Failure Modes, Effects and Diagnostic Analysis

Project:
9116 Universal converter

Customer:

PR electronics A/S
Rønde
Denmark

Contract No.: PR electronics 06/03-19

Report No.: PR electronics 06/03-19 R024

Version V2, Revision R1; August 2015

Stephan Aschenbrenner, Piotr Serwa

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights on the format of this technical report reserved.

Management summary

This report summarizes the results of the hardware assessment carried out on the 9116 Universal converter. The 9116 Universal converter consists of the versions 9116B1 / 9116B2 (Ex) and 9116A1 / 9116A2 (Standard). Table 1 shows the input/output configurations of the 9116 Universal converter that have been assessed.

Table 1: Overview of assessed configurations of the 9116 Universal converter

	FMEDA name	HW/SW version	Configuration description
[C1]	3w Pt100 Aout	9116-1-V3R0	Resistance / RTD temperature / TC temperature inputs, Current Output
[C2]	3w Pt100 Relay	9116-1-V3R0	Resistance / RTD temperature / TC temperature inputs, Relay Output
[C3]	Current Aout	9116-1-V2R0	Current Input, Current Output
[C4]	Current Relay	9116-1-V2R0	Current input, Relay output
[C5]	Voltage Aout	9116-1-V2R0	Voltage input, Current Output
[C6]	Voltage Relay	9116-1-V2R0	Voltage input, Relay output

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

For safety applications only the described input/output configurations are considered. All other possible input/output configurations are not covered by this report.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1 [1]. The analysis was carried out with the basic failure rates from the Siemens standard SN 29500. However, as the comparison between these two databases has shown that the differences are within an acceptable tolerance the failure rates of the *exida* database are listed.

The 9116 Universal converter is considered a Type B[2] subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF has to be ≥ 90% for SIL 2 subsystems according to table 2 of IEC 61508-2.

It is important to realize that the “no effect” failures and the “annunciation” failures are included in the “safe” failure category according to IEC 61508:2000. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

It is assumed that the connected safety logic solver is configured per the NAMUR NE43 signal ranges, i.e. the 9116 Universal converter with 4..20 mA current output communicates detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures are classified as dangerous detected failures.

The following tables show how the above stated requirements are fulfilled.

---

[1] For details, see Appendix 3.

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

Table 2: Summary for [C1] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**278**
Fail safe undetected	0
No effect	278
Fail Dangerous Detected (λ_{DD})	**352**
Fail detected (detected by internal diagnostics)	226
Fail low (detected by safety logic solver)	96
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**43** [3]
Fail dangerous undetected	42
Annunciation undetected	1
No part	**877**

Total failure rate (safety function)	**673 FIT**
SFF [4]	**93%**
DC_D	**89%**
MTBF	**74 Years**

SIL AC [5]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[3] This value corresponds to a PFH of 4.30E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[4] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table 3: Summary for [C2] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**359**
Fail safe undetected	107
No effect	252
Fail Dangerous Detected (λ_{DD})	**230**
Fail detected (detected by internal diagnostics)	209
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**62** [6]
Fail dangerous undetected	61
Annunciation undetected	1
No part	**899**

Total failure rate (safety function)	**651 FIT**
SFF [7]	**90%**
DC_D	**79%**
MTBF	**74 Years**

SIL AC [8]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[6] This value corresponds to a PFH of 6.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[7] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table 4: Summary for [C3] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**444**
Fail safe undetected	0
No effect	444
Fail Dangerous Detected (λ_{DD})	**554**
Fail detected (detected by internal diagnostics)	317
Fail low (detected by safety logic solver)	207
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**42** [9]
Fail dangerous undetected	41
Annunciation undetected	1
No part	**510**

Total failure rate (safety function)	**1040 FIT**
SFF [10]	**95%**
DC_D	**93%**
MTBF	**74 Years**

SIL AC [11]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[9] This value corresponds to a PFH of 4.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[10] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table 5: Summary for [C4] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**1**
Fail safe detected	1
Fail Safe Undetected (λ_{SU})	**636**
Fail safe undetected	218
No effect	418
Fail Dangerous Detected (λ_{DD})	**320**
Fail detected (detected by internal diagnostics)	299
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**62** [12]
Fail dangerous undetected	61
Annunciation undetected	1
No part	**533**

Total failure rate (safety function)	**1019 FIT**
SFF [13]	**93%**
DC_D	**83%**
MTBF	**74 Years**

SIL AC [14]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[12] This value corresponds to a PFH of 6.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[13] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table 6: Summary for [C5] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**395**
Fail safe undetected	0
No effect	395
Fail Dangerous Detected (λ_{DD})	**479**
Fail detected (detected by internal diagnostics)	350
Fail low (detected by safety logic solver)	99
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**56** [15]
Fail dangerous undetected	55
Annunciation undetected	1
No part	**620**

Total failure rate (safety function)	**930 FIT**
SFF [16]	**93%**
DC_D	**89%**
MTBF	**74 Years**

SIL AC [17]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[15] This value corresponds to a PFH of 5.60E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[16] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table 7: Summary for [C6] - IEC 61508 failure rates

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**1**
Fail safe detected	1
Fail Safe Undetected (λ_{SU})	**480**
Fail safe undetected	111
No effect	369
Fail Dangerous Detected (λ_{DD})	**353**
Fail detected (detected by internal diagnostics)	332
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**76** [18]
Fail dangerous undetected	75
Annunciation undetected	1
No part	**642**

Total failure rate (safety function)	**910 FIT**
SFF [19]	**91%**
DC_D	**82%**
MTBF	**74 Years**

SIL AC [20]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[18] This value corresponds to a PFH of 7.60E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[19] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 3.

