



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

Project:

Model 3051S Electronic Remote Seal System

Company:

Rosemount Inc.  
Chanhassen, MN  
United States

Contract Number: Q10/04-83

Report No.: ROS 10/04-83 R001

Version V1, Revision R1, June 1, 2010

Griff Francis

## 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 Model 3051S Electronic Remote Seal System. 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 Model 3051S ERS. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Model 3051S ERS is a two wire, 4 – 20 mA architecture that calculates differential pressure electronically using two pressure transmitters that are linked together with a digital cable. The transmitter system uses standard, well-proven sensor boards in combination with a microprocessor board that performs diagnostics. It is programmed to send its output to a specified failure state, either high or low, when an internal failure is detected. The device is externally powered from 24 Volts DC.

It is assumed that the 4 – 20 mA output is used as a primary safety variable. No other output variants are covered by this report.

Table 1 gives an overview of the different Primary and Secondary Transmitter Models. A Model 3051S Electronic Remote Seal System consists of a Primary and a Secondary Transmitter.

### Table 1 Version Overview

#### Primary Transmitter Models

<u>Model Number</u>	<u>Description</u>
3051SAM_PA	Absolute pressure, coplanar sensor, measurement transmitter
3051SAL_PA	Absolute pressure, coplanar sensor, level transmitter
3051SAM_PD	Differential pressure, coplanar sensor, measurement transmitter
3051SAL_PD	Differential pressure, coplanar sensor, level transmitter
3051SAM_PG	Gage pressure, coplanar sensor, measurement transmitter
3051SAL_PG	Gage pressure, coplanar sensor, level transmitter
3051SAM_PE	Absolute pressure, in-line sensor, measurement transmitter
3051SAL_PE	Absolute pressure, in-line sensor, level transmitter
3051SAM_PT	Gage pressure, in-line sensor, measurement transmitter
3051SAL_PT	Gage pressure, in-line sensor, level transmitter

#### Secondary Transmitter Models

<u>Model Number</u>	<u>Description</u>
3051SAM_SA	absolute pressure, coplanar sensor, measurement transmitter
3051SAL_SA	absolute pressure, coplanar sensor, level transmitter
3051SAM_SD	differential pressure, coplanar sensor, measurement transmitter
3051SAL_SD	differential pressure, coplanar sensor, level transmitter
3051SAM_SG	gage pressure, coplanar sensor, measurement transmitter
3051SAL_SG	gage pressure, coplanar sensor, level transmitter
3051SAM_SE	absolute pressure, in-line sensor, measurement transmitter
3051SAL_SE	absolute pressure, in-line sensor, level transmitter
3051SAM_ST	gage pressure, in-line sensor, measurement transmitter
3051SAL_ST	gage pressure, in-line sensor, level transmitter



The Model 3051S ERS is classified as a Type B<sup>1</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

The complete final element subsystem, of which the Model 3051S ERS is the sensor, will need to be evaluated to determine the Safe Failure Fraction.

The failure rates for the Model 3051S ERS are listed in Table 2.

**Table 2 Failure rates Model 3051S ERS**

Primary Transmitter with Coplanar Sensor and Secondary Transmitter with Coplanar Sensor

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	319.1
Fail Dangerous Detected	896.7
Fail Detected (detected by internal diagnostics)	611.3
Fail High (detected by logic solver)	144.2
Fail Low (detected by logic solver)	141.2
Fail Dangerous Undetected	131.0
Residual	474.7
Annunciation Undetected	29.6
External Leak	45.0

Primary Transmitter with Coplanar Sensor and Secondary Transmitter with In-Line Sensor or  
Primary Transmitter with In-Line Sensor and Secondary Transmitter with Coplanar Sensor

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	237.3
Fail Dangerous Detected	995.8
Fail Detected (detected by internal diagnostics)	801.9
Fail High (detected by logic solver)	85.2
Fail Low (detected by logic solver)	108.7
Fail Dangerous Undetected	113.8
Residual	441.8
Annunciation Undetected	31.5
External Leak	45.0

