



Failure Modes, Effects and Diagnostic Analysis

Project:

3051S pressure transmitter,
Software Revision 7.0 and above

Customer:

Rosemount Inc.
Chanhassen, Minnesota
USA

Contract No.: ROS 05/05-05
Report No.: ROS 05/05-05 R001
Version V1, Revision R3, August 27, 2007
John C. Grebe - Rachel Amkreutz



Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 3051S pressure transmitter with Software Revision 7.0 and above. 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 pressure transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The 3051S 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. 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 lists the versions of the 3051S pressure transmitter, Software Revision 7.0 and above, that have been considered for the hardware assessment.

Table 1 Version overview

1	3051S pressure transmitter, 3051S_C and 3051S_L Coplanar
2	3051S pressure transmitter, 3051S_T In-Line

The 3051S 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 may be used up to SIL 2 as a single device.

The failure rates for the 3051S pressure transmitter, 3051S_C and 3051S_L Coplanar configuration, are listed in Table 2.

Table 2 Failure rates 3051S pressure transmitter, 3051S_C and 3051S_L Coplanar

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	356
Fail Detected (detected by internal diagnostics)	264
Fail High (detected by the logic solver)	59
Fail Low (detected by the logic solver)	33
Fail Dangerous Undetected	37
No Effect	138
Annunciation Undetected	5

The failure rates for the 3051S pressure transmitter, 3051S_T In-Line configuration, are listed in Table 3.

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



Table 3 Failure rates 3051S pressure transmitter, 3051S_T In-Line

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	340
Fail Detected (detected by internal diagnostics)	256
Fail High (detected by the logic solver)	58
Fail Low (detected by the logic solver)	26
Fail Dangerous Undetected	34
No Effect	115
Annunciation Undetected	7

Table 4 lists the failure rates for the 3051S pressure transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 4 Failure rates and SFF according to IEC 61508

Device	λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF
3051S pressure transmitter, 3051S_C and 3051S_L Coplanar configuration	0 FIT	143 FIT	356 FIT	37 FIT	93.1%
3051S pressure transmitter, 3051S_T In-Line configuration	0 FIT	122 FIT	340 FIT	34 FIT	93.1%

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

A user of the 3051S pressure transmitter, Software Revision 7.0 and above, 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 “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	5
2 Project management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved.....	6
2.3 Standards / Literature used.....	6
2.4 Reference documents.....	6
2.4.1 Documentation provided by Rosemount Inc.	6
2.4.2 Documentation generated by <i>exida</i>	6
3 Product Description	6
4 Failure Modes, Effects, and Diagnostics Analysis.....	6
4.1 Description of the failure categories.....	6
4.2 Methodology – FMEDA, Failure rates.....	6
4.2.1 FMEDA.....	6
4.2.2 Failure rates	6
4.3 Assumptions	6
4.4 Results	6
5 Using the FMEDA results	6
5.1 Impulse line clogging	6
5.2 PFD _{AVG} calculation 3051S pressure transmitter.....	6
6 Terms and Definitions	6
7 Status of the document.....	6
7.1 Liability	6
7.2 Releases	6
7.3 Future Enhancements.....	6
7.4 Release Signatures.....	6
Appendix A: Lifetime of critical components	6
Appendix B Proof test to reveal dangerous undetected faults	6
B.1 Suggested Proof Test	6
B.1 Alternative Proof Test	6
Appendix C: Common Cause - redundant transmitter configuration	6



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 DIN V VDE 0801, 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}).

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 DIN V VDE 0801, 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}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software 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 justify the reduced fault tolerance requirements of 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 DIN V VDE 0801, 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 is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

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 3051S pressure transmitter with Software Revision 7.0 and above. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

It shall be assessed whether the 3051S pressure transmitter with Software Revision 7.0 and above meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 2 sub-systems according to 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 150 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

Rosemount Inc. Manufacturer of the 3051S pressure transmitter

exida Project leader of the FMEDA

Rosemount Inc. contracted *exida* with the FMEDA and PFD_{AVG} calculation of the above-mentioned device.