This document describes the results of the FMEDA carried out on the 9116 Universal converter (9116B2). Table 1 shows the input/output configurations of the 9116 Universal converter that have been assessed. The FMEDA is part of a full functional safety assessment according to IEC 61508.

The information in this report can be used to evaluate whether a sensor subsystem, including the 9116 Universal converter meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a partnership company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles and parties

PR electronics A/S	Manufacturer of the 9116 Universal converter.
exida	Performed the hardware assessment and reviewed the FMEDA provided by the customer.

PR electronics A/S contracted *exida* with the review of the FMEDA of the devices mentioned above.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	9116 CPU failure distribution estimation.xls of 2009.12.21	Failure distribution for used CPUs
[D2]	9116 Circuit Description V2R0.doc of 11.02.10	Circuit description
[D3]	9116-1-02-PDF.pdf of 2009.12.16	Circuit schematics and layout diagrams (9116-1-2)
[D4]	9116-1-03-PDF.pdf of 2010.01.26	Circuit schematics and layout diagrams (9116-1-3)
[D5]	9116V100_DK.pdf of 2007.05.09	Users' manual (in Danish)
[D6]	9116 Derating Analysis V0R8.xls of 23.03.10	Derating analysis

[D7]	9116 FMEDA 3W Pt100 Relay V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Pt100 Aout
[D8]	9116 FMEDA 3w Pt100 Aout V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Pt100 Relay
[D9]	9116 FMEDA Current Aout V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Current Aout
[D10]	9116 FMEDA Current Relay V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Current Relay
[D11]	9116 FMEDA Voltage Aout V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Voltage Aout
[D12]	9116 FMEDA Voltage Relay V0R8.xls of 23.03.10	FMEDA results file generated by customer for 3w Voltage Relay
[D13]	9116V001.pdf of 2010.03.17	Users' manual (multilingual), from PRelectronics website.
[D14]	9116 Hardware Fault Insertion Test Report V2R0.doc of11.02.10	Hardware Fault Insertion Test Report
[D15]	9116 Safety Manual V0R9.pdf	Safety Manual
[D16]	New A variant to the 9000 series of transmitters with grey terminals.msg of 15.05.14	Description of changes between Ex and standard versions.

2.4.2 Documentation generated by *exida*

[R1]	9116 FMEDA 3w Pt100 Aout - Review SA.xls	Review of FMEDA by Stephan Aschenbrenner
[R2]	9116 FMEDA 3W Pt100 Relay - Review SA.xls	Review of FMEDA by Stephan Aschenbrenner
[R3]	Review and Feedback 05.02.10.txt	Review comments by Stephan Aschenbrenner

3 Description of the analyzed subsystem

The 9116 Universal converter converts various sensor input signals to either (1) a 4..20 mA current output, or to (2) a relay output.

The hardware for the 9116 Universal converter is divided into 4 major modules. Each of these modules is then divided in sub modules. In this document, all component functions of each sub module will be described. The general description of the modules is as follows:

- MAIN SUPPLY: Power supply circuit with external supply connection or from Power Rail. Additionally, this block contains the Status signal latching relay and the Power Rail status output.
- MAIN CPU: Contains the Main CPU circuit with front LEDS and interface to 4501 and Output.
- INPUT: Measurement circuits with ADC and a P to transfer measured values to Output. The input is isolated from the other modules with Ex-quality.
- OUPUT: Contains the Output P which handles all the main calculations, output current, output relay setting and the Ex isolation and power supply for Input.

