



Failure Modes, Effects and Diagnostic Analysis

Project:

Guided wave radar transmitter Rosemount 5300 Series with 4..20mA
output for continuous level measurement of liquids and solids

Customer:

Rosemount Tank Radar AB
Gothenburg
Sweden

Contract No.: Rosemount 08/02-17
Report No.: Rosemount 08/02-17 R005
Version V1, Revision R0, July 2008
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the guided wave radar transmitter Rosemount 5300 Series with software version 2A1. Table 1 gives an overview of the different types that belong to the considered guided wave radar transmitter Rosemount 5300 Series.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

Type	Application	Sensor element
Rosemount 5301	Liquid level or submerged interface	Coaxial, twin element (rod or cable), and single element (rod or cable)
Rosemount 5302	Liquid level and interface	Coaxial, twin element (rod or cable), and single element (rod or cable)
Rosemount 5303	Solid level	Coaxial, twin element (rod or cable), and single element (rod or cable)

For safety applications only the 4..20 mA output was considered. All other possible output variants, electronics or applications are not covered by this report.

The failure rates used in this analysis are from *exida's* Electrical and Mechanical Component Reliability Handbook (see [N2]).

The guided wave radar transmitter Rosemount 5300 Series is considered to be a Type B¹ subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF shall be > 90% for SIL2 subsystems according to table 3 of IEC 61508-2.

Rosemount Tank Radar AB together with *exida* performed a quantitative analysis of the sensor element parts of the guided wave radar transmitter Rosemount 5300 Series to calculate the mechanical failure rates of the sensor element using *exida's* experienced-based data compilation for the different mechanical components. The results of the quantitative analysis were used for the calculations described in section 4.5.1.

The failure rates listed below do not include failures resulting from incorrect use of the guided wave radar transmitter Rosemount 5300 Series, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

A user of the guided wave radar transmitter Rosemount 5300 Series 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 4.5.1 along with all assumptions.

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.

The failure rates are valid for the useful life of the guided wave radar transmitter Rosemount 5300 Series (see Appendix 2).

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



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.

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.

It is assumed that the connected logic solver is configured as per the NAMUR NE43 signal ranges (alarm current ≤ 3.6 mA or ≥ 21 mA) or the Rosemount standard (alarm current ≤ 3.75 mA or ≥ 21.75 mA), i.e. the guided wave radar transmitter Rosemount 5300 Series with 4..20 mA current output communicates detected faults by an alarm output current according to these levels. This is due to fact that a user of the guided wave radar transmitter Rosemount 5300 Series can use either NAMUR NE43 or Rosemount Standard configurations of the alarm levels. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled.

Table 2: Summary – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	490
Fail safe undetected	57
Residual	410
Annunciation undetected (95%)	23
Fail Dangerous Detected (λ_{DD})	884
Fail detected (internal diagnostics or indirectly ²)	629
Fail high (detected by the logic solver)	25
Fail low (detected by the logic solver)	229
Fail Dangerous Undetected (λ_{DU})	140
Fail dangerous undetected	139
Annunciation undetected (5%)	1
No part	273
Total failure rate (safety function)	1514 FIT
SFF	90.7%
DC_S	0%
DC_D	86%
MTBF	64 years
SIL AC ³	SIL2

² “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

³ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.



Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards / Literature used.....	7
2.4 Reference documents.....	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida</i>	8
3 Description of the analyzed subsystem.....	9
3.1 Product description	9
3.2 Measuring principle.....	10
4 Failure Modes, Effects, and Diagnostics Analysis	11
4.1 Description of the failure categories.....	11
4.2 Methodology – FMEDA, Failure rates.....	13
4.2.1 FMEDA.....	13
4.2.2 Failure rates	13
4.3 Assumptions	14
4.4 Analysis of the process connection.....	14
4.5 Results	15
4.5.1 Guided wave radar transmitter Rosemount 5300 Series	16
5 Using the FMEDA results.....	17
5.1 PFD_{AVG} / PFH calculation.....	17
6 Terms and Definitions	19
7 Status of the document.....	20
7.1 Liability.....	20
7.2 Releases.....	20
7.3 Release Signatures.....	20
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	21
Appendix 2: Possible proof tests to detect dangerous undetected faults.....	22
Appendix 3: Impact of lifetime of critical components on the failure rate	23