Primary Transmitter with In-Line Sensor and Secondary Transmitter with In-Line Sensor

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



<b>Failure Category</b>	<b>Failure Rate (FIT)</b>	
Fail Safe Undetected	155.5	
Fail Dangerous Detected	1094.8	
Fail Detected (detected by internal diagnostics)	992.5	
Fail High (detected by logic solver)	26.1	
Fail Low (detected by logic solver)	76.2	
Fail Dangerous Undetected	96.5	
Residual	408.9	
Annunciation Undetected	33.4	
External Leak	45.0	

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 3 lists the failure rates for the Model 3051S ERS according to IEC 61508.

**Table 3 Failure rates according to IEC 61508**

Device	$\lambda_{SD}$	$\lambda_{SU}^2$	$\lambda_{DD}$	$\lambda_{DU}$	SFF <sup>3</sup>
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with Coplanar Sensor	-	823.4 FITs	896.7 FITs	131.0 FITs	92.9%
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with In-Line Sensor or Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with Coplanar Sensor	-	710.6 FITs	995.8 FITs	113.8 FITs	93.7%
Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with In-Line Sensor	-	597.8 FITs	1,094.8 FITs	96.5 FITs	94.6%

A user of the Model 3051S ERS can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

<sup>2</sup> It is important to realize that the 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

<sup>3</sup> Safe Failure Fraction needs to be calculated on (sub)system level

## Table of Contents

Management Summary .....	2
1 Purpose and Scope.....	7
2 Project Management .....	8
2.1 <i>exida</i> .....	8
2.2 Roles of the parties involved.....	8
2.3 Standards and Literature used .....	8
2.4 Reference documents .....	9
2.4.1 Documentation provided by Rosemount Inc.....	9
2.4.2 Documentation generated by <i>exida</i> .....	9
3 Product Description .....	10
4 Failure Modes, Effects, and Diagnostic Analysis.....	12
4.1 Failure Categories description .....	12
4.2 Methodology – FMEDA, Failure Rates .....	13
4.2.1 FMEDA .....	13
4.2.2 Failure Rates .....	13
4.3 Assumptions .....	14
4.4 Results.....	15
5 Using the FMEDA Results.....	18
5.1 Impulse line clogging .....	18
5.2 PFD <sub>AVG</sub> Calculation Model 3051S ERS .....	18
6 Terms and Definitions .....	21
7 Status of the Document.....	22
7.1 Liability.....	22
7.2 Releases.....	22
7.3 Future Enhancements .....	22
7.4 Release Signatures .....	23
Appendix A Lifetime of Critical Components.....	24
Appendix B Proof tests to reveal dangerous undetected faults .....	25
B.1 Comprehensive Proof Test.....	25

## 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 Model 3051S ERS. 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.



## 2.4 Reference documents

### 2.4.1 Documentation provided by Rosemount Inc.

[D1]	00825-0100-4804_apr12_2010.pdf, Preliminary Copy	Quick Installation Guide, Rosemount 3051S ERS
[D2]	Preliminary 3051S PDS.pdf, Rev MA, March 2010	Product Data Sheet, Rosemount 3051S Series
[D3]	3051S User Manual, Rev DA, February 2009	Reference Manual, Rosemount 3051S Series
[D4]	ERS hw architecture.pptx	3051S ERS Electrical Architecture
[D5]	03151_3750_rev_AA.pdf	Schematic, Feature Board 3051S ERS
[D6]	03151-1511.pdf, Rev AR	Schematic, COSMOS Supermodule, 3051T (aka In-Line Sensor or Strain Gage Sensor)
[D7]	03151-1514.pdf, Rev AE	Schematic, Coplanar Board II, 3051S (aka Capacitive Sensor or Metal Cell Sensor)
[D8]	03151-4270.pdf, Rev AB	Schematic, Terminal Block, Dual Compartment, 3051S ERS
[D9]	03151-4280.pdf, Rev AB	Schematic, Terminal Block, Single Compartment, 3051S ERS