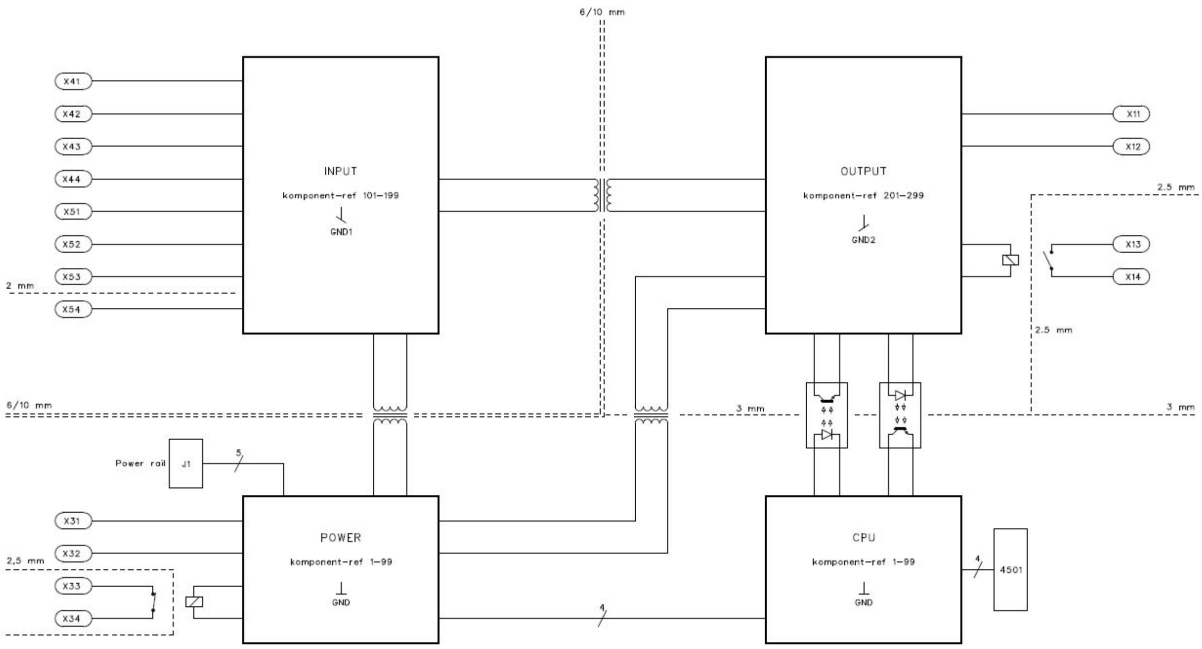

Figure 1: 9116 Universal converter circuit diagram

As shown by Figure 2, the 9116 Universal converter has the following inputs: Input for RTD, TC, Ohm, potentiometer, mA and V. it has the following outputs: active mA output, passive mA output and relay output.

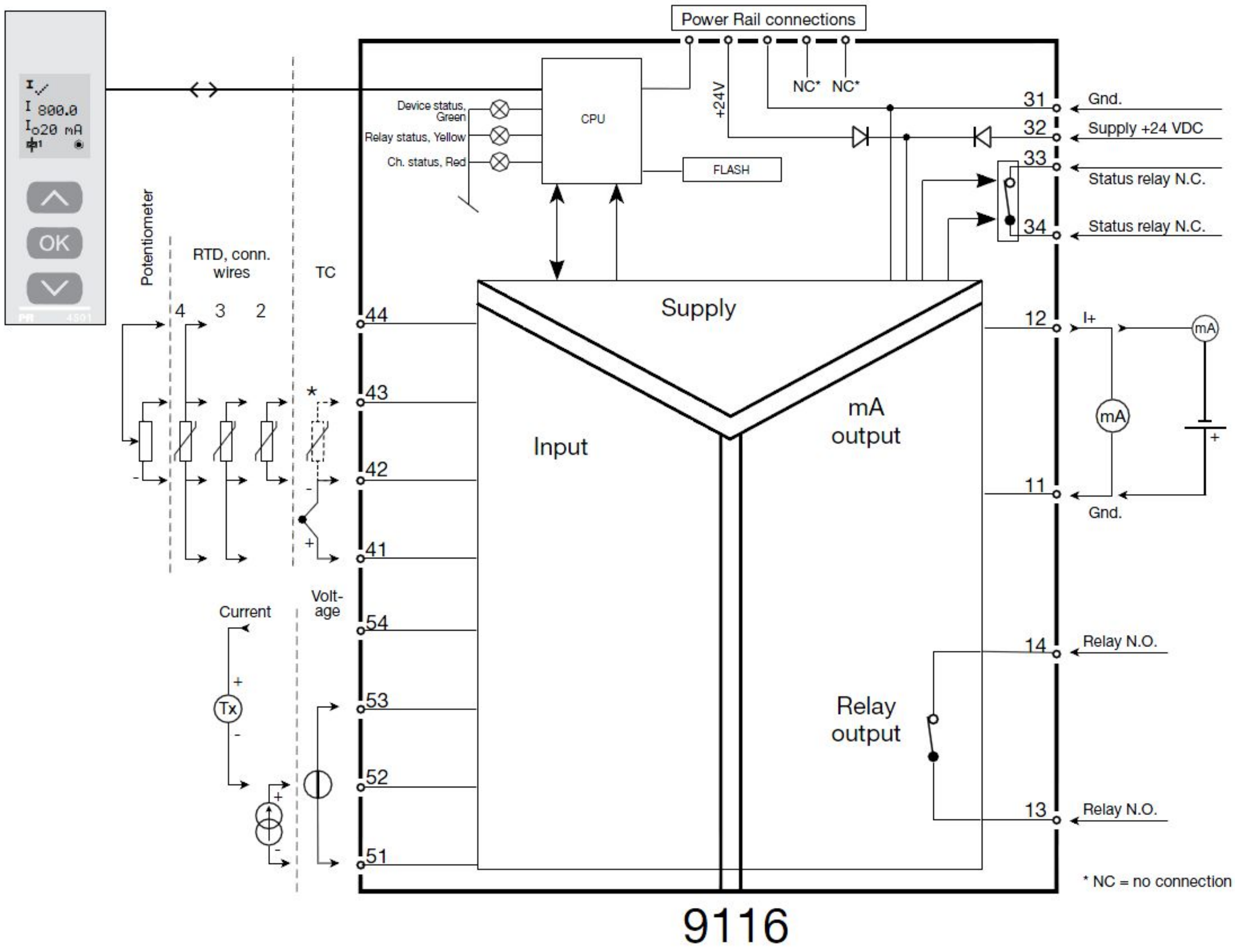

Figure 2: 9116 Universal converter block diagram

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was prepared by PR electronics A/S and reviewed by *exida*. The resulting FMEDAs are documented in [D7] to [D12]. When the effect of a certain component failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see fault insertion test report [D14]). 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 9116 Universal converter, the following definitions for the failure of the product were considered.