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 FMEDA carried out on the guided wave radar transmitter Rosemount 5300 Series with software version 2A1. From this, failure rates, Safe Failure Fraction (SFF), PFH and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a sensor subsystem, including the guided wave radar transmitter Rosemount 5300 Series meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.



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 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, internet based safety engineering tools, detail 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 Tank Radar AB Manufacturer of the guided wave radar transmitter Rosemount 5300 Series

exida Performed the hardware assessment

Rosemount Tank Radar AB contracted *exida* in February 2008 with the FMEDA 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 61508-2:2000	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

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	03151-4211.pdf	Circuit diagram "COSMOS SUPERMODULE TERMINAL BLOCK DUAL COMPARTMENT – STANDARD" 03151-4211 of 19.07.01
[D2]	9150079-307_I01_Pxx_A3.pdf	Circuit diagram "Main Board" 9150079-307 Issue 1
[D3]	9150079-312_I01_PXX_A3.pdf	Circuit diagram "Interface Board (HART)" 9150079-312 Issue 1
[D4]	9150079-325_i02_pxx_a3.pdf	Circuit diagram "Pulsed Microwave Module DC" 9150079-325 Issue 2
[D5]	9240030-313_I01_PXX_A3.pdf	Circuit diagram "BARRIER BOARD HART (BBH)" 9240030-313 Issue 1
[D6]	9240030-317_I01_PXX_A3.pdf	Circuit diagram "EMC BOARD (EB)" 9240030-317 Issue 1

[D7]	LCD_03031-0589_IA.pdf	Circuit diagram "160 SEGMENT LCD BOARD" 03031-0589 of 26.06.96
[D8]	9240030-932_I02 Cert dwg 5300.pdf	Mechanical drawing "CERT. DWG NEMKO ROSEMOUNT 5300 SERIES" 9240030-932 issue 02
[D9]	9240030-944_I01 Probes 5300.pdf	Mechanical drawing "CERT. DWG PROBES NEMKO ROSEMOUNT 5300 SERIES" 9240030-944 issue 01
[D10]	9240030-596_I02.pdf	Mechanical drawing "RTG 5300" 92400030-596 issue 02
[D11]	9240030-596_r_a_070509.pdf	Bill of material RTG 5300
[D12]	00813-0100-4530.pdf	Product Data Sheet 00813-0100-4530 Rev AA Catalog 2008 - 2009
[D13]	5X00-SIL-DOK0032.doc of 21.12.07	SW functions used in FMEDA 5300
[D14]	5X00-SIL-DOK0026.doc of 21.05.08	5300, SW BIT design specification
[D15]	RE FMEDA report T2.msg of 08.07.08	Feedback on FMEDA review
[D16]	FMEDA 5300 R5_1.xls of 30.05.08	
[D17]	FMEDA 5300 R5_1 with probe and housing DP.xls of 07.07.08	
[D18]	FMEDA 5300 R5_1 with probe and housing DPr1.xls of 08.07.08	
[D19]	5300 FMEDA FIT review.msg of 15.05.08	
[D20]	FMEDA 5300 R5_3 with probe and housing DP.xls of 11.07.08	

2.4.2 Documentation generated by exida

[R1]	FMEDA 5300 R04 Review SA.xls of 14.05.08
[R2]	FMEDA 5300 R04 Review SA2.xls of 15.05.08
[R3]	FMEDA_Review.txt of 15.05.08
[R4]	FMEDA 5300 R05.xls of 21.05.08
[R5]	HW FIT Witness Report - 5300 V1R0.pdf of 05.06.08
[R6]	FMEDA 5300 R5_1 with probe and housing.xls of 01.07.08
[R7]	FMEDA 5300 R5_2 with probe and housing DP.xls of 08.07.08

3 Description of the analyzed subsystem

3.1 Product description

The guided wave radar transmitter Rosemount 5300 Series is usable for level and interface measurements on liquids, slurries and solids. It consists of a sensor element (probe and tank connection) and a transmitter housing. The FMEDA has been carried out on the complete subsystem, i.e. sensor element and transmitter.

