



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

Project:

Temperature Transmitter PRetop 5335 with 4..20 mA output  
Temperature Transmitter PReTrans 6335 with 4..20 mA output

Customer:

**PR electronics A/S**  
Rønde  
Denmark

Contract No.: PR electronics 04/10-25  
Report No.: PR electronics 04/10-25 R001  
Version V1, Revision R1.4, November 2005  
Audun Opem

## Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the temperature transmitter PRetop 5335 with 4..20 mA output. Table 1 gives an overview of the different types that belong to the considered temperature transmitter. The PReTrans 6335 with 4..20 mA output is a DIN rail mounted 1- and 2-channel version with identical FW and HW. The difference is in the housing. The 2 channels are isolated and independent.

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**

PRetop 5335A	Temperature transmitter, head mounted 5335A – (Standard)
PRetop 5335B	Temperature transmitter, head mounted 5335B – (ATEX)
PRetop 5335C	Temperature transmitter, head mounted 5335C – (ATEX, FM)
PRetop 5335D	Temperature transmitter, head mounted 5335D – (ATEX, FM, CSA)
PReTrans 6335A	Temperature transmitter, rail mounted 6335A, 1 / 2-ch. – (Standard)
PReTrans 6335B	Temperature transmitter, rail mounted 6335B, 1 / 2-ch. – (ATEX)
PReTrans 6335C	Temperature transmitter, rail mounted 6335B, 1 / 2-ch. – (ATEX, FM)
PReTrans 6335D	Temperature transmitter, rail mounted 6335B, 1 / 2-ch. – (ATEX, FM, CSA)

For safety applications only the 4..20 mA output was considered. All other possible output variants or electronics are not covered by this report. The temperature transmitter PRetop 5335 / PReTrans 6335 can be programmed with a PC with Loop Link or via HART.

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

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be between  $\geq 10^{-2}$  to  $< 10^{-1}$  for SIL 1 safety functions. A generally accepted distribution of  $PFD_{AVG}$  values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF  $PFD_{AVG}$  value is caused by the sensor part. For a SIL 1 application the total  $PFD_{AVG}$  value of the SIF should be smaller than 1,00E-01, hence the maximum allowable  $PFD_{AVG}$  value for the sensor assembly consisting of PRetop 5335 / PReTrans 6335 and a thermocouple or RTD supplied with PRetop 5335 / PReTrans 6335 would then be 3,50E-02.

The temperature transmitter PRetop 5335 / PReTrans 6335 with 4..20 mA output is considered to be a Type B<sup>1</sup> component with a hardware fault tolerance of 0.

For type B components with a hardware fault tolerance of 0 a SFF of 60% to < 90% is sufficient according to table 3 of IEC 61508-2 for SIL 1 (sub-) systems.

---

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

**Table 2: Summary for PRetop 5335 / PReTrans 6335 – Failure rates**

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	223
Fail detected (internal diagnostics)	190
Fail Low (detected by the logic solver)	16
Fail High (detected by the logic solver)	17
Fail Dangerous Undetected	175
No Effect	140
Annunciation Undetected	2
Not part	39
MTBF = MTTF + MTTR	197 years

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on whether the temperature transmitter PRetop 5335 / PReTrans 6335 output is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following table shows how the above stated requirements are fulfilled.

**Transmitter configured fail-safe state = “fail high” or “fail low”**

Failure Categories	$I_{sd}$	$I_{su}$	$I_{dd}$	$I_{du}$	SFF
PRetop 5335 / PReTrans 6335	0 FIT	142 FIT	223 FIT	175 FIT	67,50%

It is important to realize that the “No Effect” failures and the “Annunciation Undetected” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

**Table 3: Summary for PRetop 5335 / PReTrans 6335 – PFD<sub>AVG</sub> values**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD <sub>AVG</sub> = 7,68E-04	PFD <sub>AVG</sub> = 3,83E-03	PFD <sub>AVG</sub> = 7,65E-03

A complete temperature sensor assembly consisting of PRetop 5335 / PReTrans 6335 and a thermocouple or cushioned RTD supplied with PRetop 5335 / PReTrans 6335 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.

Section 5.2 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

Assuming that PRetop 5335 / PReTrans 6335 is programmed to drive its output high on detected failures of the thermocouple or RTD ( $\lambda_{low} = \lambda_{dd}$ ,  $\lambda_{high} = \lambda_{dd}$ ), the failure rate contribution or the PFD<sub>AVG</sub> value for the thermocouple or RTD in a low stress environment is as follows:

**Table 4: Summary for the sensor assembly PRetop 5335 / PReTrans 6335 / thermocouple in low stress environment**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
<b>PFD<sub>AVG</sub> = 1,86E-03</b>	<b>PFD<sub>AVG</sub> = 9,30E-03</b>	<b>PFD<sub>AVG</sub> = 1,86E-02</b>	<b>92 %</b>

$$\lambda_{sd} = 0 \text{ FIT}$$

$$\lambda_{su} = 142 \text{ FIT}$$

$$\lambda_{dd} = 4973 \text{ FIT}$$

$$\lambda_{du} = 425 \text{ FIT}$$

**Table 5: Summary for the sensor assembly PRetop 5335 / PReTrans 6335 / 4-wire RTD in low stress environment**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
<b>PFD<sub>AVG</sub> = 8,54E-04</b>	<b>PFD<sub>AVG</sub> = 4,27E-03</b>	<b>PFD<sub>AVG</sub> = 8,54E-03</b>	<b>92 %</b>

$$\lambda_{sd} = 0 \text{ FIT}$$

$$\lambda_{su} = 142 \text{ FIT}$$

$$\lambda_{dd} = 2203 \text{ FIT}$$

$$\lambda_{du} = 195 \text{ FIT}$$

**Table 6: Summary for the sensor assembly PRetop 5335 and a closely coupled 2/3-wire RTD in low stress environment**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
<b>PFD<sub>AVG</sub> = 2,52E-03</b>	<b>PFD<sub>AVG</sub> = 1,26E-02</b>	<b>PFD<sub>AVG</sub> = 2,52E-02</b>	<b>77 %</b>

$$\lambda_{sd} = 0 \text{ FIT}$$

$$\lambda_{su} = 142 \text{ FIT}$$

$$\lambda_{dd} = 1823 \text{ FIT}$$

$$\lambda_{du} = 575 \text{ FIT}$$

**Table 7: Summary for the sensor assembly PReTrans 6335 and an extension wired 2/3-wire RTD in low stress environment**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
<b>PFD<sub>AVG</sub> = 2,96E-03</b>	<b>PFD<sub>AVG</sub> = 1,48E-02</b>	<b>PFD<sub>AVG</sub> = 2,96E-02</b>	<b>72 %</b>

$$\lambda_{sd} = 0 \text{ FIT}$$

$$\lambda_{su} = 142 \text{ FIT}$$

$$\lambda_{dd} = 1623 \text{ FIT}$$

$$\lambda_{du} = 675 \text{ FIT}$$

The boxes marked in green ( ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 1 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to  $3,50E-02$ .

A user of the temperature transmitter PRetop 5335 / PRetrans 6335 with 4..20 mA output 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 5.1 along with all assumptions.

The failure rates listed above do not include failures resulting from incorrect use of the temperature transmitter PRetop 5335 / PRetrans 6335, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

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 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.

The failure rates are valid for the useful life of the temperature transmitter PRetop 5335 / PRetrans 6335 with 4..20 mA output, which is estimated to be between 8 and 12 years (see Appendix 2).

## Table of Contents

Management summary.....	2
1 Purpose and Scope.....	7
2 Project management .....	8
2.1 <i>exida.com</i> .....	8
2.2 Roles of the parties involved.....	8
2.3 Standards / Literature used .....	8
2.4 Reference documents.....	9
2.4.1 Documentation provided by the customer.....	9
2.4.2 Documentation generated by <i>exida.com</i> .....	9
3 Description of the analyzed module .....	10
4 Failure Modes, Effects, and Diagnostics Analysis .....	12
4.1 Description of the failure categories .....	12
4.2 Methodology – FMEDA, Failure rates .....	13
4.2.1 FMEDA.....	13
4.2.2 Failure rates .....	13
4.2.3 Assumptions.....	14
5 Results of the assessment .....	15
5.1 PRetop 5335 / PRetrans 6335.....	16
5.2 Using the FMEDA results.....	18
5.2.1 PRetop 5335 / PRetrans 6335 with thermocouple .....	18
5.2.2 PRetop 5335 / PRetrans 6335 with RTD.....	19
6 Terms and Definitions .....	21
7 Status of the document .....	22
7.1 Liability.....	22
7.2 Releases.....	22
7.3 Release Signatures .....	22
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test.	23
Appendix 1.1: Critical failure modes contributing to $\lambda_{du}$ .....	24
Appendix 1.2: Possible proof tests to detect dangerous undetected faults .....	24
Appendix 2: Impact of lifetime of critical components on the failure rate .....	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.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ( $PFD_{AVG}$ ).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the software development process

### Option 2: Hardware assessment with prior-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ( $PFD_{AVG}$ ). In addition this option consists of an assessment of the prior-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

### Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

### **This assessment shall be done according to option 1.**

This document shall describe the results of the assessment carried out on the temperature transmitter PRetop 5335 / PReTrans 6335. Table 1 gives an overview of the series and explains the differences between the different types.

It shall be assessed whether the transmitter meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints for SIL 1 / SIL 2 sub-systems according to IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

## 2 Project management

### 2.1 exida.com

*exida.com* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* 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.com* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the temperature transmitter PRetop 5335 / PReTrans 6335
<i>exida.com</i>	Performed the hardware assessment according to option 1 (see section 1).