Fail-Safe State	For 3w Pt100 Aout, Current Aout, Voltage Aout, the fail-safe state is defined as the output reaching the user defined threshold value. For 3w Pt100 Relay, Current Relay, Voltage Relay, the fail-safe state is defined as the output being de-energized.
Fail Safe	Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.
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 and causes the output signal to go to the predefined alarm state.
Fail High	A fail high failure (H) is defined as a failure that causes the output signal to go to the over-range or high alarm output current (> 21mA).
Fail Low	A fail low failure (L) is defined as a failure that causes the output signal to go to the under-range or low alarm output current (< 3.6mA).
No Effect	A no effect failure (#) is defined as a 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	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. For the calculation of the SFF they are treated as “Dangerous Undetected” failures.

No Part — Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The failure categories listed above expand on the categories listed in IEC 61508, which are only safe and dangerous, both detected and undetected. The reason for this is that not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508:2000.

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 61508:2000 the "No Effect" 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 under consideration.

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

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1. 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 *exida* Profile 1. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its "useful life".

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 9116 Universal converter.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to the safe state is identical to MTTR.
- Only the described versions are used for safety applications.
- Only one input and one output are part of the considered safety function.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- Materials are compatible with process conditions.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Short circuit and lead breakage detection are activated.
- The worst-case internal fault detection time is 30 seconds.

4.3 Results

For the calculation of the Safe Failure Fraction (SFF) and λ_{total} the following has to be noted:

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

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

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

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

4.3.1 9116 Universal converter, configuration 3w Pt100 Aout

The FMEDA carried out on the 9116 Universal converter, configuration 3w Pt100 Aout ([C1]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**278**
Fail safe undetected	0
No effect	278
Fail Dangerous Detected (λ_{DD})	**352**
Fail detected (detected by internal diagnostics)	226
Fail low (detected by safety logic solver)	96
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**43** [21]
Fail dangerous undetected	42
Annunciation undetected	1
No part	**877**

Total failure rate (safety function)	**673 FIT**
SFF [22]	**93%**
DC_D	**89%**
MTBF	**74 Years**

SIL AC [23]	**SIL 2**

[21] This value corresponds to a PFH of 4.30E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[22] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

4.3.2 9116 Universal converter, configuration 3w Pt100 Relay

The FMEDA carried out on the 9116 Universal converter, configuration 3w Pt100 Relay ([C2]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**359**
Fail safe undetected	107
No effect	252
Fail Dangerous Detected (λ_{DD})	**230**
Fail detected (detected by internal diagnostics)	209
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**62** [24]
Fail dangerous undetected	61
Annunciation undetected	1
No part	**899**

Total failure rate (safety function)	**651 FIT**
SFF [25]	**90%**
DC_D	**79%**
MTBF	**74 Years**

SIL AC [26]	**SIL 2**

[24] This value corresponds to a PFH of 6.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[25] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

4.3.3 9116 Universal converter, configuration Current Aout

The FMEDA carried out on the 9116 Universal converter, configuration Current Aout ([C3]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**444**
Fail safe undetected	0
No effect	444
Fail Dangerous Detected (λ_{DD})	**554**
Fail detected (detected by internal diagnostics)	317
Fail low (detected by safety logic solver)	207
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**42** [27]
Fail dangerous undetected	41
Annunciation undetected	1
No part	**510**

Total failure rate (safety function)	**1040 FIT**
SFF [28]	**95%**
DC_D	**93%**
MTBF	**74 Years**

SIL AC [29]	**SIL 2**

[27] This value corresponds to a PFH of 4.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[28] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

4.3.4 9116 Universal converter, configuration Current Relay

The FMEDA carried out on the 9116 Universal converter, configuration Current Relay ([C4]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**1**
Fail safe detected	1
Fail Safe Undetected (λ_{SU})	**636**
Fail safe undetected	218
No effect	418
Fail Dangerous Detected (λ_{DD})	**320**
Fail detected (detected by internal diagnostics)	299
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**62** [30]
Fail dangerous undetected	61
Annunciation undetected	1
No part	**533**

Total failure rate (safety function)	**1019 FIT**
SFF [31]	**93%**
DC_D	**83%**
MTBF	**74 Years**

SIL AC [32]	**SIL 2**

[30] This value corresponds to a PFH of 6.20E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[31] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

4.3.5 9116 Universal converter, configuration Voltage Aout

The FMEDA carried out on the 9116 Universal converter, configuration Voltage Aout ([C5]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**395**
Fail safe undetected	0
No effect	395
Fail Dangerous Detected (λ_{DD})	**479**
Fail detected (detected by internal diagnostics)	350
Fail low (detected by safety logic solver)	99
Fail high (detected by safety logic solver)	5
Annunciation detected	25
Fail Dangerous Undetected (λ_{DU})	**56** [33]
Fail dangerous undetected	55
Annunciation undetected	1
No part	**620**

Total failure rate (safety function)	**930 FIT**
SFF [34]	**93%**
DC_D	**89%**
MTBF	**74 Years**

SIL AC [35]	**SIL 2**

[33] This value corresponds to a PFH of 5.60E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[34] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

4.3.6 9116 Universal converter, configuration Voltage Relay

The FMEDA carried out on the 9116 Universal converter, configuration Voltage Relay ([C6]) leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**1**
Fail safe detected	1
Fail Safe Undetected (λ_{SU})	**480**
Fail safe undetected	111
No effect	369
Fail Dangerous Detected (λ_{DD})	**353**
Fail detected (detected by internal diagnostics)	332
Annunciation detected	21
Fail Dangerous Undetected (λ_{DU})	**76** [36]
Fail dangerous undetected	75
Annunciation undetected	1
No part	**642**