The guided wave radar transmitter Rosemount 5300 Series is considered to be a Type B subsystem with a hardware fault tolerance of 0.

Figure 1 gives an overview of the main components of the considered guided wave radar transmitter Rosemount 5300 Series.

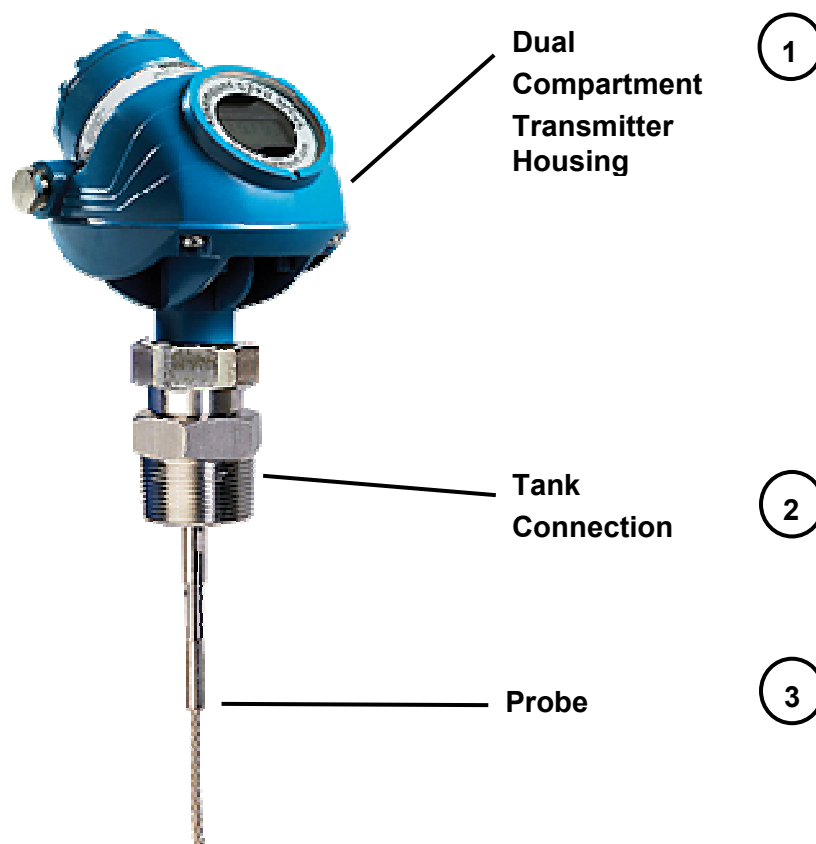


Figure 1: Rosemount 5300 Series

3.2 Measuring principle

The guided wave radar transmitter Rosemount 5300 Series is based on the Time Domain Reflectometry (TDR) technology.

Low power nano-second microwave pulses are guided down a probe submerged in the process media. When a radar pulse reaches a media with a different dielectric constant, part of the energy is reflected to the transmitter. The time difference between the transmitted and the reflected pulse is converted into a distance from which the total level or interface level is calculated.

The intensity of the reflection depends on the dielectric constant of the product. The higher the dielectric constant value is, the stronger the reflection will be

Figure 2 gives an overview of the measuring principle of the guided wave radar transmitter Rosemount 5300 Series.