PR electronics A/S contracted *exida.com* in November 2004 and in October 2005 with the FMEDA and PFD<sub>AVG</sub> calculation of the above mentioned devices.

### 2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Deleted	Deleted
[N3]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N4]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N5]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N6]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N7]	SN 29500	Failure rates of components
[N8]	NSWC-98/LE1	Handbook of Reliability Prediction Procedures for Mechanical Equipment

## 2.4 Reference documents

### 2.4.1 Documentation provided by the customer

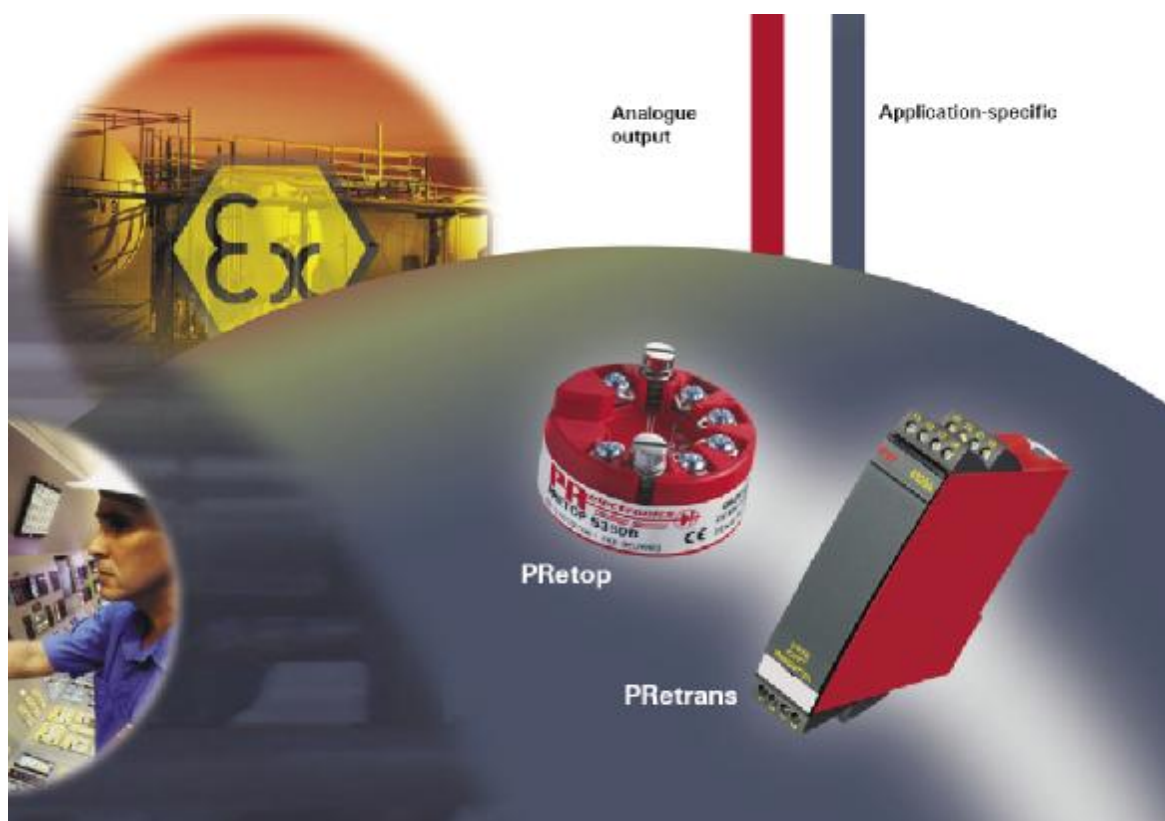
[D1]	5335AY108-UK (0435) PRetop 5335A "2-wire transmitter, with Hart® protocol"	Data sheet
[D2]	5335BY108-UK (0435) PRetop 5335B "2-wire transmitter, with Hart® protocol"	Data sheet
[D3]	5335V "5335 2-wire Transmitters with HART protocol"	Users Manual
[D4]	5335-1011 A of 15.06.2004	Circuit diagram "5335 Input"
[D5]	5335-1011 of 15.06.2004	Circuit diagram "5335 output"
[D6]	5335smd Rev. xx	Parts list
[D7]	DS00097T Microchip Reliability Report	2nd Quarter 2004
[D8]	SV UNCHECKED FMEDA.msg	Email from PR electronics 24-Feb-2005
[D9]	5335 input modes failures.xls	Behavior differences for mV, TC and RTD
[D10]	6335 2-wire HART Transmitter	Users manual
[D11]	6335-2A version 2022, dated 04/10-05	Parts List, 1-channel Ex-version 6335
[D12]	6335-2B version 2021, dated 04/10-05	Parts List, 2-channel, Ex-version 6335
[D13]	Letter from PR electronics A/S dated 2005.10.06	Manufacturer Declaration

### 2.4.2 Documentation generated by *exida.com*

[R1]	PRetop 5335 09-12 revised 1 apr.xls (FMEDA)
------	---

### 3 Description of the analyzed module

The temperature transmitter PRetop 5335 / PReTrans 6335 is an isolated two-wire 4...20 mA device used in many different industries for both control and safety applications. Combined with a temperature sensing device, the temperature transmitter PRetop 5335 / PReTrans 6335 becomes a temperature sensor assembly.