Total failure rate (safety function)	**910 FIT**
SFF [37]	**91%**
DC_D	**82%**
MTBF	**74 Years**

SIL AC [38]	**SIL 2**

[36] This value corresponds to a PFH of 7.60E-08 1/h. A fault reaction time of 30 seconds requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

[37] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

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

5 Using the FMEDA results

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

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

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

5.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 9116 Universal converter considering a proof test coverage of 95% (see Appendix 1.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in sections 4.3.1 to 4.3.6. The resulting PFD_{AVG} values for a variety of proof test intervals are shown in Table 8.

Table 8: PFD_{AVG} values

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
3w Pt100 Aout	PFD_{AVG} = 2,82E-04	PFD_{AVG} = 4,63E-04	PFD_{AVG} = 1,00E-03
3w Pt100 Relay	PFD_{AVG} = 4,03E-04	PFD_{AVG} = 6,63E-04	PFD_{AVG} = 1,44E-03
Current Aout	PFD_{AVG} = 2,77E-04	PFD_{AVG} = 4,52E-04	PFD_{AVG} = 9,76E-04
Current Relay	PFD_{AVG} = 4,00E-04	PFD_{AVG} = 6,56E-04	PFD_{AVG} = 1,42E-03
Voltage Aout	PFD_{AVG} = 3,66E-04	PFD_{AVG} = 5,99E-04	PFD_{AVG} = 1,30E-03
Voltage Relay	PFD_{AVG} = 4,89E-04	PFD_{AVG} = 8,04E-04	PFD_{AVG} = 1,75E-03

For SIL2 applications, the PFD_{AVG} value needs to be < 1.00E-02. This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is within the range 3% - 5% of the allowed range.

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

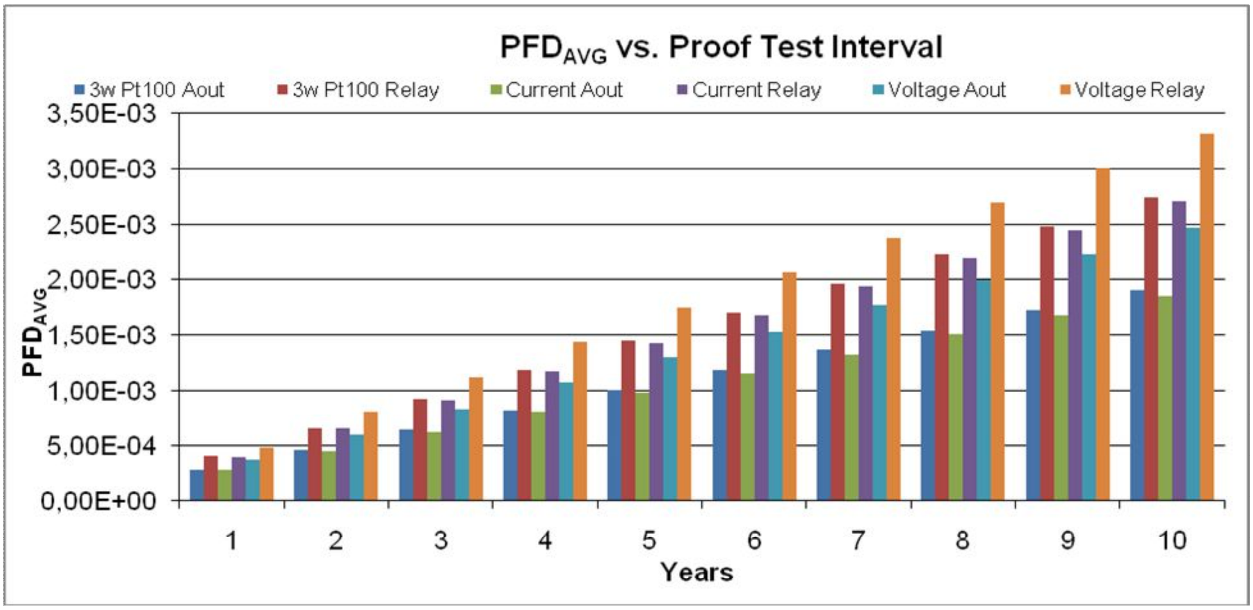

Figure 3: PFD_{AVG}(t)

6 Terms and Definitions

DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B subsystem	"Complex" subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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:	V2R1	Corrected Tables 21 and 32; August 11, 2015
	V2R0:	Non-Ex versions added; July 8, 2014
	V1R1:	Purpose and Scope section modified; September 27, 2010
	V1R0:	Review comments incorporated; May 18, 2010
	V0R1:	Initial version; March 31, 2010
Authors:	Stephan Aschenbrenner, Piotr Serwa	
Review:	V0R1:	Hans Jørgen Eriksen (PR electronics A/S); April 15, 2010
		Rachel Amkreutz (*exida*); May 17, 2010
Release status:	Released to PR electronics A/S as part of a complete functional safety assessment according to IEC 61508.	

Appendix 1 Possibilities to reveal dangerous undetected faults during proof test

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 that have been noted during the FMEDA can be detected during proof testing.

