Failure Modes, Effects and Diagnostic Analysis

Project:

Universal Transmitter PReasy 4114 with current output
Universal Transmitter PReasy 4116 with current and relay output

Customer:

PR electronics A/S
Rønde
Denmark

Contract No.: PR electronics 05**/**14-14
Report No.: PRe 05/04-14 R003
Version V2, Revision R3, April 2009
Mats Gunnmarker

Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the Universal Transmitter PReasy 4114 / PReasy 4116. Table 1 gives an overview of the different types that belong to the considered transmitter. The Universal Transmitter PReasy 4114 / PReasy 4116 are DIN rail mounted.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). An 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

PReasy 4114	Universal transmitter, rail mounted – (Standard Version)
PReasy 4116	Universal transmitter, rail mounted – (Standard Version)

For safety applications only the 4..20 mA current output was considered for PReasy 4114. For PReasy 4116 both the 4..20 mA current output and the relay output has been considered for safety applications. All other possible output variants are not covered by this report. The Universal Transmitter PReasy 4114 / PReasy 4116 are programmed with the 4501 interface unit.

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 $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. For systems operating in high demand mode of operation the PFH value has to be $\geq 10^{-7}$ to $< 10^{-6}$ for SIL 2 safety functions according to table 3 of IEC 61508-1. A generally accepted distribution of PFD_{AVG} or PFH values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} or PFH value is caused by the sensor part.

For a SIL 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-03.

For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 1,00E-06 1/h, hence the maximum allowable PFH value for the sensor part would then be 3,50E-07 1/h.

The Universal Transmitter PReasy 4114 and PReasy 4116 are considered Type B[1] components with a hardware fault tolerance of 0.

For Type B components with a hardware fault tolerance of 0 the SFF shall be > 90% according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

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

PReasy 4114 / PReasy 4116 – Current outputs:

The following data applies for the Universal Transmitter PReasy 4114 and PReasy 4116 when using the current outputs in a safety function.

Table 2: Summary for PReasy 4114 / PReasy 4116 – Failure rates

Failure category		Failure rate (in FIT)
Fail Dangerous Detected		**628**
	Fail detected (internal diagnostics)	432
	Fail Low (detected by the logic solver)	193
	Fail High (detected by the logic solver)	3
Fail Dangerous Undetected		**82**
No Effect		**208**
Annunciation Undetected		**15**
Not part		**169**
MTBF = MTTF + MTTR		**104 years**

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), and that the logic solver is configured to not trip on these failures, the high and low failures can be classified as dangerous detected failures. For this application the following table shows the failure rates according to IEC 61508.

Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF
PReasy 4114 / PReasy 4116	0 FIT	223 FIT	628 FIT	82 FIT	91,20%

Table 3: Summary for PReasy 4114 / PReasy 4116 – PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 8,22E-08 1/h	**PFD_{AVG} = 3,60E-04**	**PFD_{AVG} = 1,80E-03**	**PFD_{AVG} = 3,60E-03**

A complete temperature sensor assembly consisting of PReasy 4114 / PReasy 4116 and a thermocouple or cushioned RTD supplied with PReasy 4114 / PReasy 4116 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 5.3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

Assuming that the Universal Transmitter PReasy 4114 / PReasy 4116 is programmed to drive its output high or low on detected failures of the thermocouple or RTD ($\lambda_{low} = \lambda_{dd}$, $\lambda_{high} = \lambda_{dd}$), the failure rate contribution or the PFD_{AVG} value for the thermocouple or RTD in a low stress environment is as follows:

[2] Note that the SU category includes failures that do not cause a spurious trip

Table 4: Summary for the sensor assembly PReasy 4114 / PReasy 4116 / thermocouple in low stress environment

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFH = 3,32E-07 1/h	PFD_{AVG} = 1,45E-03	PFD_{AVG} = 7,27E-03	PFD_{AVG} = 1,45E-02	94 %

λ_{sd} = 0 FIT

λ_{su} = 223 FIT

λ_{dd} = 5378 FIT

λ_{du} = 332 FIT

Table 5: Summary for the sensor assembly PReasy 4114 / PReasy 4116 / 4-wire RTD in low stress environment

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFH = 1,02E-07 1/h	PFD_{AVG} = 4,46E-04	PFD_{AVG} = 2,23E-03	PFD_{AVG} = 4,46E-03	96 %

λ_{sd} = 0 FIT

λ_{su} = 223 FIT

λ_{dd} = 2698 FIT

λ_{du} = 102 FIT

Table 6: Summary for the sensor assembly PReasy 4114 / PReasy 4116 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
PFH = 4,82E-07 1/h	PFD_{AVG} = 2,11E-03	PFD_{AVG} = 1,05E-02	PFD_{AVG} = 2,11E-02	84 %

λ_{sd} = 0 FIT

λ_{su} = 223 FIT

λ_{dd} = 2328 FIT

λ_{du} = 482 FIT

The boxes marked in yellow (▭) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03 respectively 3,50E-7 1/h. The boxes marked in green (▭) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 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-03 respectively 3,50E-7 1/h.