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]	SN 29500	Failure rates of components
[N5]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N6]	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.
[N7]	Safety Equipment Reliability Handbook, 2003	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N8]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods



2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	03151-1514, Rev AB, 8/12/2005	Schematic drawing 3051S pressure transmitter
[D2]	03151-1511, Rev AL	Schematic drawing 3051S pressure transmitter

2.4.2 Documentation generated by *exida*

[R1]	COSMOS SM Coplanar II 3051S - project projected 081205.xls	Failure Modes, Effects, and Diagnostic Analysis, 3051S pressure transmitter, Coplanar
[R2]	COSMOS SM Inline 3051T - project projected 081205.xls	Failure Modes, Effects, and Diagnostic Analysis, 3051S pressure transmitter, In-Line
[R3]	ROS 05-05-05 R001 V1 R3 FMEDA 3051S, 8/27/2007	FMEDA report, 3051S pressure transmitter (this report)



3 Product Description

The 3051S pressure transmitter, Software Revision 7.0 and above, is a smart two-wire device used in many different industries for both control and safety applications. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (output state is programmable). The device can be equipped with or without display.

The FMEDA has been performed for two different configurations of the 3051S pressure transmitter, i.e. Coplanar, and In-Line configuration. Table 5 lists the versions of the 3051S pressure transmitter that have been considered for the hardware assessment.

Table 5 Version overview

1	3051S pressure transmitter, 3051S_C and 3051S_L Coplanar
2	3051S pressure transmitter, 3051S_T In-Line

The 3051S pressure transmitter with Software Revision 7.0 and above is classified as a Type B³ device according to IEC 61508, having a hardware fault tolerance of 0.

The 3051S 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.

³ 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 based on documentation obtained from Rosemount Inc. and is documented in [R1] through [R2]. 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 3051S pressure transmitter with Software Revision 7.0 and above, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as state where the output exceeds the user defined threshold.
Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
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 (includes frozen output).
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 (> 21.5mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.6mA)
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 or a Fail Low 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.

The Annunciation Undetected 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 in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with 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) 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 a 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 3051S 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) and over-range (Fail High) failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- The HART protocol is only used for setup, calibration, and diagnostic purposes; not for safety critical operation.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.



- 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.



4.4 Results

Using reliability data extracted from the exida component reliability database the following failure rates resulted from the 3051S pressure transmitter FMEDA. Table 6 lists the failure rates for the 3051S pressure transmitter, 3051S_C and 3051S_L Coplanar configuration.

Table 6 Failure rates 3051S pressure transmitter, 3051S_C and 3051S_L Coplanar

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	356
Fail Detected (detected by internal diagnostics)	264
Fail High (detected by the logic solver)	59
Fail Low (detected by the logic solver)	33
Fail Dangerous Undetected	37
No Effect	138
Annunciation Undetected	5

Table 7 lists the failure rates for the 3051S pressure transmitter, 3051S_T In-Line configuration.

Table 7 Failure rates 3051S pressure transmitter, 3051S_T In-Line

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	340
Fail Detected (detected by internal diagnostics)	256
Fail High (detected by the logic solver)	58
Fail Low (detected by the logic solver)	26
Fail Dangerous Undetected	34
No Effect	115
Annunciation Undetected	7

The failure rates that are derived from the FMEDA for the 3051S pressure transmitter are in a format different from the IEC 61508 format. Table 8 lists the failure rates for 3051S pressure transmitter, Software Revision 7.0 and above, according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

According to IEC 61508 [N1], also the Safe Failure Fraction (SFF) of the 3051S pressure transmitter should be calculated. The SFF 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 formula for SFF:

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

Note that according to IEC 61508 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 8 Failure rates and SFF according to IEC 61508

Device	λ_{sd}	λ_{su}^4	λ_{dd}	λ_{du}	SFF
3051S pressure transmitter, 3051S_C and 3051S_L Coplanar configuration	0 FIT	143 FIT	356 FIT	37 FIT	93.1%
3051S pressure transmitter, 3051S_T In-Line configuration	0 FIT	122 FIT	340 FIT	34 FIT	93.1%

The architectural constraint type for 3051S 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.

⁴ 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 Impulse line clogging

The 3051S 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 rate for the clogged impulse line and add this failure rate to the 3051S SIS Pressure Transmitter failure rates.

5.2 PFD_{AVG} calculation 3051S pressure transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) 3051S pressure transmitter, Software Revision 7.0 and above. 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 the figure the PFD_{AVG} value for a single 3051S pressure transmitter with a proof test interval of 1 year equals 1.65E-04 (Coplanar configuration) and 1.52E-04 (In-Line configuration) respectively.

