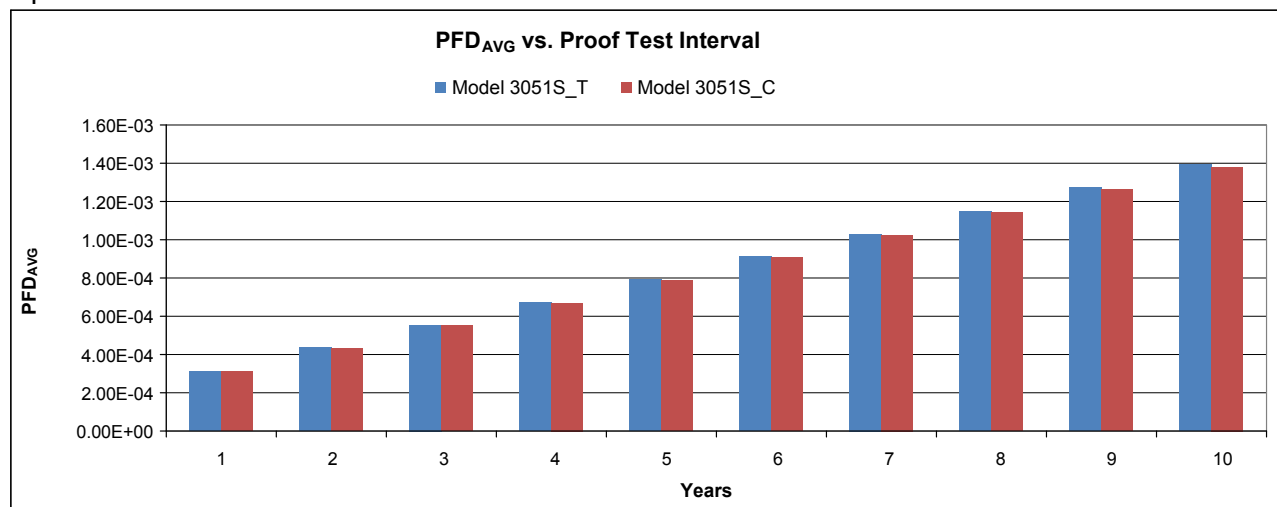


Figure 2 $PFD_{AVG}(t)$ 3051S HART Diagnostics Pressure Transmitter

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.

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 1-year Proof Test Interval of the 3051S HART Diagnostics Pressure Transmitter of either model is approximately equal to 3.1% 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 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” component (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2 |
| Type B component | “Complex” component (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.

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: V1

Revision: R2

Version History: V0, R0: Draft; June 10, 2009

V0, R1: Updated to reflect changes to default diagnostic; October 21, 2009

V1, R0: Updated based on Fault Injection results; November 25, 2009

V1, R1: Updated per review, December 1, 2009

V1, R2 Updated after fault injection testing

Author(s): John Grebe

Review: V1, R0: William M. Goble (*exida*)

Release Status: Released

7.3 Future Enhancements

At request of client.



7.4 Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble", written above a solid black horizontal line.

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "John C. Grebe Jr.", written above a solid black horizontal line.

John C. Grebe Jr., Principal 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 4.2.2) this only applies provided that the useful lifetime⁷ 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 subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the 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 10 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 10 Useful lifetime of components contributing to dangerous undetected failure rate

| Component | Useful Life |
|---|-----------------------|
| Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte | Approx. 500,000 hours |

It is the responsibility of the end user to maintain and operate the 3051S HART Diagnostics Pressure Transmitter per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

As there are no aluminum electrolytic capacitors used, the limiting factors with regard to the useful lifetime of the system are the Tantalum electrolytic capacitors. The Tantalum electrolytic capacitors have an estimated useful lifetime of about 50 years.

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.

Appendix B Proof tests 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 Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Simple Proof Test

The simple suggested proof test consists of a power cycle plus reasonability checks of the transmitter output. This test will detect ~ 41% of possible DU failures in the device.

Table 11 Simple Proof Test

| Step | Action |
|------|--|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip |
| 2. | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3. | Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value ⁸ . |
| 4. | Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ⁹ . |
| 5. | Perform a “reasonability check” on the pressure sensor reading and the sensor temperature sensor ¹⁰ . |
| 6. | Remove the bypass and otherwise restore normal operation |

B.2 Comprehensive Proof Test

The comprehensive proof test consists of performing the same steps as the simple suggested proof test but with a two point calibration of the pressure and temperature sensors in place of the reasonability check of the sensors. This test will detect ~ 87% of possible DU failures in the device.

Table 12 Comprehensive Proof Test

| Step | Action |
|------|---|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip |
| 2. | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3. | Send a HART command to the transmitter to go to the high alarm current output and |

⁸ This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

⁹ This tests for possible quiescent current related failures.

¹⁰ This tests for faults in the input multiplexer and A to D converter.

| | |
|----|--|
| | verify that the analog current reaches that value ¹¹ . |
| 4. | Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ¹² . |
| 5. | Perform a two-point calibration ¹³ of the transmitter over the full working range. |
| 6. | Remove the bypass and otherwise restore normal operation |

¹¹ This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

¹² This tests for possible quiescent current related failures.

¹³ If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor



Appendix C: Common Cause for redundant configurations

A method for estimating the beta factor is provided in IEC 61508 – 6. Based on this approach, a Beta Factor of 5% may be used based on factors under control of the manufacturer. If the owner-operator of the plant institutes training and maintenance procedures specifically oriented toward common cause defense, a Beta Factor of 2% may be used.

Note that it was assumed that the safety instrumented function would not automatically be shut down when a diagnostic failure was detected.