The failure rates are valid for the useful life of the Universal Transmitter PReasy 4114 / PReasy 4116, which is estimated to be about 10 years (see Appendix 2).

PReasy 4116 – Relay outputs:

The following data applies for the Universal Transmitter PReasy 4116 when using the relay outputs in a safety function.

Table 7: Summary for PReasy 4116 – Failure rates

Failure category		Failure rate (in FIT)
Fail Safe Detected		**0**
	Fail safe detected	0
Fail Safe Undetected		**478**
	Fail safe undetected	292
	Residual	186
Fail Dangerous Detected		**108**
	Fail detected (internal diagnostics)	68
	Annunciation detected	40
Fail Dangerous Undetected		**63**
	Fail dangerous undetected	62
	Annunciation undetected	1
Not part		**226**
MTBF = MTTF + MTTR		**130 years**

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

Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su} [3]	λ_{dd}	λ_{du}	SFF
PReasy 4116	0 FIT	478 FIT	108 FIT	63 FIT	90,28 %

Table 8: Summary for PReasy 4116 – PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 6,31E-08 1/h	**PFD_{AVG} = 2,76E-04**	**PFD_{AVG} = 1,38E-03**	**PFD_{AVG} = 2,76E-03**

A complete temperature sensor assembly consisting of PReasy 4116 and a thermocouple or cushioned RTD supplied with PReasy 4116 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 5.3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

[3] Note that the SU category includes failures that do not cause a spurious trip

Assuming that the Universal Transmitter PReasy 4116 is programmed to set the relay output in safe state on detected failures of the thermocouple or RTD, the failure rate contribution or the PFD_{AVG} value for the thermocouple or RTD in a low stress environment is as follows:

Table 9: Summary for the sensor assembly PReasy 4116 / thermocouple in low stress environment

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFH = 3,13E-07 1/h	PFD_{AVG} = 1,37E-03	PFD_{AVG} = 6,85E-03	PFD_{AVG} = 1,37E-02	94 %

λ_{sd} = 0 FIT

λ_{su} = 478 FIT

λ_{dd} = 4858 FIT

λ_{du} = 313 FIT

Table 10: Summary for the sensor assembly PReasy 4116 / 4-wire RTD in low stress environment

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFH = 8,31E-08 1/h	PFD_{AVG} = 3,64E-04	PFD_{AVG} = 1,82E-03	PFD_{AVG} = 3,64E-03	96 %

λ_{sd} = 0 FIT

λ_{su} = 478 FIT

λ_{dd} = 2178 FIT

λ_{du} = 83 FIT

Table 11: Summary for the sensor assembly PReasy 4116 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
PFH = 4,63E-07 1/h	PFD_{AVG} = 2,03E-03	PFD_{AVG} = 1,01E-02	PFD_{AVG} = 2,03E-02	83 %

λ_{sd} = 0 FIT

λ_{su} = 478 FIT

λ_{dd} = 1808 FIT

λ_{du} = 463 FIT

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03 respectively 3,50E-7 1/h. The boxes marked in green ( ) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 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-03 respectively 3,50E-7 1/h.

The maximum demand rate is 1.5 hours and is based on the internal fault detection and reaction time as stated in 4.3.

PReasy 4114 / PReasy 4116 – General information:

When the Safe Failure Fraction (SFF) is above 90% also the architectural constraints requirements of table 3 of IEC 61508-2 for Type B subsystems with a Hardware Fault Tolerance (HFT) of 0 are fulfilled.

The failure rates listed above do not include failures resulting from incorrect use of the Universal Transmitter PReasy 4114 / PReasy 4116, 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 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 user of the Universal Transmitter PReasy 4114 / PReasy 4116 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). Tables with failure rates are presented in section 5.1 and 5.2 along with all assumptions.

It is important to realize that the “no effect” failures and the “annunciation” 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.

The failure rates are valid for the useful life of the Universal Transmitter PReasy 4114 / PReasy 4116, which is estimated to be about 10 years (see Appendix 2).

Table of Contents

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 contains a FMEDA to determine the fault behavior and the different failure rates resulting in 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 contain any software assessment.

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 contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). The option contains in addition an assessment of the proven-in-use demonstration of the device and its software including the modification process.

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

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.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 Universal Transmitter PReasy 4114 / PReasy 4116. 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 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 Universal Transmitter PReasy 4114 / PReasy 4116 and performed the FMEDA according to option 1 (see section 1)
exida.com	Reviewed the FMEDA according to option 1 (see section 1).

PR electronics A/S contracted *exida.com* in October 2005 with the review of the FMEDA and PFD_{AVG} calculation for the above mentioned devices using their current outputs. *exida.com* was additionally contracted in March 2009 to review the FMEDA and PFD_{AVG} calculation for the PReasy 4116 device when using the relay outputs.