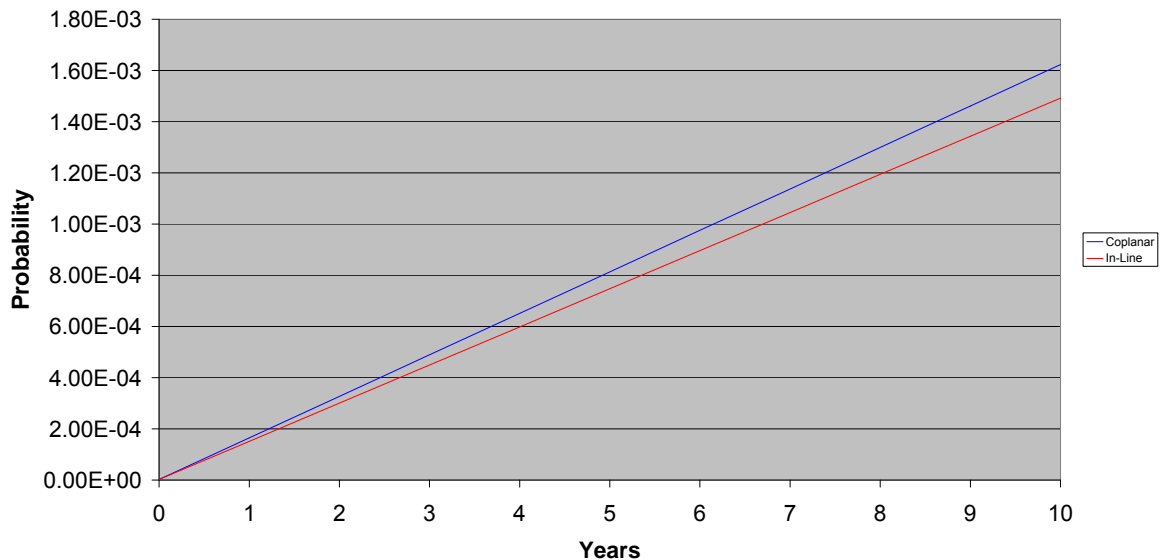


Figure 1 PFD_{AVG}(t) 3051S pressure transmitter, Software Revision 7.0 and above

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 pressure transmitter, Coplanar configuration is equal to 1.7% of the range. The PFD_{AVG} for a 1-year Proof Test Interval of the 3051S pressure transmitter, In-Line configuration, is equal to 1.5% 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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
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: R3
Version History: V1, R3: Clarify product revision; August 27, 2007
V1, R2: Product name, proof tests updated; November 30, 2005
V1, R1: Released to Rosemount Inc.; November 15, 2005
V0, R1: Draft; November 14, 2005
Authors: John C. Grebe - Rachel Amkreutz
Review: V0, R1: Iwan van Beurden (*exida*); November 15, 2005
V1, R1: Randy Longsdorf, Chad Blumeyer; November 30, 2005
Release status: Released to Rosemount Inc.

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble".

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "John C. Grebe".

John C. Grebe, Partner

A handwritten signature in black ink, appearing to read "Rachel Amkreutz".

Ir. Rachel Amkreutz, Safety Engineer



Appendix A: Lifetime of critical components

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is 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 9 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 9 Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours

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 3051S pressure transmitter have an estimated useful lifetime of about 50 years. According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed⁵.

⁵ According to section 7.4.7.4 Note 3 of IEC 61508, experiences have shown that the useful lifetime often lies within a range of 8 to 12 years for transmitters.



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 consists of an analog output loop test, as described in Table 10. This test will detect approximately 52% of possible DU failures in the 3051S pressure transmitter, Coplanar configuration, and 62% of possible DU failure for the In-Line configuration.

Table 10 Steps for Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. <small>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.</small>
3.	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. <small>This tests for possible quiescent current related failures</small>
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or otherwise restore normal operation.

B.1 Alternative Proof Test

The alternative proof test consists of the following steps, as described in Table 11. This test will detect approximately 92% of possible DU failures in the 3051S pressure transmitter, Coplanar configuration, and 95% of possible DU failure for the In-Line configuration.

Table 11 Steps for Alternative Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Perform Proof Test 1.
3.	Perform a minimum two-point sensor calibration check using the 4-20mA range points as the calibration points and verify that the mA output corresponds to the pressure input value.
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or otherwise restore normal operation.



Appendix C: Common Cause - redundant transmitter configuration

A method for estimating the beta factor is provided in IEC 61508, part 6. This portion of the standard is only informative and other techniques may be used to estimate the beta factor. Based on the approach presented in IEC 61508 a series of questions are answered. Based on the total points scored for these questions, the beta factor number is determined from IEC 61508-6 Table D.4.