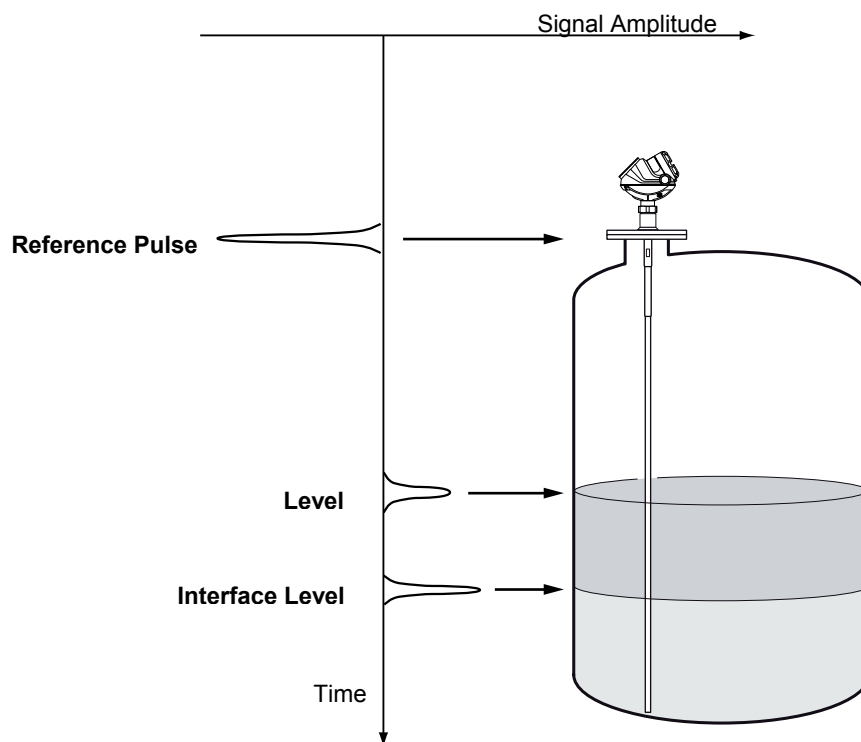


Figure 2: Measuring principle

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by Rosemount Tank Radar AB and reviewed by *exida*. The results are documented in [D20]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced at the component level and the effects of these failure modes were examined on system level. The results are documented in [R5]. Failures 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 guided wave radar transmitter Rosemount 5300 Series, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output reaching the user defined threshold value.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or that deviates the output current by more than 2% of full span.
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 (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 21.75 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.75 mA)
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (high or low).
Annunciation	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). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. For the calculation of the SFF the AU failures are treated to 5% as dangerous failures and to 95% as a residual failures.
Residual	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure and does not deviate the output current by not more than 2% full span. For the calculation of the SFF it is treated like a safe undetected failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508.

The “Residual” and “Annunciation” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. 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.

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 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 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 due to random events will be less than the number predicted by these failure rates.

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 or physical abuse.

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 guided wave radar transmitter Rosemount 5300 Series.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 8 hours.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not during normal operation.
- The test time of a connected safety PLC to react on a dangerous detected failure and bring the process to the safe state is 1 hour.
- The worst-case internal fault detection time is 90 minutes.
- 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.
- Only the current output 4..20mA is used for safety applications.
- The current output signal is fed to a SIL 2 compliant analog input board of a safety PLC.
- Because the display is not part of the safety function, the failure rate of the display is not considered in the calculation.
- 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 according to NAMUR NE43 or Rosemount Standard to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

4.4 Analysis of the process connection

Rosemount Tank Radar AB together with *exida* performed a quantitative analysis of the sensor element parts of the guided wave radar transmitter Rosemount 5300 Series to calculate the mechanical failure rates of the sensor element using *exida's* experienced-based data compilation for the different mechanical components. The results of the quantitative analysis were used for the calculations described in section 4.5.1.