**Figure 1 PRetop 5335 / PReTrans 6335 temperature transmitter**

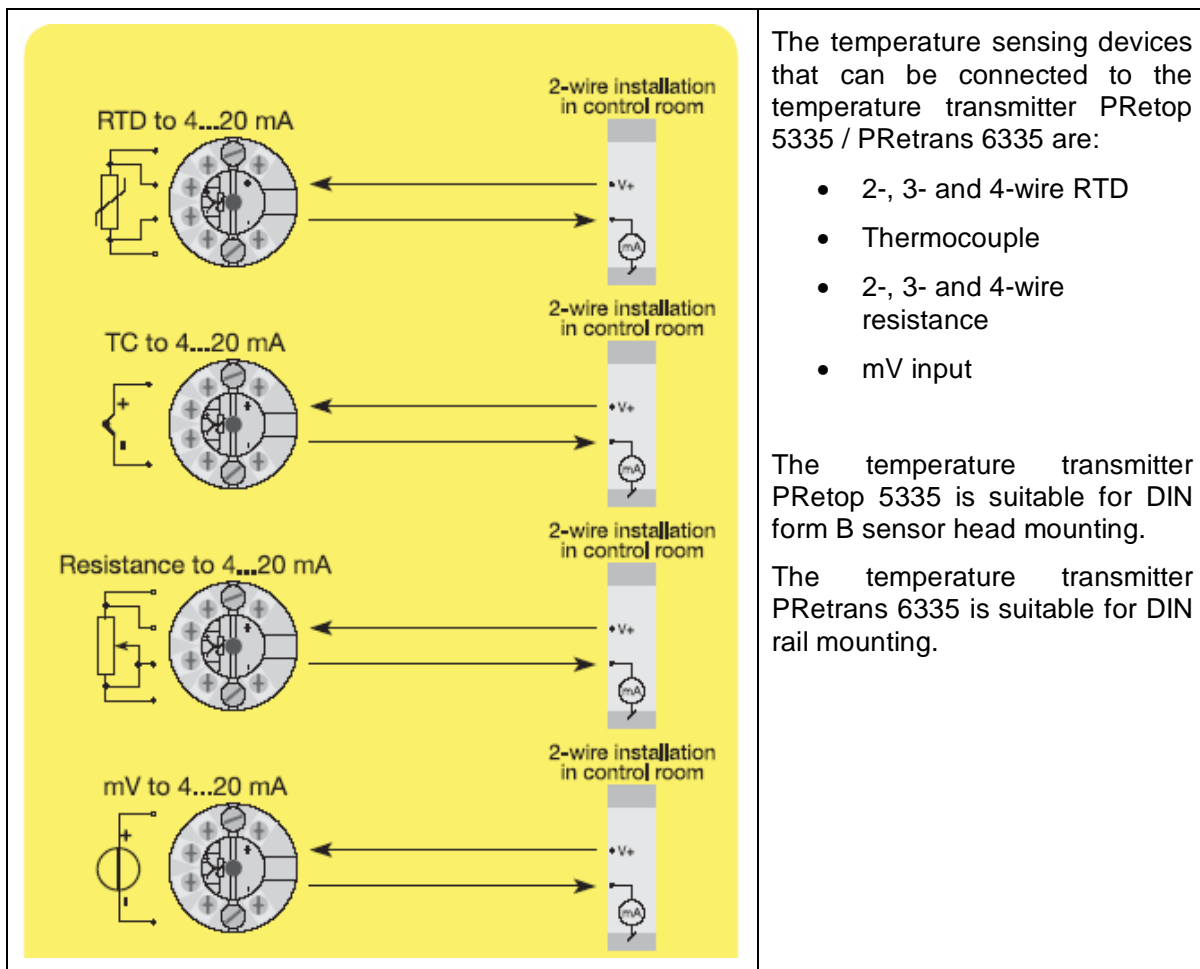
PRetop 5335 / PReTrans 6335 can be configured in the following 3 ways:

- 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 temperature transmitter PRetop 5335 / PReTrans 6335 is considered to be a Type B component with a hardware fault tolerance of 0.

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 PRetop 5335 / PReTrans 6335 are:

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

The temperature transmitter PRetop 5335 is suitable for DIN form B sensor head mounting.