Example – 2oo3 Pressure Transmitters

A design is being evaluated where three 3051S pressure transmitter are chosen. The transmitters are connected to a logic solver programmed to detect over-range and under-range currents as a diagnostic alarm. The process is does not shutdown when an alarm occurs on one transmitter. The logic solver has a two out of three (2oo3) function block that votes to trip when two of the three transmitters indicate the need for a trip. Following the questions from the sensor portion of Table D.1 of IEC 61508, Part 6, the following results are obtained.

Table 12 Example version of Table D.1, IEC 61508-6

Item	X _{SF}	Y _{SF}	Example	Score
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	Not guaranteed	0.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	2.5	1.5	Transmitters are separate	4.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?	2.5	0.5	Transmitters are in different housings	3.0
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc.?	7.5		No – transmitters are identical	0.0
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?	5.5		No – transmitters are identical	0.0
Do the channels employ enhanced redundancy with MooN architecture, where $N > M + 2$?	2.0	0.5	No – 2oo3	0.0
Do the channels employ enhanced redundancy with MooN architecture, where $N = M + 2$?	1.0	0.5	No – 2oo3	0.0
Are separate test methods and people used for each channel during commissioning?	1.0	1.0	No - impractical	0.0
Is maintenance on each channel carried out by different people at different times?	2.5		No - impractical	0.0
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5	No cross channel information between transmitters	1.0
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	3051S pressure transmitter based on well proven design	2.0
Is there more than 5 years experience with the same hardware used in similar environments?	1.5	1.5	Extensive experience in process control	3.0
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	Transient voltage and current protection provided	2.0



Item	X _{SF}	Y _{SF}	Example	Score
Are all devices/components conservatively rated? (for example, by a factor of 2 or more)	2.0		Design has conservative rating factors proven by field reliability	2.0
Have the results of the failure modes and effects analysis or fault tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3.0	FMEDA done by third party – exida. No common cause issues	3.0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3.0	Design review is part of the development process. Results are always fed back into the design	3.0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	Field failure feedback procedure reviewed by third party – exida. Results are fed back into the design.	4.0
Is there a written system of work which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?	0.5	1.5	Proof test procedures are provided but they cannot insure root cause failure analysis.	0.0
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	2.0	1.0	Procedures are not sufficient to ensure staggered maintenance.	0.0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.), intended to be independent of each other, must not be relocated?	0.5	0.5	MOC procedures require review of proposed changes, but relocation may inadvertently be done.	0.0
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	Repair is done by returning product to the factory, therefore this requirement is met.	2.0
Do the system diagnostic tests report failures to the level of a field-replaceable module?	1.0	1.0	Logic solver is programmed to detect current out of range and report the specific transmitter.	2.0
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures	2.0	3.0	Control system designers have not been trained.	0.0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures	0.5	4.5	Maintenance personnel have not been trained.	0.0



Item	X _{SF}	Y _{SF}	Example	Score
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	A tool is required to open the transmitter therefore this requirement is met.	3.0
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	Environmental conditions are checked at installation.	4.0
Are all signal and power cables separate at all positions?	2.0	1.0	No	0.0
Has a system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	Complete testing of all environmental stress variables and run-in during production testing.	20.0
Totals	23	37	S=X+Y	58

A score of 58 results in a beta factor of 5%. If the owner-operator of the plant would institute common cause training and more detailed maintenance procedures specifically oriented toward common cause defense, a score of greater than 70 could be obtained. Then the beta factor would be 2%.

Note that the diagnostic coverage for the transmitter is not being considered. Additional points can be obtained when diagnostics are taken into account. However this assumes that a shutdown occurs whenever any diagnostic alarm occurs. In the process industries this could even create dangerous conditions. Therefore the practice of automatic shutdown on a diagnostic fault is rarely implemented. IEC 61508-6 has a specific note addressing this issue. The note states:

“NOTE 5: In the process industries, it is unlikely to be feasible to shut down the EUC when a fault is detected within the diagnostic test interval as described in table D.2. This methodology should not be interpreted as a requirement for process plants to be shut down when such faults are detected. However, if a shut down is not implemented, no reduction in the b-factor can be gained by the use of diagnostic tests for the programmable electronics. In some industries, a shut down may be feasible within the described time. In these cases, a non-zero value of Z may be used.”

In this example, automatic shutdown on diagnostic fault was not implemented so no credit for diagnostics was taken.