4.5 Results

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

λ_{total} consists of the sum of all component failure rates. This means:

$$\lambda_{\text{total}} = \lambda_{\text{SD}} + \lambda_{\text{SU}} + \lambda_{\text{DD}} + \lambda_{\text{DU}}$$

$$\text{SFF} = 1 - \lambda_{\text{DU}} / \lambda_{\text{total}}$$

$$\text{DC}_S = \lambda_{\text{SD}} / (\lambda_{\text{SD}} + \lambda_{\text{SU}})$$

$$\text{DC}_D = \lambda_{\text{DD}} / (\lambda_{\text{DD}} + \lambda_{\text{DU}})$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = (1 / (\lambda_{\text{total}} + \lambda_{\text{no part}})) + 8 \text{ h}$$

4.5.1 Guided wave radar transmitter Rosemount 5300 Series

The FMEDA carried out on the guided wave radar transmitter Rosemount 5300 Series leads under the assumptions described in sections 4.3 to 4.5 to the following failure rates:

Table 3: Summary – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	490
Fail safe undetected	57
Residual	410
Annunciation undetected (95%)	23
Fail Dangerous Detected (λ_{DD})	884
Fail detected (internal diagnostics or indirectly ⁴)	629
Fail high (detected by the logic solver)	25
Fail low (detected by the logic solver)	229
Fail Dangerous Undetected (λ_{DU})	140
Fail dangerous undetected	139
Annunciation undetected (5%)	1
No part	273

Total failure rate (safety function)	1514 FIT
SFF	90.7%
DC_s	0%
DC_D	86%
MTBF	64 years

SIL AC ⁵	SIL2
----------------------------	-------------

⁴ “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

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.

The following results must be considered in combination with PFD_{AVG} / PFH values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

5.1 PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) calculation is performed for a single (1oo1D) guided wave radar transmitter Rosemount 5300 Series. The failure rate data used in this calculation are displayed in section 4.5.1. The resulting PFD_{AVG} (for a variety of proof test intervals) / PFH values are displayed in Table 4.

Table 4: PFD_{AVG} / PFH values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	
$PFD_{AVG} = 6.13E-04$	$PFD_{AVG} = 1.23E-03$	$PFD_{AVG} = 3.06E-03$	PFH = $1.40E-07$ 1/h ⁶

Figure 3 shows the time dependent curve of PFD_{AVG} .

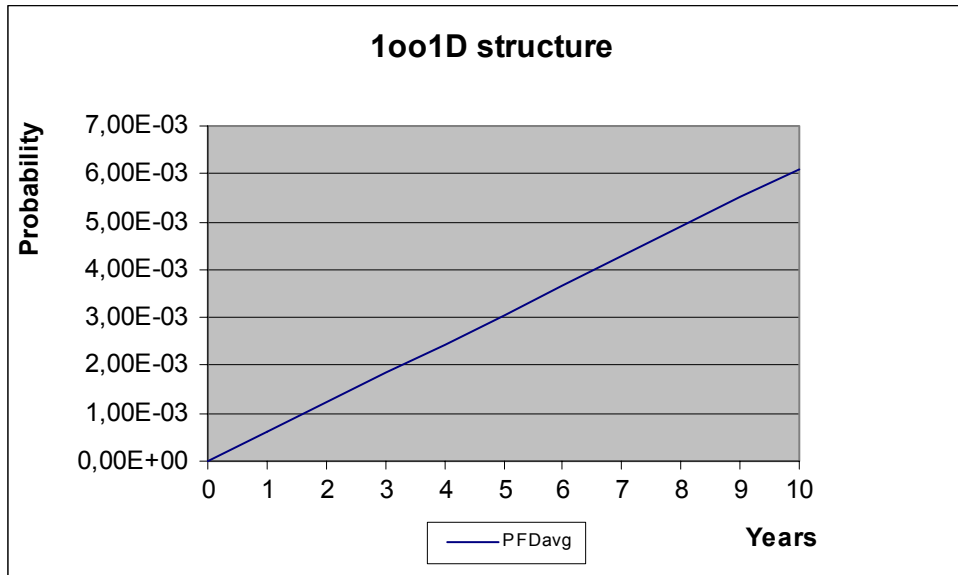


Figure 3: $PFD_{AVG}(t)$

For SIL2 applications, the PFD_{AVG} value needs to be $< 1.00E-02$. This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the guided wave radar transmitter Rosemount 5300 Series is approximately equal to 6% of the range.

For SIL2 applications, the PFH value needs to be $< 1.00E-06$ 1/h. This means that for a SIL2 application, the PFH value of the guided wave radar transmitter Rosemount 5300 Series is approximately equal to 14% of the range.

⁶ The PFH value is based on an internal fault reaction time of 90 minutes. This time interval should be compared against the demand frequency to ensure the effectiveness of the diagnostic capability of the device.

6 Terms and Definitions

DC _S	Diagnostic Coverage of safe failures
DC _D	Diagnostic Coverage of dangerous failures
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
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof test frequency.
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
PFH	Probability of dangerous Failure per Hour. The term "Probability" is misleading, correctly defined it is a Rate.
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
Type B subsystem	"Complex" subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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.

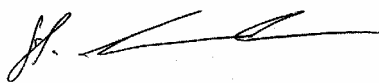
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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.

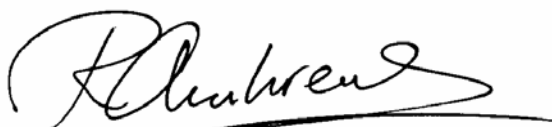
7.2 Releases

Version History: V1R0: Review comments incorporated; July 30, 2008
V0R1: Initial version; July 8, 2008
Author: Stephan Aschenbrenner
Review: V0R1: Dajana Prastalo (Rosemount Tank Radar AB), July 11, 2008
V0R1: Rachel Amkreutz (*exida*), July 29, 2008
Release status: Released to Rosemount Tank Radar AB

7.3 Release Signatures

A handwritten signature in black ink, appearing to be "S. Aschenbrenner", written over a horizontal line.

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

A handwritten signature in black ink, appearing to be "Rachel Amkreutz", written over a horizontal line.

Rachel Amkreutz, Safety Engineer

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

Appendix 2 shall be considered when writing the safety manual as it contains important safety related information.

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.

Table 5 shows an importance analysis of the most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Table 5: Importance Analysis

Component	% of total λ_{du}	Detection through
U4	11,52%	100% functional test with different input signals and monitoring of the output signal
M1	6,84%	100% functional test with different input signals and monitoring of the output signal
M8	6,48%	100% functional test with different input signals and monitoring of the output signal
V29, V30, V31	4,75%	100% functional test with different input signals and monitoring of the output signal
V1, V4	3,96%	100% functional test with different input signals and monitoring of the output signal
V2, V5	3,96%	100% functional test with different input signals and monitoring of the output signal
U201B	3,70%	100% functional test with different input signals and monitoring of the output signal
U506	2,97%	100% functional test with different input signals and monitoring of the output signal
V3,V6	2,88%	100% functional test with different input signals and monitoring of the output signal
U401B	2,88%	100% functional test with different input signals and monitoring of the output signal

Appendix 2: Possible proof tests to detect dangerous undetected faults

A possible proof test consists of the following steps, as described in Table 6.

Table 6 Steps for a possible 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. 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.
3	Perform a two-point calibration of the transmitter and verify that the analog current reaches the expected values.
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. This tests for possible quiescent current related failures
5	Set a certain level and verify that the current output corresponds to the set level
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 95% of possible “du” failures of the transmitter including the sensor element.

Appendix 3: Impact of lifetime of critical components on the failure rate

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful 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 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 which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

Table 7 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 7: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	C14, C313, C314	Appr. 500 000 hours
Sensor part		According to Rosemount manual

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.