Table 9 shows the importance analysis of the dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Table 9: Importance analysis for 9116 Universal converter 3w Pt100 Aout

Component	% of total λ_{du}	Detection through
IC106-FLASH	24,43%	100% functional test with different expected output signals over the entire range
IC104	17,34%	100% functional test with different expected output signals over the entire range
Z201	14,49%	100% functional test with different expected output signals over the entire range
IC203-RAM	9,15%	100% functional test with different expected output signals over the entire range
IC106-CPU	6,20%	100% functional test with different expected output signals over the entire range
Z104	4,77%	100% functional test with different expected output signals over the entire range
T103	3,58%	100% functional test with different expected output signals over the entire range
IC203-CPU	3,43%	100% functional test with different expected output signals over the entire range
C112	2,38%	100% functional test with different expected output signals over the entire range
C114	2,38%	100% functional test with different expected output signals over the entire range

Table 10: Importance analysis for 9116 Universal converter 3w Pt100 Relay

Component	% of total λ_{du}	Detection through
RE201	32,56%	100% functional test with different expected output signals over the entire range
IC106-FLASH	16,69%	100% functional test with different expected output signals over the entire range
IC104	11,84%	100% functional test with different expected output signals over the entire range
Z201	9,90%	100% functional test with different expected output signals over the entire range
IC203-RAM	6,25%	100% functional test with different expected output signals over the entire range
IC106-CPU	4,23%	100% functional test with different expected output signals over the entire range
Z104	3,26%	100% functional test with different expected output signals over the entire range
T103	2,44%	100% functional test with different expected output signals over the entire range
IC203-CPU	2,34%	100% functional test with different expected output signals over the entire range
C112	1,63%	100% functional test with different expected output signals over the entire range

Table 11: Importance analysis for 9116 Universal converter Current Aout

Component	% of total λ_{du}	Detection through
IC106-FLASH	25,20%	100% functional test with different expected output signals over the entire range
IC104	17,89%	100% functional test with different expected output signals over the entire range
Z201	14,95%	100% functional test with different expected output signals over the entire range
IC203-RAM	9,44%	100% functional test with different expected output signals over the entire range
IC106-CPU	6,39%	100% functional test with different expected output signals over the entire range
Z104	4,92%	100% functional test with different expected output signals over the entire range
IC203-CPU	3,54%	100% functional test with different expected output signals over the entire range
IC106-RAM	2,21%	100% functional test with different expected output signals over the entire range
Z116, Z117, Z118, Z119, Z120, Z121	2,03%	100% functional test with different expected output signals over the entire range
C24	1,48%	100% functional test with different expected

		output signals over the entire range

Table 12: Importance analysis for 9116 Universal converter Current Relay

Component	% of total λ_{du}	Detection through
RE201	33,05%	100% functional test with different expected output signals over the entire range
IC106-FLASH	16,94%	100% functional test with different expected output signals over the entire range
IC104	12,02%	100% functional test with different expected output signals over the entire range
Z201	10,05%	100% functional test with different expected output signals over the entire range
IC203-RAM	6,35%	100% functional test with different expected output signals over the entire range
IC106-CPU	4,30%	100% functional test with different expected output signals over the entire range
Z104	3,31%	100% functional test with different expected output signals over the entire range
IC203-CPU	2,38%	100% functional test with different expected output signals over the entire range
IC106-RAM	1,49%	100% functional test with different expected output signals over the entire range
Z116, Z117, Z118, Z119, Z120, Z121	1,36%	100% functional test with different expected output signals over the entire range

Table 13: Importance analysis for 9116 Universal converter Voltage Aout

Component	% of total λ_{du}	Detection through
IC106-FLASH	18,73%	100% functional test with different expected output signals over the entire range
IC104	13,29%	100% functional test with different expected output signals over the entire range
Z201	11,11%	100% functional test with different expected output signals over the entire range
Z109	10,87%	100% functional test with different expected output signals over the entire range
IC203-RAM	7,02%	100% functional test with different expected output signals over the entire range
IC106-CPU	4,75%	100% functional test with different expected output signals over the entire range
IC107	4,39%	100% functional test with different expected output signals over the entire range
Z104	3,65%	100% functional test with different expected output signals over the entire range
Z129, Z130, Z131	3,01%	100% functional test with different expected

		output signals over the entire range
IC203-CPU	2,63%	100% functional test with different expected output signals over the entire range

Table 14: Importance analysis for 9116 Universal converter Voltage Relay

Component	% of total λ_{du}	Detection through
RE201	26,82%	100% functional test with different expected output signals over the entire range
IC106-FLASH	13,75%	100% functional test with different expected output signals over the entire range
IC104	9,76%	100% functional test with different expected output signals over the entire range
Z201	8,15%	100% functional test with different expected output signals over the entire range
Z109	7,98%	100% functional test with different expected output signals over the entire range
IC203-RAM	5,15%	100% functional test with different expected output signals over the entire range
IC106-CPU	3,49%	100% functional test with different expected output signals over the entire range
IC107	3,22%	100% functional test with different expected output signals over the entire range
Z104	2,68%	100% functional test with different expected output signals over the entire range
Z129, Z130, Z131	2,21%	100% functional test with different expected output signals over the entire range

Appendix 1.1 Possible proof tests to detect dangerous undetected faults

A possible proof test is described in section 10 of the safety manual ([D15]) for the 9116 Universal converter.