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]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components
[N7]	NSWC-98/LE1	Handbook of Reliability Prediction Procedures for Mechanical Equipment
[N8]	IEC 60654-1: 1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by PR electronics A/S

[D1]	4114Y101-UK (0530) PReasy 4114 “Universal Transmitter“	Data sheet
[D2]	4116Y101-UK (0530) PReasy 4116 “Universal Transmitter“	Data sheet
[D3]	4114V “4114 Universal Transmitter“	Users Manual
[D4]	4116V “4116 Universal Transmitter“	Users Manual
[D5]	4116-1-04.SH1 to SH4 of 18.07.2005	Circuit diagram “4116”
[D6]	4114 input modes failures.xls	Behavior differences for current, voltage, potentiometer, TC and PT100
[D7]	4116SMD version 2014, dated 16/12-05	Parts List, 4114 / 4116 (SMD level)
[D8]	4114L version 2018, dated 23/11-05	Parts List, 4114 (leaded level)
[D9]	4116L version 2018, dated 23/11-05	Parts List, 4116 (leaded level)
[D10]	4116 FMEDA relay V1R0.xls	FMEDA

2.4.2 Documentation generated by *exida.com*

[R1]	4116-rev5 V6 R0.5.xls (FMEDA)

3 Description of the analyzed module

The Universal Transmitter PReasy 4114 and PReasy 4116 are isolated universal input devices used in many different industries for both control and safety applications. Combined with e.g. a temperature sensing device, the Universal Transmitter PReasy 4114 / PReasy 4116 becomes a temperature sensor assembly.

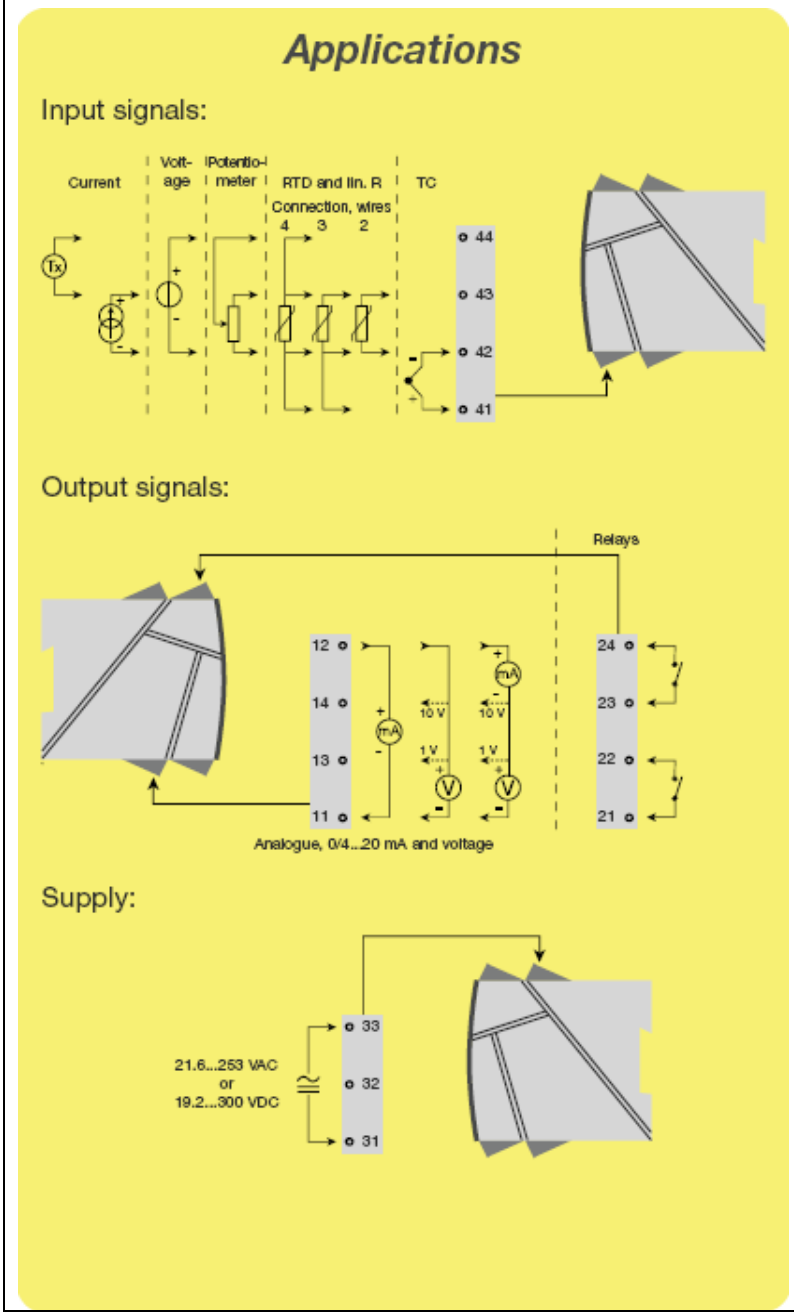
Figure 1 PReasy 4114 / PReasy 4116 Universal Transmitter

The Universal Transmitter PReasy 4114 / PReasy 4116 are configured with the interface unit 4501 which is plugged into the front of the universal transmitter.