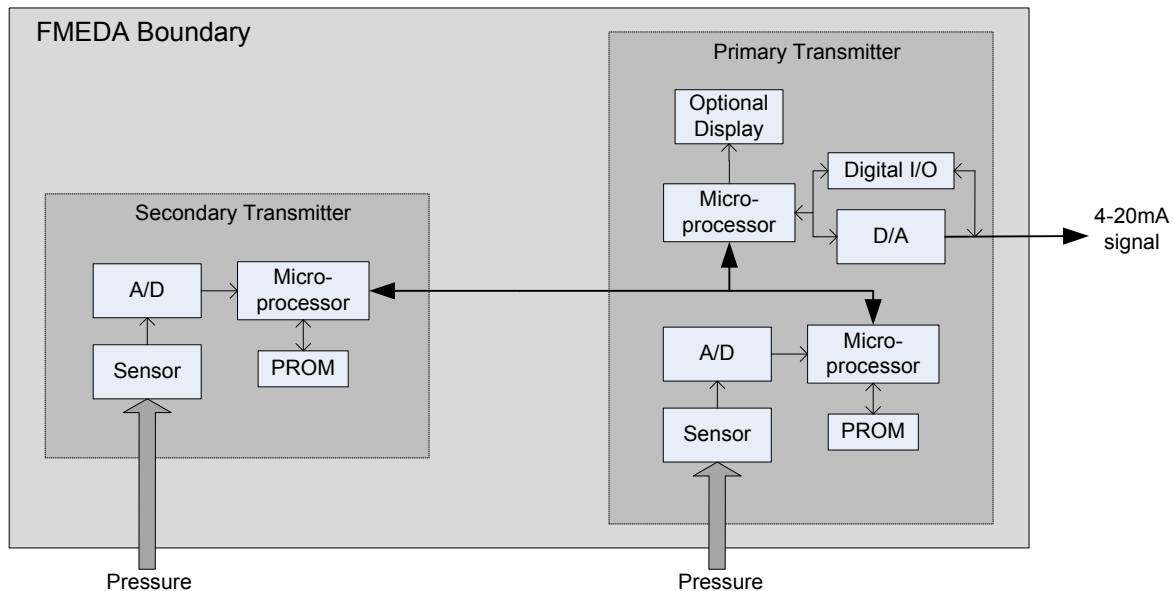
### 2.4.2 Documentation generated by *exida*

[R1]	3051S ERS Feature Board100510.emf	Failure Modes, Effects, and Diagnostic Analysis – Model 3051S ERS Feature Board
[R2]	3051S ERS Single Terminal Board100518.emf	Failure Modes, Effects, and Diagnostic Analysis – Model 3051S ERS Single Terminal Board
[R3]	3051S ERS Dual Terminal Board100516.emf	Failure Modes, Effects, and Diagnostic Analysis – Model 3051S ERS Dual Terminal Board
[R4]	CAN Mode SM Coplanar II 3051S Rev_AE.xls	Failure Modes, Effects, and Diagnostic Analysis –Model 3051S ERS Coplanar Board
[R5]	CAN Mode SM inline 3051T Rev_AR.xls	Failure Modes, Effects, and Diagnostic Analysis –Model 3051S ERS
[R6]	3051S_ERS_FMEDA Summary.xls	Failure Modes, Effects, and Diagnostic Analysis - Summary –Model 3051S ERS
[R7]	ROS Q10-04-083 R001 V1R1 1Jun10, 06/01/2010	FMEDA report, Model 3051S ERS (this report)

### 3 Product Description

The Model 3051S ERS is a two wire, 4 – 20 mA architecture that calculates differential pressure electronically using two pressure transmitters (primary and secondary) that are linked together with a digital cable. The transmitter system uses standard, well-proven sensor boards in combination with a microprocessor board that performs diagnostics. It is programmed to send its output to a specified failure state, either high or low, when an internal failure is detected. The device is externally powered from 24 Volts DC.