The temperature transmitter PReTrans 6335 is suitable for DIN rail mounting.

**Figure 2: Input configurations with temperature transmitter PRetop 5335 / PReTrans 6335**

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

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with PR electronics A/S and is documented in [R1]. When the effect of a certain 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. This resulted in failures that can be classified according to the following failure categories.

### 4.1 Description of the failure categories

In order to judge the failure behavior of the temperature transmitter PRetop 5335 / PRetrans 6335, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output being controlled according to NE 43, i.e. current < 3.6 mA or current > 21 mA. Depending on the application the fail-safe state is defined as the output going to fail low or fail high.
Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	A dangerous failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 2% 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 (These failures may be converted to the selected fail-safe state).
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)
Fail No Effect	Failure of a component that is part of the safety function but has no effect on the safety function or deviates the output current by not more than 2% full span. For the calculation of the SFF it is treated like a safe undetected failure.
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. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which is not part of the safety function but 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, depending on the application programming of the safety logic solver a fail low or fail high can either be dangerous detected or safe detected. Consequently during Safety Integrity Level (SIL) verification assessment the fail high and fail low categories need to be classified as either safe detected (S) or dangerous detected (DD).

The “No Effect” and “Annunciation Undetected” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the “No Effect” and “Annunciation Undetected” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

## **4.2 Methodology – FMEDA, Failure rates**

### **4.2.1 FMEDA**

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

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

### **4.2.2 Failure rates**

The failure rate data used by *exida.com* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

### 4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the temperature transmitter PRetop 5335 / PReTrans 6335:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- All modules are operated in the low demand mode of operation.
- The safety function is carried out via 1 input and 1 output channel.
- Only the current output 4..20 mA is used for safety applications.
- External power supply failure rates are not included.
- The application program in the safety logic solver is constructed in such a way that fail low and fail high failures are detected regardless of the effect, safe or dangerous, on the safety function.

## 5 Results of the assessment

exida.com did the FMEDAs together with PR electronics A/S.

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

$\lambda_{total}$  consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$$

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

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

For the calculation of the  $PFD_{AVG}$  the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the Microsoft® Excel 2000 based FMEDA tool of exida.com as a simulation tool. The results are documented in the following sections.

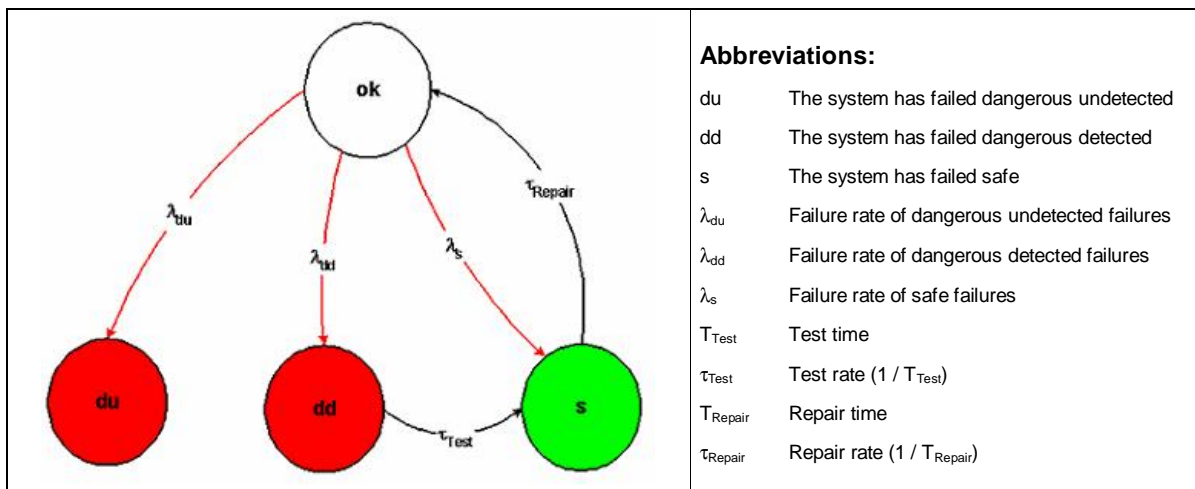


Figure 3: Markov model for a 1oo1D structure

## 5.1 PRetop 5335 / PReTrans 6335

The FMEDA carried out on the temperature transmitter PRetop 5335 / PReTrans 6335 leads under the assumptions described in section 4.2.3 to the following failure rates:

$$\lambda_{su} = \lambda_{su} + 0,5 \cdot \lambda_{not\ considered} = 1,15E-07\ 1/h + 3,0E-10\ 1/h = 1,15E-07\ 1/h$$

$$\lambda_{dd} = 7,50E-08\ 1/h$$

$$\lambda_{du} = \lambda_{du} + 0,5 \cdot \lambda_{not\ considered} = 1,75E-07\ 1/h + 3,0E-10\ 1/h = 1,75E-07\ 1/h$$

$$\lambda_{high} = 1,58E-08\ 1/h$$

$$\lambda_{low} = 1,68E-08\ 1/h$$

$$\lambda_{no\ effect} = 1,40E-07\ 1/h$$

$$\lambda_{annunciation} = 1,80E-09\ 1/h$$

$$\lambda_{total} = 5,40E-07\ 1/h$$

$$\lambda_{not\ part} = 3,93E-08\ 1/h$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not\ part}) + 8\ h = 197\ years$$