The Universal Transmitter PReasy 4114 / PReasy 4116 are considered Type B components with a hardware fault tolerance of 0.

The universal transmitters operate with a 2-wire current output and with separate wires for the supply voltage. The universal transmitter PReasy 4116 has also a relay output. The supply voltage can be from 19.2V to 300V DC or from 21.6V to 253V AC.

This is also indicated in the following figure.



The sensing devices that can be connected to the Universal Transmitter PReasy 4114 / PReasy 4116 are:

- 2-, 3- and 4-wire RTD
- Thermocouple
- 2-, 3- and 4-wire resistance
- Voltage input
- Potentiometer
- Current

The following output signals are possible with the Universal Transmitter PReasy 4114

- Current 4..20mA
- Current 20..4mA

The following output signal are possible with the Universal Transmitter PReasy 4116

- Current 4..20mA
- Current 20..4mA
- Relay

The Universal Transmitter PReasy 4114 / PReasy 4116 are suitable for DIN rail mounting.

Figure 2: Input configurations with Universal Transmitter PReasy 4114 / PReasy 4116

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 by PR electronics A/S and reviewed by *exida.com*. The results are documented in [R1] and [D10]. 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 was then indicated in the FMEDA effects with a (TEST).

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 Universal Transmitter PReasy 4114 / PReasy 4116, the following definitions for the failure of the product were considered.

General

Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.
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 No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function. 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.

PReasy 4114 / PReasy 4116 – Current output

Fail-Safe State	The fail-safe state is defined as the output exceeding the user defined threshold.
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 deviate the output current by more than 2% full span.
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)

PReasy 4116 – Relay output

Fail-Safe State	The fail-safe state is defined as the output being de-energized.
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).

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 are considered to be appropriate for safety integrity level verification calculations. The rates match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Universal Transmitter PReasy 4114 / PReasy 4116:

- 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 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 internal fault detection time is 38 seconds.
- 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 40ºC. Humidity levels are assumed within manufacturer's rating.
- Both modules are suitable for high demand mode of operation with a maximum demand rate of 1.5 hours.
- The safety function is carried out via 1 input and 1 output channel.
- Only the described output versions are used for safety applications.
- The related current output is used and programmed to provide 4..20 mA or 20..4 mA.
- When using the relay output on PReasy 4116, the related current output shall be connected to a compatible safety PLC input or be short circuit with a wire.
- External power supply failure rates are not included.
- The application program in the safety logic solver is configured to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- No inductive load.
- The relay output is protected by a fuse which initiates at 2A to avoid contact welding (this is based on the assumption that 2A is less than 60% of the rated current for the relay).
- The maximum allowed switching frequency for the relay output is 3 Hz. The user must calculate the product lifetime with respect to the relay lifetime. The relay lifetime is 100 000 times.

5 Results of the assessment

exida.com reviewed the FMEDAs performed by PR electronics A/S.

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:

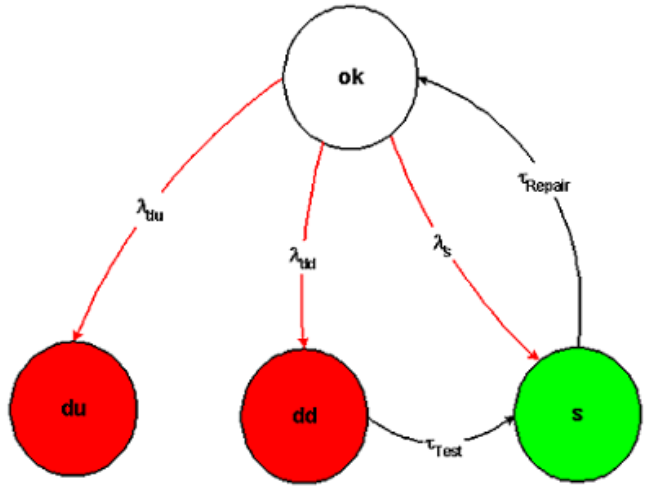
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$.

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

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.