This test will detect approximately 95% of possible “du” failures in the transmitter and the connected sensing element.

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[39] 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 components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 15: Useful lifetime of components with reduced useful lifetime contributing to λdu

FMEDA	Type	Name	Useful lifetime
32 Pt100 Relay, Current Relay, Voltage Relay	Relay (w. FE) - Plastic-sealed, low gas emission, tempered plastic, single contacts (alloy on silver basis), >20cN	RE201 (Relay)	Approximately 100.000 switching cycles

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

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

[39] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term that covers product obsolescence, warranty, or other commercial issues.

Appendix 3 Description of the considered profiles

Appendix 3.1 *exida* electronic database:

Profile	Profile according to IEC 60654-1	Ambient Temperature [°C]		Temperature Cycle [°C / 365 days]
		Average (external)	Mean (inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25

PROFILE 1:

Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

PROFILE 2:

Low power electrical (two-wire) field products have minimal self-heating and are subjected to daily temperature swings.

PROFILE 3:

General (four-wire) field products may have moderate self-heating and are subjected to daily temperature swings.

Appendix 4 Using the FMEDA results

The 9116 Universal converter together with a temperature sensing device becomes a temperature sensor assembly. 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.

Appendix 4.1 9116 Universal converter with thermocouple

The failure mode distributions for thermocouples (TC) 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 16 and Table 17 when thermocouples are supplied with the 9116 Universal converter. The drift failure mode is primarily due to T/C aging. The 9116 Universal converter will detect a thermocouple burn-out failure and drive its output to the specified failure state.

Table 16: Typical failure rates for thermocouples (with extension wire)

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

Table 17: Typical failure rates for thermocouples (close coupled)

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

A complete temperature sensor assembly consisting of the 9116 Universal converter and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Table 18: Thermocouple fault classification

Failure mode	Classification
Open circuit	Dangerous detected
Short circuit	Dangerous undetected
Drift	Dangerous undetected

As a result, the failure rate contribution for the thermocouple is as follows.

Table 19: Thermocouple (with extension wire)

Low stress environment	High stress environment
λ_{dd} = 900 FIT	λ_{dd} = 18000 FIT
λ_{du} = 50 FIT + 50 FIT = 100 FIT	λ_{du} = 1000 FIT + 1000 FIT = 2000 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

Table 20: Thermocouple (close coupled)

Low stress environment	High stress environment
λ_{dd} = 95 FIT	λ_{dd} = 1900 FIT
λ_{du} = 4 FIT + 1 FIT = 5 FIT	λ_{du} = 80 FIT + 20 FIT = 100 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

This results in a failure rate distribution and SFF as shown below for a 9116 Universal converter together with a thermocouple with current output or relay output.

The failure rates for the 9116 Universal converter with the thermocouple are sums of corresponding failure rates of the converter and of the thermocouple.

Table 21: 9116 Universal converter with thermocouple

Transmitter	Extension wire	Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
TC Aout	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	900 FIT + 310 FIT = 1 210 FIT	100 FIT + 42 FIT = 142 FIT	91%
TC Aout	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	18 000 FIT + 310 FIT = 18 310 FIT	2 000 FIT + 42 FIT = 2 042 FIT	90%
TC Aout	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	95 FIT + 310 FIT = 405 FIT	5 FIT + 42 FIT = 47 FIT	93%
TC Aout	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	1 900 FIT + 310 FIT = 2 210 FIT	100 FIT + 42 FIT = 142 FIT	94%
TC Relay	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	900 FIT + 261 FIT = 1 161 FIT	100 FIT + 61 FIT = 161 FIT	90%
TC Relay	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	18 000 FIT + 261 FIT = 18 261 FIT	2 000 FIT + 61 FIT = 2 061 FIT	90%
TC Relay	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	95 FIT + 261 FIT = 356 FIT	5 FIT + 61 FIT = 66 FIT	91%
TC Relay	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	1 900 FIT + 261 FIT = 2 161 FIT	100 FIT + 61 FIT = 161 FIT	93%

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

Appendix 4.2 9116 Universal converter with RTD

The failure mode distribution for an RTD depends on the application with the key variables being stress level, presence (or not) of extension wire and wire configuration (2-wire/3-wire or 4-wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions are shown in Table 22, Table 23, Table 24 and Table 25. The 9116 Universal converter will detect open circuit, short circuit and a certain percentage of drift RTD failures and drive their output to the specified failure state.

Table 22: Typical failure rates for 4-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	Low Stress	High Stress
Open Circuit (Burn-out)	410 FIT	8200 FIT
Short Circuit (Temperature measurement in error)	20 FIT	400 FIT
Drift (Temperature Measurement in error)	70 FIT [40]	1400 FIT [41]

Table 23: Typical failure rates for 4-Wire RTDs (close coupled)

RTD Failure Mode Distribution	Low Stress	High Stress
Open Circuit (Burn-out)	41.5 FIT	830 FIT
Short Circuit (Temperature measurement in error)	2.5 FIT	50 FIT
Drift (Temperature Measurement in error)	6 FIT [42]	120 FIT [43]

Table 24: Typical failure rates for 2-Wire and 3-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	Low Stress	High Stress
Open Circuit (Burn-out)	370.5 FIT	7410 FIT
Short Circuit (Temperature measurement in error)	9.5 FIT	190 FIT
Drift (Temperature Measurement in error)	95 FIT	1900 FIT