It is assumed that the 4 – 20 mA output is used as a primary safety variable. No other output variants are covered by this report.



**Figure 1 Model 3051S ERS, Parts included in the FMEDA**

Table 4 gives an overview of the different Primary and Secondary Transmitter Models. A Model 3051S Electronic Remote Seal System consists of a Primary and a Secondary transmitter.

**Table 4 Version Overview**

**Primary Transmitter Models**

3051SAM_PA	Absolute pressure, coplanar sensor, measurement transmitter
3051SAL_PA	Absolute pressure, coplanar sensor, level transmitter
3051SAM_PD	Differential pressure, coplanar sensor, measurement transmitter
3051SAL_PD	Differential pressure, coplanar sensor, level transmitter

3051SAM_PG	Gage pressure, coplanar sensor, measurement transmitter
3051SAL_PG	Gage pressure, coplanar sensor, level transmitter
3051SAM_PE	Absolute pressure, in-line sensor, measurement transmitter
3051SAL_PE	Absolute pressure, in-line sensor, level transmitter
3051SAM_PT	Gage pressure, in-line sensor, measurement transmitter
3051SAL_PT	Gage pressure, in-line sensor, level transmitter

#### Secondary Transmitter Models

3051SAM_SA	absolute pressure, coplanar sensor, measurement transmitter
3051SAL_SA	absolute pressure, coplanar sensor, level transmitter
3051SAM_SD	differential pressure, coplanar sensor, measurement transmitter
3051SAL_SD	differential pressure, coplanar sensor, level transmitter
3051SAM_SG	gage pressure, coplanar sensor, measurement transmitter
3051SAL_SG	gage pressure, coplanar sensor, level transmitter
3051SAM_SE	absolute pressure, in-line sensor, measurement transmitter
3051SAL_SE	absolute pressure, in-line sensor, level transmitter
3051SAM_ST	gage pressure, in-line sensor, measurement transmitter
3051SAL_ST	gage pressure, in-line sensor, level transmitter

The Model 3051S ERS is classified as a Type B<sup>4</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

---

<sup>4</sup> 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 section 2.4.1.

### 4.1 Failure Categories description

In order to judge the failure behavior of the Model 3051S ERS, the following definitions for the failure of the device were considered.

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 (xx mA).
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
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> xx mA)
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current(< xx mA)
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	
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.
External Leakage	Failure that causes process fluids to leak; External leakage is not considered part of the safety function and therefore this failure rate is not included in the Safe Failure Fraction calculation

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 5. 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 5 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 Model 3051S ERS.

- Only a single component failure will fail the entire Model 3051S ERS
- 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, including the wiring between the primary and secondary transmitters
- External power supply failure rates are not included



- Worst-case internal fault detection time is 2 hours

#### 4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Model 3051S ERS FMEDA.

**Table 6 Failure rates Model 3051S ERS**

Primary Transmitter with Coplanar Sensor and Secondary Transmitter with Coplanar Sensor

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	319.1
Fail Dangerous Detected	896.7
Fail Detected (detected by internal diagnostics)	611.3
Fail High (detected by logic solver)	144.2
Fail Low (detected by logic solver)	141.2
Fail Dangerous Undetected	131.0
Residual	474.7
Annunciation Undetected	29.6
External Leak	45.0

Primary Transmitter with Coplanar Sensor and Secondary Transmitter with In-Line Sensor or Primary Transmitter with In-Line Sensor and Secondary Transmitter with Coplanar Sensor

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	237.3
Fail Dangerous Detected	995.8
Fail Detected (detected by internal diagnostics)	801.9
Fail High (detected by logic solver)	85.2
Fail Low (detected by logic solver)	108.7
Fail Dangerous Undetected	113.8
Residual	441.8
Annunciation Undetected	31.5
External Leak	45.0