Abbreviations:

du	The system has failed dangerous undetected
dd	The system has failed dangerous detected
s	The system has failed safe
λ_{du}	Failure rate of dangerous undetected failures
λ_{dd}	Failure rate of dangerous detected failures
λ_{s}	Failure rate of safe failures
T_{Test}	Test time
τ_{Test}	Test rate ($1 / T_{Test}$)
T_{Repair}	Repair time
τ_{Repair}	Repair rate ($1 / T_{Repair}$)

Figure 3: Markov model for a 1oo1D structure

5.1 Universal Transmitter PReasy 4114 / PReasy 4116 – Current outputs

The FMEDA carried out on the Universal Transmitter PReasy 4114 / PReasy 4116 when using the current outputs, leads under the assumptions described in section 4.3 to the following failure rates:

λ_{su} = 1,65E-07

λ_{dd} = 2,67E-07

λ_{du} = 8,22E-08

λ_{high} = 2,94E-09

λ_{low} = 1,93E-07

$\lambda_{annunciation}$ = 1,51E-08 1/h

$\lambda_{no\ effect}$ = 2,08E-07

λ_{total} = 9,33E-07

$\lambda_{not\ part}$ = 1,69E-07 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 104 years

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

Failure category		**Failure rate (in FITs)**
Fail Dangerous Detected		**628**
	Fail detected (internal diagnostics)	432
	Fail Low (detected by the logic solver)	193
	Fail High (detected by the logic solver)	3
Fail Dangerous Undetected		**82**
No Effect		**208**
Annunciation Undetected		**15**
No part		**169**
MTBF = MTTF + MTTR		**104 years**

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

Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF
PReasy 4114 / PReasy 4116	0 FIT	223 FIT	628 FIT	82 FIT	91,20 %

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
PFH = 8,22E-08 1/h	PFD_{AVG} = 3,60E-04	PFD_{AVG} = 1,80E-03	PFD_{AVG} = 3,60E-03

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03 respectively 3,50E-7 1/h. The boxes marked in green ( ) mean that the calculated PFD_{AVG} and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 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-03 respectively 3,50E-7 1/h. Figure 4 shows the time dependent curve of PFD_{AVG}.

The maximum demand rate is 1.5 hours and is based on the internal fault detection and reaction time as stated in 4.3.

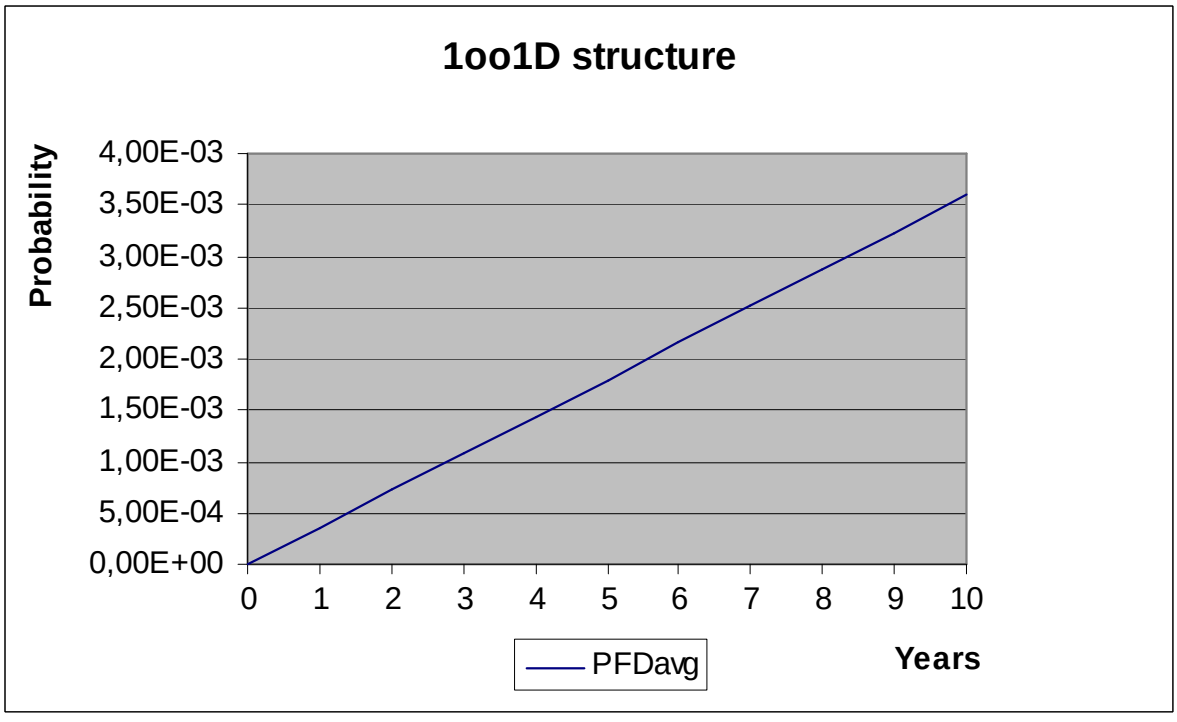


Figure 4: $PFD_{AVG}(t)$

[4] Note that the SU category includes failures that do not cause a spurious trip