These failure rates can be turned over into the following typical transmitter failure rates:

Failure category	Failure rate (in FITs)
Fail Dangerous Detected	223
Fail detected (internal diagnostics)	190
Fail Low (detected by the logic solver)	16
Fail High (detected by the logic solver)	17
Fail Dangerous Undetected	175
No Effect	140
Annunciation Undetected	2
Not part	39
MTBF = MTTF + MTTR	197 years

Under the assumptions described in section 5 the following table shows the failure rates according to IEC 61508:

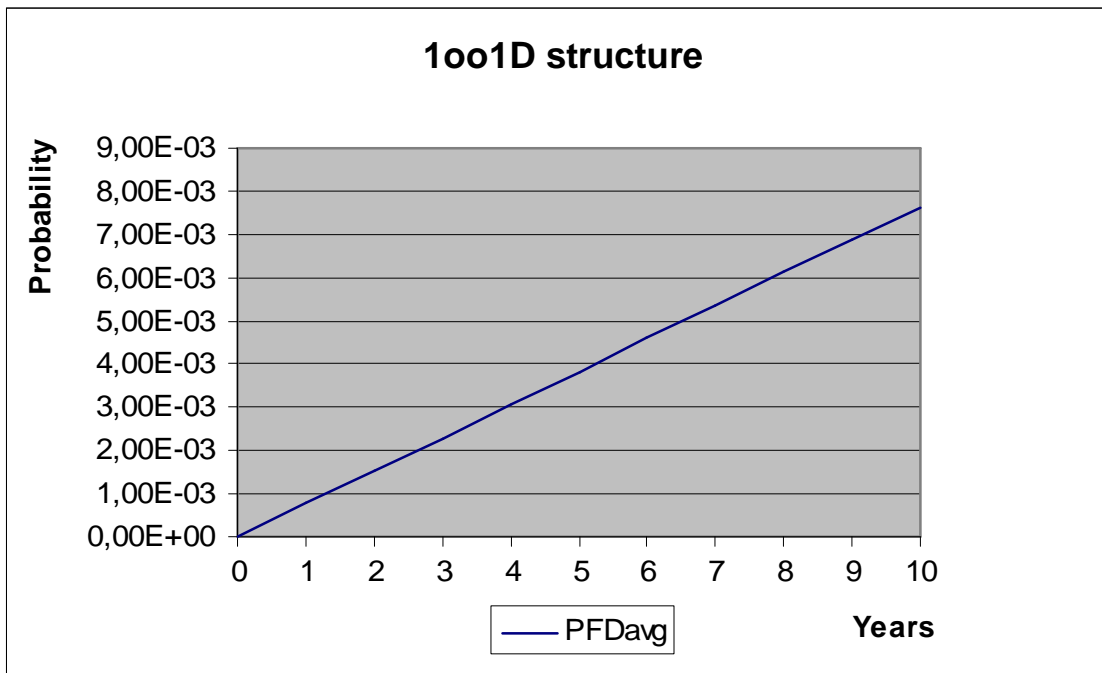
**Transmitter configured fail-safe state = “fail high” or “fail low”**

Failure Categories	$l_{sd}$	$l_{su}$	$l_{dd}$	$l_{du}$	SFF
PRetop 5335 / PRetrans 6335	0 FIT	142 FIT	223 FIT	175 FIT	67,50%

The  $PFD_{AVG}$  for the electronic part was calculated for three different proof test times using the Markov model as described in Figure 3.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{AVG} = 7,68E-04$	$PFD_{AVG} = 3,83E-03$	$PFD_{AVG} = 7,65E-03$

The boxes marked in green ( ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 1 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to  $3,50E-02$ . Figure 4 shows the time dependent curve of  $PFD_{AVG}$ .



**Figure 4: PFD<sub>AVG</sub>(t)**

## 5.2 Using the FMEDA results

The temperature transmitter PRetop 5335 / PReTrans 6335 together with a temperature sensing device becomes a temperature sensor assembly as indicated in Figure 2. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered. Typical failure rates for thermocouples are listed in the following table.

**Table 8 Typical failure rates for thermocouples**

<i>Temperature sensing device</i>	<i>Failure rate (in FIT)</i>
Thermocouple low stress environment	5.000
Thermocouple high stress environment	20.000

### 5.2.1 PRetop 5335 / PReTrans 6335 with thermocouple

The failure mode distributions for thermocouples vary 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 9 when thermocouples are supplied with the temperature transmitter PRetop 5335 / PReTrans 6335. The drift failure mode is primarily due to T/C aging. The temperature transmitter PRetop 5335 / PReTrans 6335 will detect a thermocouple burn-out failure and drive its output to the specified failure state.

**Table 9 Typical failure mode distributions for thermocouples**

<i>Thermocouple Failure Mode Distribution</i>	<i>Percentage</i>
Open Circuit (Burn-out)	95%
Wire Short (Temperature measurement in error)	1%
Drift (Temperature measurement in error)	4%

A complete temperature sensor assembly consisting of the temperature transmitter PRetop 5335 / PReTrans 6335 and a thermocouple supplied with PRetop 5335 / PReTrans 6335 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 PRetop 5335 / PReTrans 6335 is programmed to drive its output either high or low on detected failures of the thermocouple (Fail low (L) = DD, Fail High (H) = DD), the failure rate contribution for the thermocouple in a low stress environment is:

- $\lambda_{dd} = (5.000 \text{ FIT}) * (0,95) = 4.750 \text{ FIT}$
- $\lambda_{du} = (5.000 \text{ FIT}) * (0,05) = 250 \text{ FIT}$

This results in a failure rate distribution, SFF and PFD<sub>AVG</sub> (assuming T[Proof] = 1 year) to:

$I_{sd}$	$I_{su}$	$I_{dd}$	$I_{du}$	<b>SFF</b>	<b>PFD<sub>AVG</sub></b>
0 FIT	142 FIT	4973 FIT	425 FIT	92,33 %	1,86E-03

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

## 5.2.2 PRetop 5335 / PReTrans 6335 with RTD

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 for a low stress environment are shown in Table 10 and Table 11. The temperature transmitter PRetop 5335 / PReTrans 6335 will detect open circuit and short circuit RTD failures and drive it's output to the specified failure state.

**Table 10 Typical failure rate for 4-Wire RTDs in a Low Stress environment**

<i>RTD Failure Mode Distribution</i>	<i>Close – Coupled / Extension wired</i>
Open Circuit	1400 FIT
Short Circuit	580 FIT
Drift (Temperature Measurement in error)	20 FIT

**Table 11 Typical failure rates for 2/3-Wire RTDs in a Low Stress environment or using a cushioned / extension wired sensor construction assuming absolute worst-case**

<i>RTD Failure Mode Distribution</i>	<i>Extension wired</i>	<i>Close – Coupled</i>
Open Circuit	800	1000 FIT
Short Circuit	600	600 FIT
Drift (Temperature Measurement in error)	600	400 FIT

A complete temperature sensor assembly consisting of the temperature transmitter PRetop 5335 and a closely coupled, cushioned 4-wire RTD supplied with PRetop 5335 or the temperature transmitter PReTrans 6335 and an extension wired 4-wire RTD supplied with PReTrans 6335 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 PRetop 5335 / PReTrans 6335 is programmed to drive its output either high or low on a detected failure of the RTD (Fail low (L) = DD, Fail High (H) = DD), the failure rate contribution for the 4-wire RTD in a low stress environment is:

- $\lambda_{dd} = 1400 \text{ FIT} + 580 \text{ FIT} = 1980 \text{ FIT}$
- $\lambda_{du} = 20 \text{ FIT}$

This results in a failure rate distribution, SFF and PFD<sub>AVG</sub> (assuming T[Proof] = 1 year) to:

$l_{sd}$	$l_{su}$	$l_{dd}$	$l_{du}$	<b>SFF</b>	<b>PFD<sub>AVG</sub></b>
0 FIT	142 FIT	2203 FIT	195 FIT	92,32 %	8,54E-04

The same can be calculated for a complete temperature sensor assembly consisting of the temperature transmitter PRetop 5335 and a closely coupled, cushioned 2/3-wire RTD supplied with PRetop 5335. Assuming that the PRetop 5335 is programmed to drive its output either high or low on a detected failure of the RTD (Fail low (L) = DD, Fail High (H) = DD), the failure rate contribution for the 2/3-wire RTD in a low stress environment is:

- $\lambda_{dd} = 1.000 \text{ FIT} + 600 \text{ FIT} = 1.600 \text{ FIT}$
- $\lambda_{du} = 400 \text{ FIT}$

This results in a failure rate distribution, SFF and  $\text{PFD}_{\text{AVG}}$  (assuming  $T[\text{Proof}] = 1 \text{ year}$ ) to:

$I_{sd}$	$I_{su}$	$I_{dd}$	$I_{du}$	SFF	$\text{PFD}_{\text{AVG}}$
0 FIT	142 FIT	1823 FIT	575 FIT	77,36 %	2,52E-03