Primary Transmitter with In-Line Sensor and Secondary Transmitter with In-Line Sensor

<b>Failure Category</b>	<b>Failure Rate (FIT)</b>	
Fail Safe Undetected	155.5	
Fail Dangerous Detected	1094.8	
Fail Detected (detected by internal diagnostics)	992.5	
Fail High (detected by logic solver)	26.1	
Fail Low (detected by logic solver)	76.2	
Fail Dangerous Undetected	96.5	
Residual	408.9	
Annunciation Undetected	33.4	
External Leak	45.0	

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



Table 7 lists the failure rates for the Model 3051S ERS according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the Model 3051S ERS is only one part of a (sub)system, the SFF should be calculated for the entire sensor / logic / final element combination. 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 7 Failure rates according to IEC 61508**

Device	$\lambda_{SD}$	$\lambda_{SU}^5$	$\lambda_{DD}$	$\lambda_{DU}$	SFF <sup>6</sup>
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with Coplanar Sensor	-	823.4 FITs	896.7 FITs	131.0 FITs	92.9%
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with In-Line Sensor or Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with Coplanar Sensor	-	710.6 FITs	995.8 FITs	113.8 FITs	93.7%
Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with In-Line Sensor	-	597.8 FITs	1,094.8 FITs	96.5 FITs	94.6%

The architectural constraint type for the Model 3051S ERS 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.

<sup>5</sup> 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

<sup>6</sup> 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 Model 3051S ERS 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 Model 3051S ERS failure rates.

### 5.2 PFD<sub>AVG</sub> Calculation Model 3051S ERS

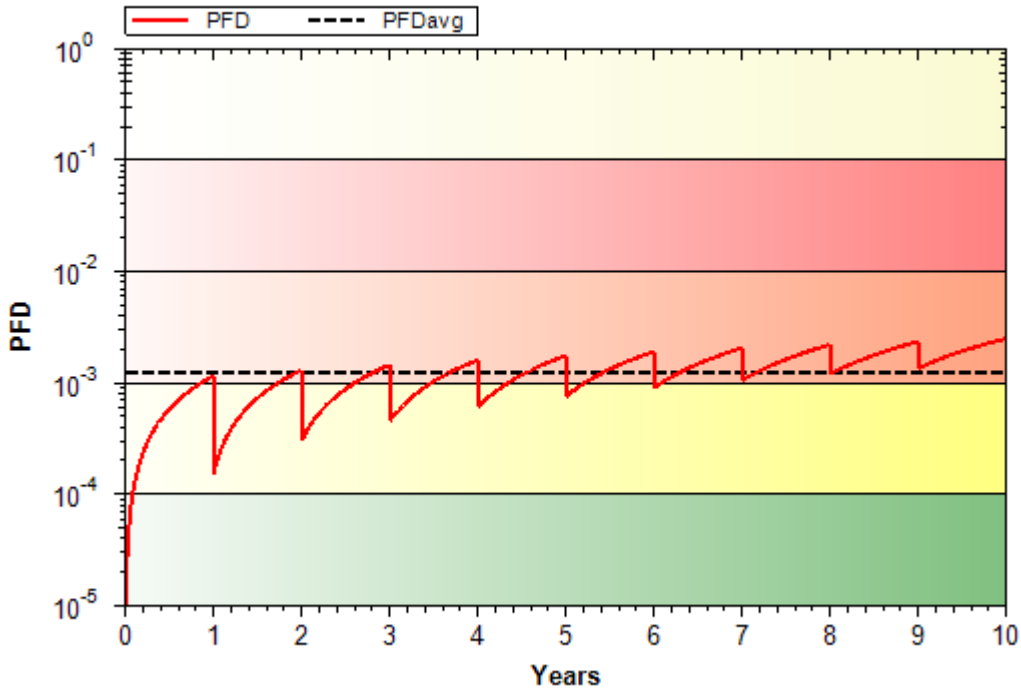
An average Probability of Failure on Demand (PFD<sub>AVG</sub>) calculation is performed for a single (1001) Model 3051S ERS with *exida's* exSILentia tool. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. Table 8 lists the proof test coverage (see Appendix B) used for the models as well as the results when the proof test interval equals 1 year.