5.2 Universal Transmitter PReasy 4116 – Relay outputs

The FMEDA carried out on the Universal Transmitter PReasy 4116 when using the relay outputs, leads under the assumptions described in section 4.3 to the following failure rates:

λ_{su} = 2,92E-07

λ_{dd} = 6,86E-08

λ_{du} = 6,23E-08

$\lambda_{annunciation\ detected}$ = 3,96E-08 1/h

$\lambda_{annunciation\ undetected}$ = 8,11E-10 1/h

$\lambda_{no\ effect}$ = 1,86E-07

λ_{total} = 6,49E-07

$\lambda_{not\ part}$ = 2,26E-07 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 130 years

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

Failure category		**Failure rate (in FIT)**
Fail Safe Detected		**0**
	Fail safe detected	0
Fail Safe Undetected		**478**
	Fail safe undetected	292
	Residual	186
Fail Dangerous Detected		**108**
	Fail detected (internal diagnostics)	68
	Annunciation detected	40
Fail Dangerous Undetected		**63**
	Fail dangerous undetected	62
	Annunciation undetected	1
No part		**226**
MTBF = MTTF + MTTR		**130 years**

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

Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su} [5]	λ_{dd}	λ_{du}	SFF
PReasy 4116	0 FIT	478 FIT	108 FIT	63 FIT	90,28 %

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
PFH = 6,31E-08 1/h	PFD_{AVG} = 2,76E-04	PFD_{AVG} = 1,38E-03	PFD_{AVG} = 2,76E-03

The green (▭) mark mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 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-03 respectively 3,50E-7 1/h. Figure 4 shows the time dependent curve of PFD_{AVG}.

The maximum demand rate is 1.5 hours and is based on the internal fault detection and reaction time as stated in 4.3.

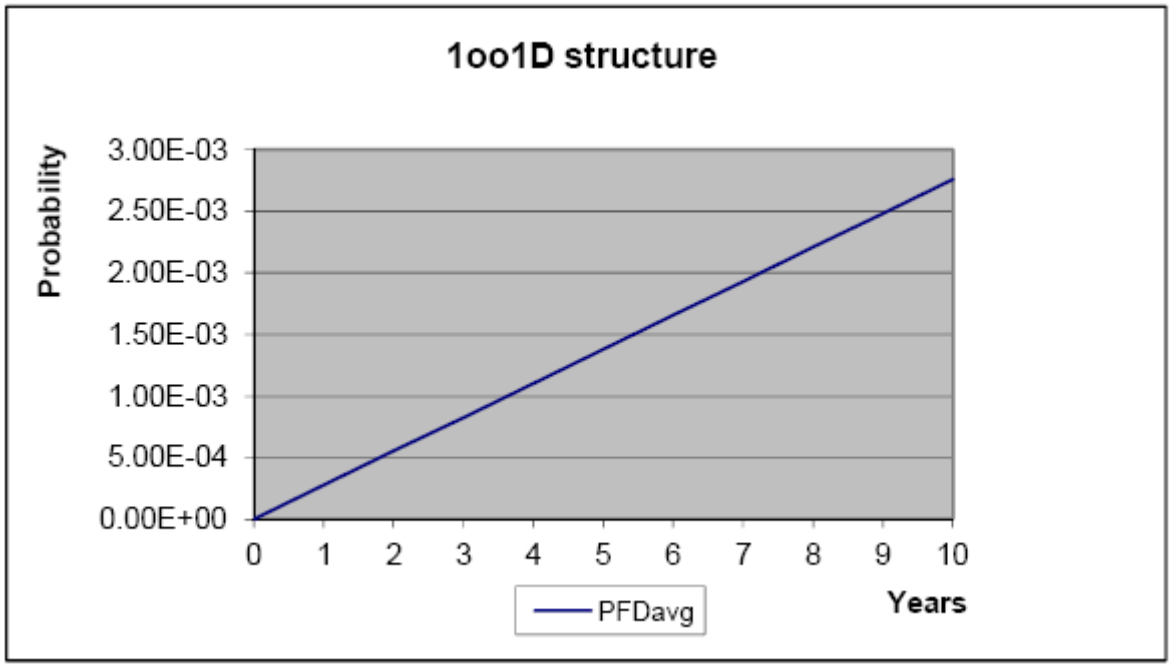


Figure 5: $PFD_{AVG}(t)$

[5] Note that the SU category includes failures that do not cause a spurious trip

5.3 Using the FMEDA results

The Universal Transmitter PReasy 4114 / PReasy 4116 together with e.g. a temperature sensing device become 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 12 Typical failure rates for thermocouples

Temperature sensing device	***Failure rate (in FIT)***
Thermocouple low stress environment	5.000
Thermocouple high stress environment	20.000

5.3.1 PReasy 4114 / PReasy 4116 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 13 when thermocouples are supplied with the Universal Transmitter PReasy 4114 / PReasy 4116. The drift failure mode is primarily due to T/C aging. The Universal Transmitter PReasy 4114 / PReasy 4116 will detect a thermocouple burn-out failure and drive its output to the specified failure state.

Table 13 Typical failure mode distributions for thermocouples

Thermocouple Failure Mode Distribution	***Percentage***
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 Universal Transmitter PReasy 4114 / PReasy 4116 and a thermocouple supplied with PReasy 4114 / PReasy 4116 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.

5.3.1.1 PReasy 4114 / PReasy 4116 – Thermocouple and Current output

Assuming a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4114 / PReasy 4116 and a thermocouple supplied with PReasy 4114 / PReasy 4116. Also assuming that the Universal Transmitter PReasy 4114 / PReasy 4116 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:

- λ_{dd} = (5.000 FIT) * (0,95) = 4.750 FIT
- λ_{du} = (5.000 FIT) * (0,05) = 250 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF	PFD_{AVG}
0 FIT	223 FIT	5378 FIT	332 FIT	94,40 %	1,45 E-03

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

5.3.1.2 PReasy 4116 – Thermocouple and Relay output

Assuming a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4116 and a thermocouple supplied with PReasy 4116. Also assuming that the Universal Transmitter PReasy 4116 is programmed to set the relay output in safe state on detected (open circuit) failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

- λ_{dd} = (5.000 FIT) * (0,95) = 4.750 FIT
- λ_{du} = (5.000 FIT) * (0,05) = 250 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF	PFD_{AVG}
0 FIT	478 FIT	4858 FIT	313 FIT	94,46 %	1,37 E-03

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

5.3.2 PReasy 4114 / PReasy 4116 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 14 and Table 15.

Table 14 Typical failure rate for 4-Wire RTDs in a Low Stress environment

RTD Failure Mode Distribution	***Extension wired***
Open Circuit	1490 FIT
Short Circuit	590 FIT
Drift (Temperature Measurement in error)	20 FIT

Table 15 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

RTD Failure Mode Distribution	***Extension wired***
Open Circuit	1090 FIT
Short Circuit	610 FIT
Drift (Temperature Measurement in error)	400 FIT

A complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4114 / PReasy 4116 and an extension wired 4-wire RTD supplied with PReasy 4114 / PReasy 4116 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.

5.3.2.1 PReasy 4114 / PReasy 4116 – RTD and Current output

Assuming a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4114 / PReasy 4116 and an extension wired 4-wire RTD supplied with PReasy 4114 / PReasy 4116. Also assuming that the Universal Transmitter PReasy 4114 / PReasy 4116 are programmed to drive its output either high or low on a detected (open or short circuit) 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:

- λ_{dd} = 1490 FIT + 580 FIT = 2070 FIT
- λ_{du} = 20 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	**SFF**	**PFD_{AVG}**
0 FIT	223 FIT	2698 FIT	102 FIT	96,63 %	4,46 E-04

The same can be calculated for a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4114 / PReasy 4116 and an extension wired 2/3-wire RTD supplied with PReasy 4114 / PReasy 4116. Assuming that the Universal Transmitter PReasy 4114 / PReasy 4116 are programmed to drive its output either high or low on a detected (open or short circuit) 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:

- λ_{dd} = 1090 FIT + 610 FIT = 1.700 FIT
- λ_{du} = 400 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	**SFF**	**PFD_{AVG}**
0 FIT	223 FIT	2328 FIT	482 FIT	84,11 %	2,11 E-03

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

5.3.2.2 PReasy 4116 – RTD and Relay output

Assuming a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4116 and an extension wired 4-wire RTD supplied with PReasy 4116. Also assuming that the Universal Transmitter PReasy 4116 is programmed to set the relay output in safe state on detected (open or short circuit) failures of the RTD, the failure rate contribution for the 4-wire RTD in a low stress environment is:

- λ_{dd} = 1490 FIT+ 580 FIT = 2070 FIT
- λ_{du} = 20 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	**SFF**	**PFD_{AVG}**
0 FIT	478 FIT	2178 FIT	83 FIT	96,97 %	3,64 E-04

The same can be calculated for a complete temperature sensor assembly consisting of the Universal Transmitter PReasy 4116 and an extension wired 2/3-wire RTD supplied with PReasy 4116. Assuming that the Universal Transmitter PReasy 4116 is programmed to set the relay output in safe state on detected (open or short circuit) failures of the RTD, the failure rate contribution for the 2/3-wire RTD in a low stress environment is:

- λ_{dd} = 1090 FIT+ 610 FIT = 1.700 FIT
- λ_{du} = 400 FIT

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

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	**SFF**	**PFD_{AVG}**
0 FIT	478 FIT	1808 FIT	463 FIT	83,16 %	2,03 E-03

