Failure Modes, Effects and Diagnostic Analysis

Project:
9113 Temperature / mA converter

Customer:

PR electronics A/S
Rønde
Denmark

Contract No.: PR electronics 06/03-19
Report No.: PR electronics 06/03-19 R022
Version V2, Revision R1; July 2014
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the 9113 Temperature / mA converter with HW/SW version 9113-1-V4R0.

There are two variants of the 9113 Temperature / mA converter: The 9113BA (Ex version) / 9113AA (standard version) with one channel and the variant 9113BB (Ex version) / 9113AB (standard version) which provides two channels.

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

For safety applications only the described version is considered. All other possible output variants or electronics 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. 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 two channels on the two channel devices shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

The 9113 Temperature / mA converter is considered to be a Type B[1] 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. 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 as per the NAMUR NE43 signal ranges, i.e. the 9113 Temperature / mA 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 have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled.

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

Table 1: Summary for the 9113 Temperature / mA converter - IEC 61508 failure rates

	exida Profile 1 [2]
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**234**
Fail safe undetected	31
No effect	202
Annunciation undetected (95%)	1
Fail Dangerous Detected (λ_{DD})	**367**
Fail detected (detected by internal diagnostics)	219
Fail low (detected by safety logic solver)	123
Fail high (detected by safety logic solver)	5
Annunciation detected	20
Fail Dangerous Undetected (λ_{DU})	**61** [3]
Fail dangerous undetected	61
Annunciation undetected (5%)	0
No part	364

Total failure rate (safety function)	**662 FIT**
SFF [4]	**90.7%**
DC_D	**86%**
MTBF	**111 years**

SIL AC [5]	**SIL2**

The failure rates are valid for the useful life of the 9113 Temperature / mA converter (see Appendix 2).

[2] For details see Appendix 3.

[3] This value corresponds to a PFH of 6.10E-08 1/h. A fault reaction time of 5 seconds requires also 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 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 shall describe the results of the FMEDA carried out on the 9113 Temperature / mA converter with HW/SW version 9113-1-V4R0. 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 9113 Temperature / mA 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 9113 Temperature / mA 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 and PFD_{AVG} calculation of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*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]	9113 schematic V4R0.pdf of 10.08.09	Schematic drawings, No. 9113-1-V4R0-SH (page 1 to 6) of 10.08.09
[D2]	9113-BA-2005.pdf of 07.09.09	Components of housing for 9113
[D3]	9113SMDA-2015.pdf of 07.09.09	List of components for 9113
[D4]	9113 Hardware Fault Insertion Test Report V3R0.doc of 04.09.09	Hardware fault insertion test report
[D5]	9113 Circuit description V1R0.doc of 31.08.09	Circuit description revision of 13.08.09
[D6]	9113 CPU failure distribution estimation V0R3.xls of 26.08.09	Failure distribution for used CPUs
[D7]	9113 FMEDA single channel V0R13.xls of 23.09.09	FMEDA results file generated by customer
[D8]	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]	FMEDA_Review_120809.txt	FMEDA review comments
[R2]	FMEDA_Review_200909.txt	FMEDA review comments

3 Description of the analyzed subsystem

The 9113 Temperature / mA converter converts various sensor input signals to a 4..20 mA current output signal and provides an isolation of input signals from hazardous areas (9113BA and 9113BB), temperature or standard signal (e.g. 4..20mA, 0..10V, etc.) signals, to any superior logic solver system or safety PLC.

These sensors/input signals may vary as such as RTD, thermocouple input, linear current/voltage input, 2(3 or 4)-wire transmitter, linear resistance and potentiometer input.

The 9113 Temperature / mA converter is available in a single (type 9113BA / 9113AA) and a dual channel version (type 9113BB / 9113AB).

The 9113BB / 9113AB - Temperature / mA Converter has two separate measurement channels. The required level of independence between them is provided by the clear separation of the channel related hardware circuitry which have their own pair of input / output micro-controllers, including isolation, meeting applicable requirement for ex-products (9113BB) and provide protection of the effect of faults related to power distribution in the channel-related circuitry.

Figure 1 gives an overview of the considered device.