**Table 8 Sample PFD<sub>AVG</sub> Results**

Device	Proof Test Coverage	PFD <sub>AVG</sub>	% of SIL 2 Range
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with Coplanar Sensor	87%	1.25E-03	12.5%
Model 3051S ERS, Primary Transmitter with Coplanar Sensor + Secondary Transmitter with In-Line Sensor or Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with Coplanar Sensor	87%	1.10E-03	11.0%
Model 3051S ERS, Primary Transmitter with In-Line Sensor + Secondary Transmitter with In-Line Sensor	86%	9.79E-04	9.8%

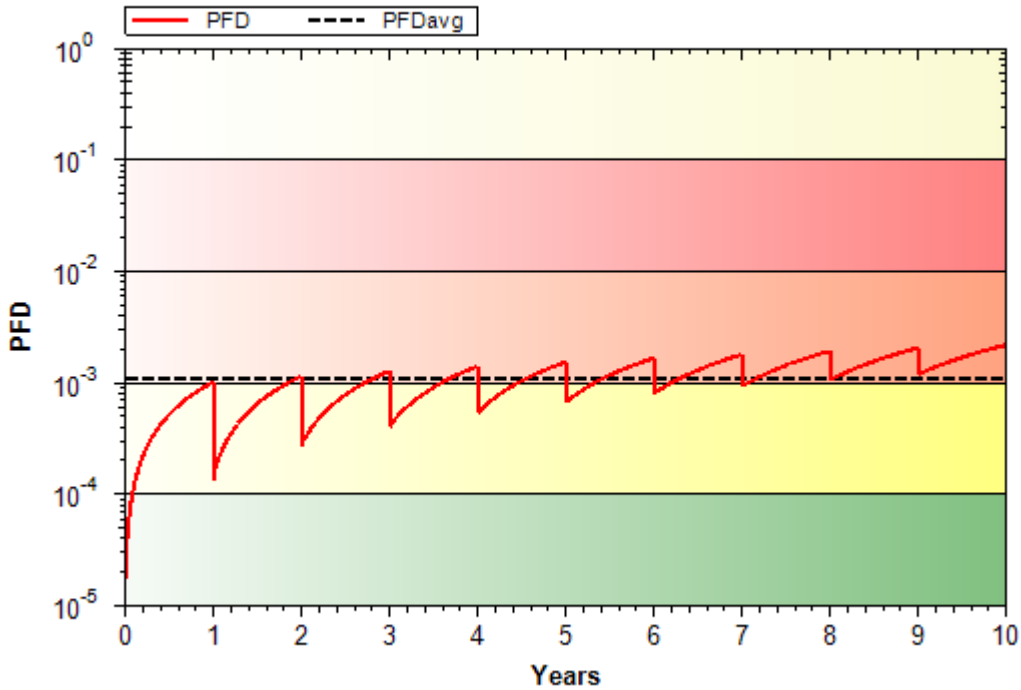
The resulting exSILentia generated PFD graphs with a one year proof test interval are displayed below.