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

6 Terms and Definitions

DC_S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
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 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 one per year or 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 one per year and 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.
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 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:	V0, R1.0:	Initial version; January 03, 2006
	V1, R1.0:	Updated after review; January 09, 2006
	V1, R1.1:	Minor updates after review; January 10, 2006
	V1, R1.2:	Updates after review by PR electronics A/S and Stephan Aschenbrenner, January 23, 2006
	V1, R1.3:	Failure rate distribution for sensor assembly corrected, January 19, 2007
	V2, R0:	Added FMEDA analysis result for using the PReasy 4116 relay outputs in a safety function, March 20, 2009.
	V2, R1:	Updated after internal exida review, March 25, 2009.
	V2, R2:	Updates after review by PR electronics A/S, March 26, 2009.
	V2, R3:	Editorial changes, April 1, 2009.
Authors:	Mats Gunnmarker	
Review:	V0, R1.0:	Rachel Amkreutz (exida); January 6, 2006
Review:	V1, R1.0:	Stephan Aschenbrenner (exida); January 9, 2006
Review:	V1, R1.1:	PR electronics A/S January 17, 2006
		Stephan Aschenbrenner (exida); January 19, 2006
	V2, R0:	Stephan Aschenbrenner (exida); March 23, 2009
	V2, R1:	PR electronics A/S March 25, 2009
Release status:	Released to PR	

7.3 Release Signatures

Mats Gunnmarker, Partner

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 16 shows, for the **current output** usage, the importance analysis of the ten most critical components and their contribution to dangerous undetected faults, and indicates how these faults can be detected during proof testing.

Table 16: Importance Analysis of "du" failures when using the current outputs

Component	% of total λ_{du}	Detection through
IC104	44,13 %	100% functional test with different expected output signals over the entire range
Z103	8,09 %	100% functional test with different expected output signals over the entire range
IC102	7,73 %	100% functional test with different expected output signals over the entire range
C121, C132, C153, C155	4,87 %	100% functional test with different expected output signals over the entire range
T101	3,04 %	100% functional test with different expected output signals over the entire range
T105	3,04 %	100% functional test with different expected output signals over the entire range
Z5	2,56 %	100% functional test with different expected output signals over the entire range
IC105	2,56 %	100% functional test with different expected output signals over the entire range
T102	2,01 %	100% functional test with different expected output signals over the entire range
T103	2,01%	100% functional test with different expected output signals over the entire range

Table 17 shows, for the **relay output** usage, the importance analysis of the ten most critical components and their contribution to dangerous undetected faults, and indicates how these faults can be detected during proof testing.

Table 17: Importance Analysis of "du" failures when using the relay outputs

Component	% of total λ_{du}	Detection through
RE1	32,12 %	100% functional test with different expected output signals over the entire range
Z103	9,56 %	100% functional test with different expected output signals over the entire range
IC102	7,84 %	100% functional test with different expected output signals over the entire range
C121, C132, C153, C155	6,42 %	100% functional test with different expected output signals over the entire range
T101	4,02 %	100% functional test with different expected output signals over the entire range
T105	4,02 %	100% functional test with different expected output signals over the entire range
IC105	3,85 %	100% functional test with different expected output signals over the entire range
IC104-RAM	3,05 %	100% functional test with different expected output signals over the entire range
T102	2,65 %	100% functional test with different expected output signals over the entire range
T103	2,65%	100% functional test with different expected output signals over the entire range

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 18.

Table 18 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	(**Current output** usage) Use the 4501 to command the transmitter (with EN:SIM) to go to the high alarm current output and verify that the analog current reaches that value, or, (**Relay output** usage) use the 4501 to command the transmitter (with EN:SIM) to go to the high alarm current output and verify that the relay is de-energized 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	(**Current output** usage) Use the 4501 to command to the transmitter (with EN.SIM) to go to the low alarm current output and verify that the analog current reaches that value, or, (**Relay output** usage) use the 4501 to command the transmitter (with EN:SIM) to go to the low alarm current output and verify that the relay is de-energized 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 and approximately 90% of the simple sensing element DU failures.

Proof test 2 consists of the following steps, as described in Table 19.

Table 19 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 and approximately 99% of the simple sensing element DU failures.

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 4.3) 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 20 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 20 Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Name	Schematic	Useful life at 40 ºC
Capacitor (electrolytic) - Aluminum electrolytic, non solid electrolyte	C8	4116-1-04-SH2	Approx. 90 000 hours[6]
Relay	RE1	4116-1-05-SH3	Approx 100 000 times

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. The limiting factors with regard to the useful lifetime of the system are the aluminum electrolytic capacitor and the output relay (depending on the switching frequency). The aluminum electrolytic capacitors have an estimated useful lifetime of about 10 years. The relays have an estimated lifetime of 100000 times, and the user must therefore calculate a device lifetime with respect to the relay lifetime.

[6] The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperature follows “The Doubling 10ºC Rule” where life is doubled for each 10ºC reduction in the operating temperature.