The same can be calculated for a complete temperature sensor assembly consisting of the temperature transmitter PReTrans 6335 and an extension wired 2/3-wire RTD supplied with PReTrans 6335. Assuming that the PReTrans 6335 is programmed to drive its output either high or low on a detected failure of the RTD (Fail low (L) = DD, Fail High (H) = DD), the failure rate contribution for the 2/3-wire RTD in a low stress environment is:

- $\lambda_{dd} = 800 \text{ FIT} + 600 \text{ FIT} = 1.400 \text{ FIT}$
- $\lambda_{du} = 600 \text{ FIT}$

This results in a failure rate distribution, SFF and  $\text{PFD}_{\text{AVG}}$  (assuming  $T[\text{Proof}] = 1 \text{ year}$ ) to:

$I_{sd}$	$I_{su}$	$I_{dd}$	$I_{du}$	SFF	$\text{PFD}_{\text{AVG}}$
0 FIT	142 FIT	1623 FIT	675 FIT	72,33 %	2,96E-03

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

## 6 Terms and Definitions

CJC	Cold Junction Compensation
DC <sub>S</sub>	Diagnostic Coverage of safe failures ( $DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$ )
DC <sub>D</sub>	Diagnostic Coverage of dangerous failures ( $DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$ )
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD <sub>AVG</sub>	Average Probability of Failure on Demand
RTD	Resistance Temperature Detector
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
Type B component	“Complex” component (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.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. exida.com accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

### 7.2 Releases

Version: V1  
Revision: R1.4  
Version History: V0, R0: Initial version; March 16, 2005  
V1, R1.0 Internal review comments integrated + updated with additional information from PR electronics on different configurations; April 01 2005  
V1, R1.1 Final comments from review integrated, April 04 2005  
V1, R1.2 Added the identical PRetrans 6335 to the report, October 20, 2005  
V1, R1.3 Final comments from review integrated, October 20, 2005  
V1, R1.4 Correction of 2 document references, Added C and D version of 5335 and 6335, November 10, 2005  
Authors: Audun Opem  
Review: V0, R0: Stephan Aschenbrenner, Rachel Amkreutz (exida.com)  
V1, R1.0: Stephan Aschenbrenner (exida.com)  
V1, R1.2: Stephan Aschenbrenner (exida.com)  
V1, R1.3 Reviewed by PR electronics A/S  
V1, R1.4 Released to PR electronics A/S

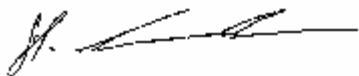
Release status: Released to PR electronics A/S

### 7.3 Release Signatures



---

Audun Opem, Senior Project Manager



---

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



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

Appendix 1 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 12 shows importance analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

**Table 12: Importance Analysis of “du” failures**

Component	% of total $l_{du}$	Detection through
IC9-B	22,83 %	100% functional test with different expected output signals over the entire range
IC4 B	22,83 %	100% functional test with different expected output signals over the entire range
IC1	7,31 %	100% functional test with different expected output signals over the entire range
IC12	6,42 %	100% functional test with different expected output signals over the entire range
Z3, Z4	4,28 %	100% functional test with different expected output signals over the entire range
IC11	3,42 %	100% functional test with different expected output signals over the entire range
C21, C23, C25, C82	2,28 %	100% functional test with different expected output signals over the entire range
IC18	2,28 %	100% functional test with different expected output signals over the entire range
C9, C16, C27	1,71 %	100% functional test with different expected output signals over the entire range
C2, C3, C60	1,71%	100% functional test with different expected output signals over the entire range

## Appendix 1.1: Critical failure modes contributing to I<sub>du</sub>

### Failures of complex integrated circuits

According to IEC 61508 the normal distribution of the failure rate of complex integrated circuits is 50% safe failures and 50% dangerous failures. In order to achieve a SFF of > 60%, diagnostics with at least low effectiveness are needed. The temperature transmitter PRe<sub>top</sub> 5335 / PRe<sub>trans</sub> 6335 achieves a SFF of about 68%.

## Appendix 1.2: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 13.

**Table 13 Steps for Proof Test 1**

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 test for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value.  This tests for possible quiescent current related failures
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 50% of possible “du” failures in the transmitter.

Proof test 2 consists of the following steps, as described in Table 14.

**Table 14 Steps for Proof Test 2**

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Perform a two-point calibration of the transmitter
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures in the transmitter.

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

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 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, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the  $PFD_{AVG}$  calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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 15 shows which electrolytic capacitors are contributing to the dangerous failure rate and therefore to the  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 15 Useful lifetime of electrolytic capacitors contributing to  $I_{du}$**

Type	Name	Schematic	Useful life at 40 °C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	C28	5335-1011 A sheet 1 of 2	Approx. 500 000 hours

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.

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.7.4 note 3 of IEC 61508 experiences have shown that the useful lifetime often lies within a range of 8 to 12 years for transmitters.