**Sensor Group 1: Primary Coplanar + Secondary Coplanar**

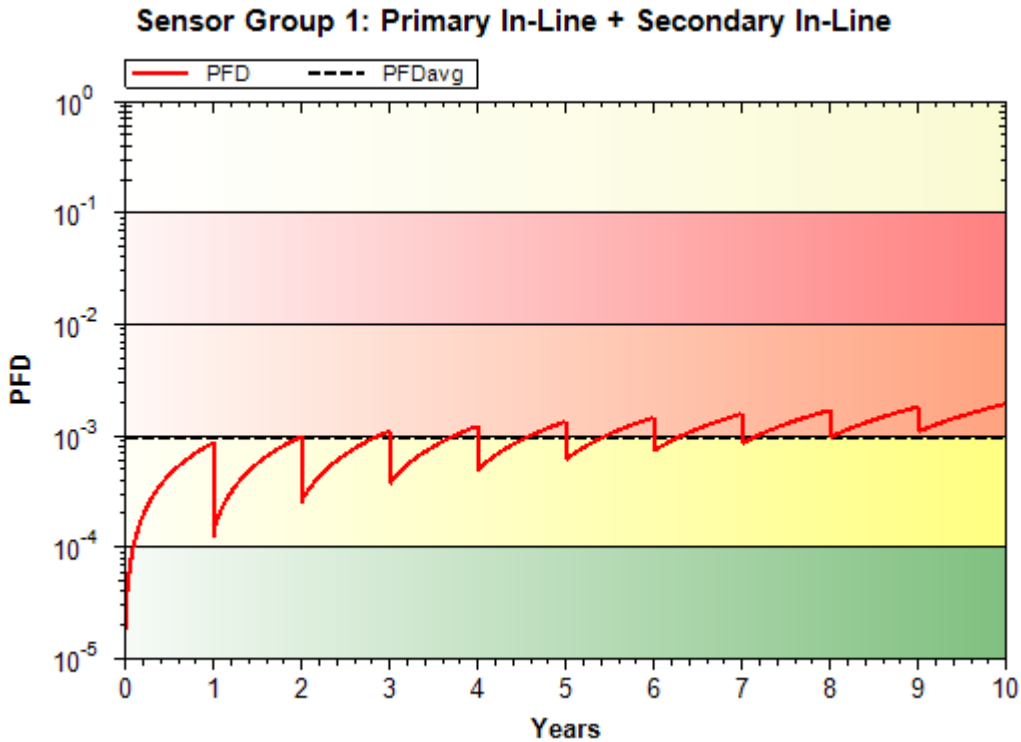


© 2009 exida.com L.L.C.

**Sensor Group 1: P Copl. + S In-Line or P In-Line + S Copl.**



© 2009 exida.com L.L.C. 1



© 2009 exida.com L.L.C.

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 Model 3051S ERS is approximately equal to 9% to 14% 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 <sup>-9</sup> 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.
PVST	Partial Valve Stroke Test  It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Stroke Testing also has an impact on the Safe Failure Fraction.
PFD <sub>AVG</sub>	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
Severe service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.

## 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: R1

Version History: V1, R1: Released to Rosemount Inc.; 1 June 2010

V0, R1: Draft; 19 May 2010

Author(s): Griff Francis

Review: V0, R1: Dr. William M. Goble, 1 June 2010

Release Status: Released to Rosemount Inc.

### 7.3 Future Enhancements

At request of client.

#### 7.4 Release Signatures

A handwritten signature in black ink that reads "William M. Goble". The signature is written in a cursive style with a prominent loop at the end of the last name.

---

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink that reads "Griff Francis". The signature is written in a cursive style with a prominent loop at the end of the last name.

---

Griff Francis, Safety Engineer

## Appendix A Lifetime of Critical Components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime<sup>7</sup> of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the 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 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 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 Model 3051S ERS 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.

---

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

## Appendix B Proof 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 Comprehensive Proof Test

The suggested proof test described in Table 10 will detect 86%-87% of possible DU failures in the Model 3051S ERS. The suggested proof test in combination with automatic diagnostics will detect 98%-99% of possible DU failures in the Model 3051S ERS.

**Table 10 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 verify that the analog current reaches that value <sup>8</sup> .
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 <sup>9</sup> .
5.	Perform a two-point calibration <sup>10</sup> of the transmitter over the full working range.
6.	Remove the bypass and otherwise restore normal operation

<sup>8</sup> 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.

<sup>9</sup> This tests for possible quiescent current related failures.

<sup>10</sup> If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor