Failure Modes, Effects and Diagnostic Analysis

Project:

Temperature transmitter PR5337 / PR6337 with 4..20 mA output

Customer:

PR electronics A/S
Rønde
Denmark

Contract No.: PR electronics A/S 11/12-052
Report No.: PR electronics A/S 11/12-052 R026
Version V1, Revision R0; February 2012

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the temperature transmitter PR5337 / PR6337 with 4..20 mA output for temperature sensors, voltage signals, resistance-type sensors and potentiometers with software version V1.1 and hardware version as shown in the referred circuit diagrams (see section 2.4.1).
Table 1 gives an overview of the considered versions of the temperature transmitter PR5337 / PR6337 with 4..20 mA output.

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

PR5337A	Temperature transmitter, head mounted – (Standard)
PR5337D	Temperature transmitter, head mounted – (ATEX, FM, CSA)
PR6337A	Temperature transmitter, rail mounted, 1 / 2-channels – (Standard)
PR6337D	Temperature transmitter, rail mounted, 1 / 2-channels – (ATEX, FM, CSA)

For safety applications only the described 4..20mA current output versions of the device were considered. All other possible variants or electronics are not covered by this report.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. This failure rate database is specified in the safety requirements specification from PR electronics A/S for the temperature transmitter PR5337 / PR6337 with 4..20 mA output.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. 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.

A full table of failure rates is presented in section 4.3.1 along with all assumptions in section 4.2.3.

The temperature transmitter PR5337 / PR6337 with 4..20 mA output is considered to be a Type B[1] element with a hardware fault tolerance of 0.

Assuming that the application program in the connected safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures of the 4..20 mA output signal, and does not automatically trip on these failures; these failures have been classified as dangerous detected failures. For these applications the following table shows the failure rates according to IEC 61508:2010 2nd edition for the temperature transmitter PR5337 / PR6337 with 4..20 mA output (considering one input and one output being part of the safety function) under worst-case assumptions.

[1] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

Table 2 Summary for PR5337 / PR6337 with 4..20 mA output – IEC 61508 failure rates

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**193**
Fail Dangerous Detected (λ_{dd})	140
Fail Annunciation Detected (λ_{AD})	0
Fail High (λ_{H})	16
Fail Low (λ_{L})	37
Fail Dangerous Undetected (λ_{DU})	**85**

Fail Annunciation Undetected (λ_{AU})	1
No effect	115
No part	65

Total failure rate of the safety function (λ_{Total})	**278**
Safe failure fraction (SFF)	**69%**
DC_D	**69%**

SIL AC [2]	**SIL 1**

MTBF	**249 years**

These failure rates are valid for the useful lifetime of the temperature transmitter PR5337 / PR6337 with 4..20 mA output (see Appendix 2).

[2] 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 that all related IEC 61508 requirements are fulfilled.

Table of Contents

Management summary 2

1 Purpose and Scope 5

2 Project management 6

2.1 *exida* 6

2.2 Roles and parties involved 6

2.3 Standards / Literature used 6

2.4 Reference documents 7

2.4.1 Documentation provided by the customer 7

2.4.2 Documentation generated by *exida* 7

3 Description of the temperature transmitters PR5337 / PR6337 8

4 Failure Modes, Effects, and Diagnostic Analysis 10

4.1 Description of the failure categories 10

4.2 Methodology – FMEDA, Failure rates 11

4.2.1 FMEDA 11

4.2.2 Failure rates 11

4.2.3 Assumptions 11

4.3 Results 12

4.3.1 Temperature transmitter PR5337 / PR6337 with 4..20 mA output 13

5 Using the FMEDA results 14

5.1 Temperature sensing devices 14

5.1.1 Thermocouple (TC) sensing devices 14

5.1.2 RTD sensing devices 15

5.2 Example PFD_{AVG} calculation 18

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: Impact of lifetime of critical components on the failure rate 22

Appendix 3: Failure rates according to IEC 61508:2000 1st Edition 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 ISO 13849-1. 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 ISO 13849-1. 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 Failure Modes, Effects and Diagnostics Analysis (FMEDA) carried out on the described temperature transmitter PR5337 / PR6337 with 4..20 mA output configurations with software version V1.1 and hardware version as shown in the referred circuit diagrams (see section 2.4.1).

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the temperature transmitter PR5337 / PR6337 with 4..20 mA output meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. This FMEDA **does not** replace a full assessment according to EC 61508 and 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 product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company 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 and parties involved

PR electronics A/S	Manufacturer of the temperature transmitter PR5337 / PR6337 with 4..20 mA output.
exida	Performed the hardware assessment.

PR electronics A/S contracted *exida* in January 2012 for 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 61508-2:2010	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, 2nd edition
[N2]	SN 29500-1:01.2004 SN 29500-1 H1:12.2005 SN 29500-2:12:2004 SN 29500-3:12.2004 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:08.1990 SN 29500-12:03.1994 SN 29500-13:03.1994 SN 29500-14:03.1994	Siemens standard with failure rates for components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	5337Auk.pdf	Datasheet "5337A - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 5337AY101-UK (1207)
[D2]	5337Duk.pdf	Datasheet "5337D - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 5337AY101-UK (1207)
[D3]	6337Auk.pdf	Datasheet "6337A - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 6337AY101-UK (1207)
[D4]	6337Duk.pdf	Datasheet "6337D - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 6337AY101-UK (1207)
[D5]	5337_BOM.xls	Parts list PR5337
[D6]	6337A2A_BOM.xls 6337A2B_BOM.xls	Parts list PR6337
[D7]	5335-1-23-PDF.pdf	5335-1-23 schematic of 23.12.11
[D8]	6335-1-01-PDF.pdf	6335-1-01 schematic of 16.11.07
[D9]	PRetop 5337 FMEDA v.6.xls	FMEDA dated 20.02.12
[D10]	PRetop 6337 FMEDA v.1.xls	FMEDA dated 22.02.12

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.4.2 Documentation generated by *exida*

[R1]	PRetop 5337 FMEDA v.4.xls of 03.02.12
[R2]	SV 5337 FMEDA report...msg of 10.02.12
[R3]	SV Comments on last FMEDA.msg of 20.02.12
[R4]	Review.txt of 22.02.12

3 Description of the temperature transmitters PR5337 / PR6337

The temperature transmitter PR5337 / PR6337 with 4..20 mA output is considered to be a Type B element with a hardware fault tolerance of 0. Figure 1 shows the two temperature transmitters PR5337 and PR6337.

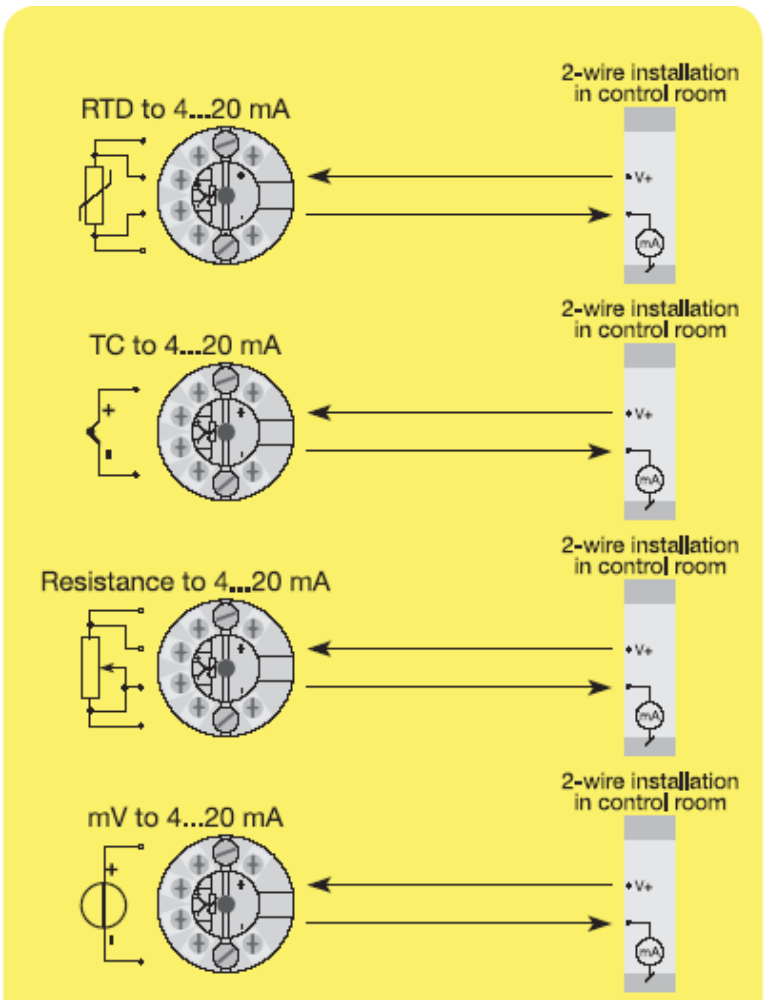
Figure 1: Temperature transmitter PR5337 and PR6337

The temperature transmitter PR5337 / PR6337 with 4..20 mA output is an isolated two-wire 4..20mA device used in many different industries for both control and safety applications. Combined with a temperature sensing device, the temperature transmitter PR5337 / PR6337 with 4..20 mA output becomes a temperature sensor assembly.

The temperature transmitter PR5337 / PR6337 with 4..20 mA output can be configured in the following 3 ways:

- With PR electronics A/S' communications interface Loop Link and PReset PC configuration software.
- With a HART® modem and PReset PC configuration software.
- With a HART® communicator with PR electronics A/S' DDL driver.

The transmitter operates with a 2-wire system. The same wires are used for the operating voltage (depending on the transmitter) and the output signal (4...20 mA) including HART® protocol. This is also indicated in the following figure.



The temperature sensing devices that can be connected to the temperature transmitter PR5337 / PR6337 with 4..20 mA output are:

- 2-, 3- and 4-wire RTD
- Thermocouple
- 2-, 3- and 4-wire resistance
- mV input

Figure 2: Input configurations with temperature transmitter PR5337 / PR6337

The FMEDAs have been performed considering the worst-case input sensor configuration.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis, documented in [D9] and [D10], was prepared by PR electronics A/S and reviewed by *exida*. When the effect of a certain component failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see fault insertion tests documented in [D9].

4.1 Description of the failure categories

In order to judge the failure behavior of the temperature transmitter PR5337 / PR6337 with 4..20 mA output configurations, the following definitions for the failure of the configurations were considered.

Fail-Safe State	The fail-safe state is defined as the output reaching the user defined threshold value.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
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.
Fail High	A fail high failure (H) is defined as a failure that causes the output signal to go to the maximum output current (> 21mA).
Fail Low	A fail low failure (L) is defined as a failure that causes the output signal to go to the minimum output current (< 3.6mA).
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.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous 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.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. 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. 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”.

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.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the temperature transmitter PR5337 / PR6337 with 4..20 mA output converter configurations.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The device is installed per manufacturer’s instructions.

- 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.
- The device is locked against unintended operation/modification.
- The worst-case internal fault detection time is 5 minutes.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- Only the described HW and SW versions are used for safety applications.
- The device is operated in the low demand mode of operation.
- The safety function is carried out via 1 input and 1 output channel.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment with an average temperature over a long period of time of 40ºC. 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 (daily fluctuation of > 15°C) must be assumed. Other environmental characteristics are assumed to be within the manufacturer's ratings.
- Only the 4..20mA current output is used for safety applications.
- The 4..20 mA output signal is fed to a SIL 2 compliant analog input board of a safety PLC.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures of the 4..20 mA output signal, and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

4.3 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:

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

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

$DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{no\ effect} + \lambda_{AU})) + 24\ h$

4.3.1 Temperature transmitter PR5337 / PR6337 with 4..20 mA output

The FMEDA carried out on the temperature transmitter PR5337 / PR6337 with 4..20 mA output leads under the assumptions described in section 4.2.3 to the following worst-case failure rates:

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**193**
Fail Dangerous Detected (λ_{dd})	140
Fail Annunciation Detected (λ_{AD})	0
Fail High (λ_{H})	16
Fail Low (λ_{L})	37
Fail Dangerous Undetected (λ_{DU})	**85**

Fail Annunciation Undetected (λ_{AU})	1
No effect	115
No part	65

Total failure rate of the safety function (λ_{Total})	**278**
Safe failure fraction (SFF)	**69%**
DC_D	**69%**

SIL AC [3]	**SIL 1**

MTBF	**249 years**

[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 that all related IEC 61508 requirements are fulfilled.

5 Using the FMEDA results

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

5.1 Temperature sensing devices

A temperature transmitter PR5337 / PR6337 with 4..20 mA output together with a temperature sensing device becomes a temperature sensor assembly. When using the results of the FMEDA in a SIL verification assessment also the failure rates and failure modes of the temperature sensing device must be considered.

5.1.1 Thermocouple (TC) sensing devices

The failure mode distribution for thermocouples varies in published literature but there is strong agreement that open circuit or "burn-out" failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 3 and Table 4, when thermocouples are supplied from the temperature transmitter PR5337 / PR6337 with 4..20 mA output. The drift failure mode is primarily due to T/C aging. The temperature transmitter PR5337 / PR6337 with 4..20 mA output will detect a thermocouple burn-out failure and drive its output to the specified failure state.

Table 3 Typical failure rates for thermocouples (with extension wire)

Thermocouple Failure Mode Distribution	***Low Stress***	***High Stress***
Open Circuit (Burn-out)	900 FIT	18000 FIT
Short Circuit (Temperature measurement in error)	50 FIT	1000 FIT
Drift (Temperature measurement in error)	50 FIT	1000 FIT

Table 4 Typical failure rates for thermocouples (close coupled)

Thermocouple Failure Mode Distribution	***Low Stress***	***High Stress***
Open Circuit (Burn-out)	95 FIT	1900 FIT
Short Circuit (Temperature measurement in error)	4 FIT	80 FIT
Drift (Temperature measurement in error)	1 FIT	20 FIT

A complete temperature sensor assembly consisting of a temperature transmitter PR5337 / PR6337 with 4..20 mA output and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Assuming that the temperature transmitter PR5337 / PR6337 with 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple, the failure rate contribution for the thermocouple is:

Low stress environment (close coupled)	**High stress environment (close coupled)**
λ_{dd} = 95 FIT	λ_{dd} = 1900 FIT
λ_{du} = 4 FIT + 1 FIT = 5 FIT	λ_{du} = 80 FIT + 20 FIT = 100 FIT

Low stress environment (extension wire)	**High stress environment (extension wire)**
λ_{dd} = 900 FIT	λ_{dd} = 18000 FIT
λ_{du} = 50 FIT + 50 FIT = 100 FIT	λ_{du} = 1000 FIT + 1000 FIT = 2000 FIT

This results in a failure rate distribution and a SFF of:

Table 5: PR5337 / PR6337 with TC

Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Low stress, close coupled	0 FIT	0 FIT	288 FIT	90 FIT	76%
Low stress, with ext. wire	0 FIT	0 FIT	1093 FIT	185 FIT	85%
High stress, close coupled	0 FIT	0 FIT	2093 FIT	185 FIT	91%
High stress, with ext. wire	0 FIT	0 FIT	18193 FIT	2085 FIT	89%

5.1.2 RTD sensing devices

The failure mode distribution for an RTD also depends on the application with the key variables being stress level, RTD wire length and RTD type (2/3 wire or 4 wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions are shown in Table 6 to Table 9. The temperature transmitter PR5337 / PR6337 with 4..20 mA output will detect open circuit, short circuit and a certain percentage of drift RTD failures and drive its output to the specified failure state.

Table 6 Typical failure rates for 4-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	410 FIT	8200 FIT
Short Circuit (Temperature measurement in error)	20 FIT	400 FIT
Drift (Temperature Measurement in error)	70 FIT [4]	1400 FIT [5]

Table 7 Typical failure rates for 4-Wire RTDs (close coupled)

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	41,5 FIT	830 FIT
Short Circuit (Temperature measurement in error)	2,5 FIT	50 FIT
Drift (Temperature Measurement in error)	6 FIT [6]	120 FIT [7]

Table 8 Typical failure rates for 2/3-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	370,5 FIT	7410 FIT
Short Circuit (Temperature measurement in error)	9,5 FIT	190 FIT
Drift (Temperature Measurement in error)	95 FIT	1900 FIT

[4] It is assumed that 65 FIT are detectable if the 4-wire RTD is correctly used.

[5] It is assumed that 1300 FIT are detectable if the 4-wire RTD is correctly used.

[6] It is assumed that 3.5 FIT are detectable if the 4-wire RTD is correctly used.

[7] It is assumed that 70 FIT are detectable if the 4-wire RTD is correctly used.

Table 9 Typical failure rates for 2/3-Wire RTDs (close coupled)

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	37,92 FIT	758,4 FIT
Short Circuit (Temperature measurement in error)	1,44 FIT	28,8 FIT
Drift (Temperature Measurement in error)	8,64 FIT	172,8 FIT

A complete temperature sensor assembly consisting of a temperature transmitter PR5337 / PR6337 with 4..20 mA output and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.
Assuming that the temperature transmitter PR5337 / PR6337 with 4..20 mA output will go to the pre-defined alarm state on a detected failure of the RTD, the failure rate contribution for the RTD is:

4-Wire RTD close coupled:

Low stress environment	**High stress environment**
λ_{dd}= 41,5 FIT + 2,5 FIT + 3,5 FIT =47,5 FIT	λ_{dd}= 830 FIT + 50 FIT + 70 FIT = 950 FIT
λ_{du}= 2,5 FIT	λ_{du}= 50 FIT

4-Wire RTD with extension wire:

Low stress environment	**High stress environment**
λ_{dd}= 410 FIT + 20 FIT + 65 FIT = 495 FIT	λ_{dd}= 8200 FIT + 400 FIT + 1300 FIT = 9900 FIT
λ_{du}= 5 FIT	λ_{du}= 100 FIT

2/3-Wire RTD close coupled:

Low stress environment	**High stress environment**
λ_{dd}= 37,92 FIT + 1,44 FIT = 39,36 FIT	λ_{dd}= 758,4 FIT + 28,8 FIT = 787,2 FIT
λ_{du}= 8,64 FIT	λ_{du}= 172,8 FIT

2/3-Wire RTD with extension wire:

Low stress environment	**High stress environment**
λ_{dd}= 370,5 FIT + 9,5 FIT = 380 FIT	λ_{dd}= 7410 FIT + 190 FIT = 7600 FIT
λ_{du}= 95 FIT	λ_{du}= 1900 FIT

This results in a failure rate distribution and SFF of:

Table 10: PR5337 / PR6337 with 4-Wire RTD

Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Low stress, close coupled	0 FIT	0 FIT	241 FIT	88 FIT	73%
Low stress, with ext. wire	0 FIT	0 FIT	688 FIT	90 FIT	88%
High stress, close coupled	0 FIT	0 FIT	1143 FIT	135 FIT	89%
High stress, with ext. wire	0 FIT	0 FIT	10093 FIT	185 FIT	98%

Table 11: PR5337 / PR6337 with 2/3-Wire RTD

Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Low stress, close coupled	0 FIT	0 FIT	232 FIT	94 FIT	71%
Low stress, with ext. wire	0 FIT	0 FIT	573 FIT	180 FIT	76%
High stress, close coupled	0 FIT	0 FIT	980 FIT	258 FIT	79%
High stress, with ext. wire	0 FIT	0 FIT	7793 FIT	1985 FIT	79%

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions.

5.2 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for the temperature transmitter PR5337 / PR6337 with 4..20 mA output, considering a proof test coverage of 95% and a mission time of 10 years. The failure rate data used in these calculations are displayed in section 4.3.1.

For SIL 2 applications, the PFD_{AVG} value needs to be < 1.00E-02.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 5.41E-04	PFD_{AVG} = 8.93E-04	PFD_{AVG} = 1.95E-03

As the temperature transmitter PR5337 / PR6337 with 4..20 mA output is a part of an entire safety function it should only consume a certain percentage of the allowed range. Assuming 25% of this range as a reasonable budget it should be better than or equal to 2.50E-03 for SIL2. The calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 25% of this range, i.e. to be better than or equal to 2.50E-03. Figure 3 shows the time dependent curve of PFD_{AVG} for the analyzed temperature transmitter PR5337 / PR6337 with 4..20 mA output.