Table 25: Typical failure rates for 2-Wire and 3-Wire RTDs (close coupled)

RTD Failure Mode Distribution	Low Stress	High Stress
Open Circuit (Burn-out)	37.92 FIT	758.4 FIT
Short Circuit (Temperature measurement in error)	1.44 FIT	28.8 FIT
Drift (Temperature Measurement in error)	8.64 FIT	172.8 FIT

A complete temperature sensor assembly consisting of the 9116 Universal converter and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

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

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

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

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

Table 26: Fault classification for 4-Wire RTD

Failure mode	Classification
Open circuit	Dangerous detected
Short circuit	Dangerous detected
Drift	Most of it is dangerous detected, remaining part dangerous undetected (assuming a correct use of 4-wire RTD)

Table 27: 4-Wire RTD (with extension wire)

Low stress environment	High stress environment
λ_{dd} = 410 FIT + 20 FIT + 65 FIT = 495 FIT	λ_{dd} = 8200 FIT + 400 FIT + 1300 FIT = 9900 FIT
λ_{du} = 5 FIT	λ_{du} = 100 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

Table 28: 4-Wire RTD (close coupled)

Low stress environment	High stress environment
λ_{dd} = 41.5 FIT + 2.5 FIT + 3.5 FIT = 47.5 FIT	λ_{dd} = 830 FIT + 50 FIT + 70 FIT = 950 FIT
λ_{du} = 2.5 FIT	λ_{du} = 50 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

Table 29: Fault classification for 2-Wire and 3-Wire RTD

Failure mode	Classification
Open circuit	Dangerous detected
Short circuit	Dangerous detected
Drift	Dangerous undetected

Table 30: 2-Wire and 3-Wire RTD (with extension wire)

Low stress environment	High stress environment
λ_{dd} = 370.5 FIT + 9.5 FIT = 380 FIT	λ_{dd} = 7410 FIT + 190 FIT = 7600 FIT
λ_{du} = 95 FIT	λ_{du} = 1900 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

Table 31: 2-Wire and 3-Wire RTD (close coupled)

Low stress environment	High stress environment
λ_{dd} = 37.92 FIT + 1.44 FIT = 39.36 FIT	λ_{dd} = 758.4 FIT + 28.8 FIT = 787.2 FIT
λ_{du} = 8.64 FIT	λ_{du} = 172.8 FIT
λ_{su} = 0 FIT	λ_{su} = 0 FIT
λ_{sd} = 0 FIT	λ_{sd} = 0 FIT

This results in a failure rate distribution and SFF as shown below for a 9116 Universal converter together with a RTD with current output or relay output.

The failure rates for the 9116 Universal converter with the RTD are sums of corresponding failure rates of the converter and of the RTD.

Table 32: 9116 Universal converter with 4-Wire RTD

Transmitter	Extension wire	Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
4w Pt100 Aout	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	495 FIT + 310 FIT = 805 FIT	5 FIT + 42 FIT = 47 FIT	95%
4w Pt100 Aout	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	9 900 FIT + 310 FIT = 10 210 FIT	100 FIT + 42 FIT = 142 FIT	98%
4w Pt100 Aout	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	48 FIT + 310 FIT = 358 FIT	3 FIT + 42 FIT = 45 FIT	93%
4w Pt100 Aout	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	950 FIT + 310 FIT = 1 260 FIT	50 FIT + 42 FIT = 92 FIT	94%
4w Pt100 Relay	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	495 FIT + 261 FIT = 756 FIT	5 FIT + 61 FIT = 66 FIT	94%
4w Pt100 Relay	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	9 900 FIT + 261 FIT = 10 161 FIT	100 FIT + 61 FIT = 161 FIT	98%
4w Pt100 Relay	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	48 FIT + 261 FIT = 309 FIT	3 FIT + 61 FIT = 64 FIT	90%
4w Pt100 Relay	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	950 FIT + 261 FIT = 1 211 FIT	50 FIT + 61 FIT = 111 FIT	93%

Table 33: 9116 Universal converter with 2-Wire and 3-Wire RTD

Transmitter	Extension wire	Environment	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
3w Pt100 Aout	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	380 FIT + 310 FIT = 690 FIT	95 FIT + 42 FIT = 137 FIT	88%
3w Pt100 Aout	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	7 600 FIT + 310 FIT = 7 910 FIT	1 900 FIT + 42 FIT = 1 942 FIT	80%
3w Pt100 Aout	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	39 FIT + 310 FIT = 349 FIT	9 FIT + 42 FIT = 51 FIT	92%
3w Pt100 Aout	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 321 FIT = 321 FIT	787 FIT + 310 FIT = 1 097 FIT	173 FIT + 42 FIT = 215 FIT	86%
3w Pt100 Relay	With	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	380 FIT + 261 FIT = 641 FIT	95 FIT + 61 FIT = 156 FIT	86%
3w Pt100 Relay	With	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	7 600 FIT + 261 FIT = 7 861 FIT	1 900 FIT + 61 FIT = 1 961 FIT	80%
3w Pt100 Relay	Without	Low stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	39 FIT + 261 FIT = 300 FIT	9 FIT + 61 FIT = 70 FIT	90%
3w Pt100 Relay	Without	High stress	0 FIT + 0 FIT = 0 FIT	0 FIT + 329 FIT = 329 FIT	787 FIT + 261 FIT = 1 048 FIT	173 FIT + 61 FIT = 234 FIT	85%

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