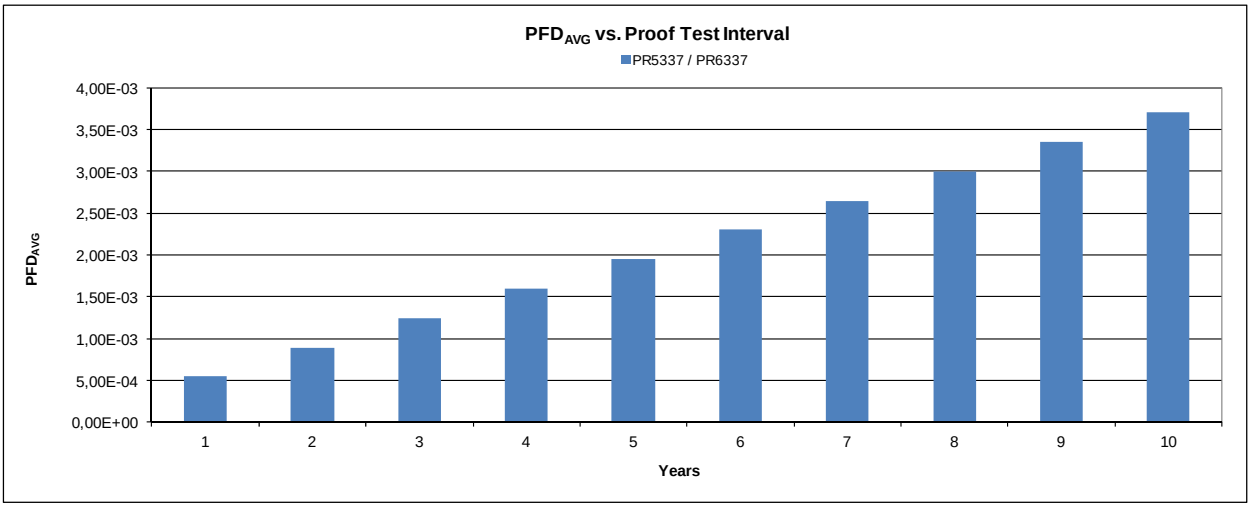


Figure 3 $PFD_{AVG}(t)$

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 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

DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration
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
Type B element	“Complex” element (using micro controllers or programmable logic). For details see 7.4.4.1.3 of IEC 61508-2, 2nd edition
T[Proof]	Proof Test Interval

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.

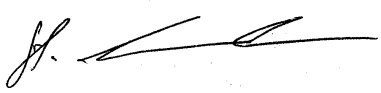
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market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

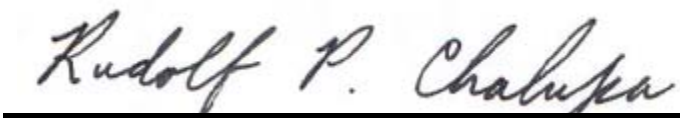
7.2 Releases

Version History:	V1R0:	Review comments incorporated; February 27, 2012
	V0R1:	Initial version; February 22, 2012
Authors:	Stephan Aschenbrenner	
Review:	V0R1:	Rudolf P. Chalupa (*exida*); February 24, 2012
		Dennis Gregersen (PR electronics A/S); February 23, 2012
Release status:	Released to PR electronics A/S	

7.3 Release Signatures



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



Rudolf P. Chalupa, Senior Safety Engineer

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

According to section 7.4.5.2 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.

A possible proof test consists of the following steps:

Step	Action
1	Bypass the safety PLC or take other appropriate actions to avoid a false trip
2	Perform a multi-point calibration of the temperature transmitter covering the applicable temperature range
3	Apply an adequate input signal to reach the pre-defined alarm level and verify that the safe state is reached (The analog current output corresponds to the provided input signal).
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

It is assumed that this proof test will detect 95% of possible “du” failures in the device.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 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 4.2.3) this only applies provided that the useful lifetime[8] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is 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, electrolytic 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 12 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 12: Useful lifetime of components with reduced useful lifetime contributing to λ_{du}

Type	Useful lifetime
Tantalum electrolytic (C40)	Approximately 500000 hours
Temperature sensor	According to manufacturer specification

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

[8] 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 3: Failure rates according to IEC 61508:2000 1st Edition

Table 13 Summary for temperature transmitter PR5337 / PR6337 with 4..20 mA output

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**116**
Fail Safe Undetected (λ_{su})	0
No effect	115
Fail Annunciation Undetected (λ_{AU})	1
Fail Dangerous Detected (λ_{DD})	**193**
Fail Dangerous Detected (λ_{dd})	140
Fail Annunciation Detected (λ_{AD})	0
Fail High (λ_{H})	16
Fail Low (λ_{L})	37
Fail Dangerous Undetected (λ_{DU})	**85**

No part	65

Total failure rate of the safety function (λ_{Total})	**394**
Safe failure fraction (SFF)	**78%**
DC_D	**69%**

SIL AC [9]	**SIL 1**

MTBF	**249 years**

[9] 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 that all related IEC 61508 requirements are fulfilled.