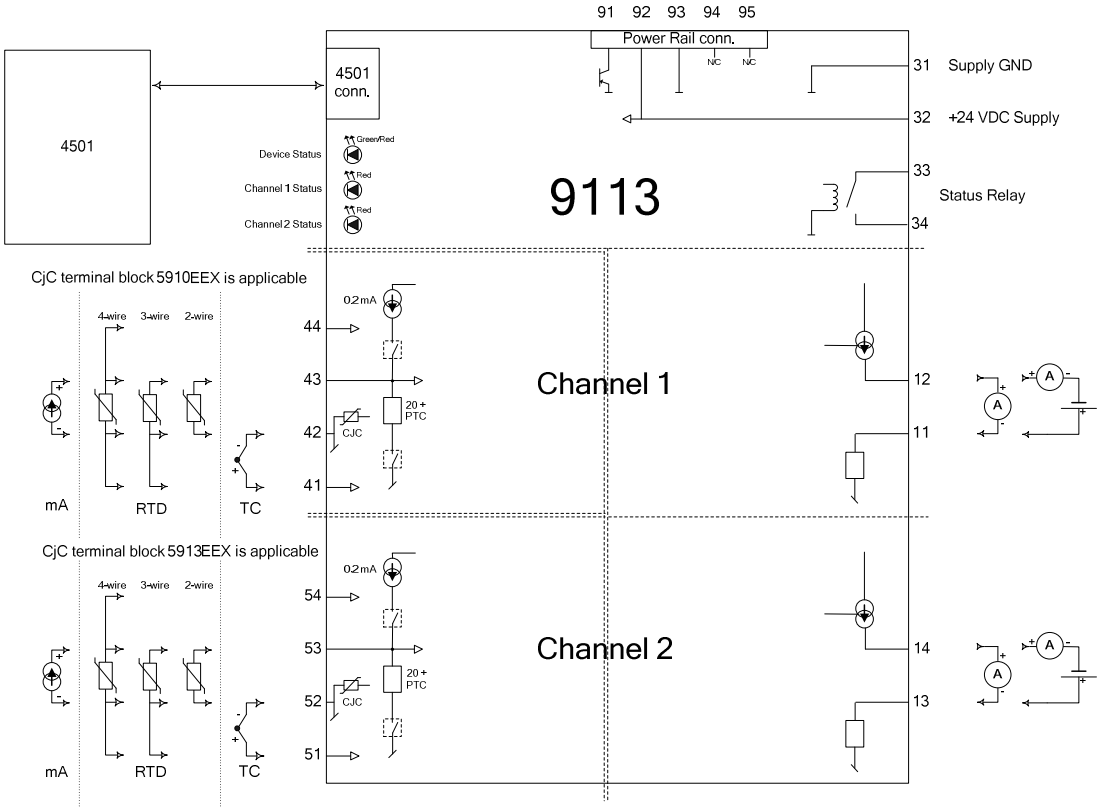

Figure 1: Block diagram

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by PR electronics A/S and reviewed by *exida*. The results are documented in [D7]. 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 [D4]). 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 9113 Temperature / mA converter, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output reaching the user defined threshold value.
Fail Safe	Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that corrupts the measured value by more than 2% of full span (0.32mA) and therefore has the potential to not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
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	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure and does not corrupt the measured value by more than 2% of full span (0.32mA). 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 to 5% as a “Dangerous Undetected” failure and to 95% as a “No Effect” failure.
No Part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

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

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 9113 Temperature / mA 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 5 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 9113 Temperature / mA converter

The FMEDA carried out on 9113 Temperature / mA converter leads under the assumptions described in section 4.2.3 to the following failure rates:

	***exida* Profile 1** [6]
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**234**
Fail safe undetected	31
No effect	202
Annunciation undetected (95%)	1
Fail Dangerous Detected (λ_{DD})	**367**
Fail detected (detected by internal diagnostics)	219
Fail low (detected by safety logic solver)	123
Fail high (detected by safety logic solver)	5
Annunciation detected	20
Fail Dangerous Undetected (λ_{DU})	**61** [7]
Fail dangerous undetected	61
Annunciation undetected (5%)	0
No part	364

Total failure rate (safety function)	**662 FIT**
SFF [8]	**90.7%**
DC_D	**86%**
MTBF	**111 years**

SIL AC [9]	**SIL2**

[6] For details see Appendix 3.

[7] This value corresponds to a PFH of 6.10E-08 1/h. A fault reaction time of 5 seconds requires also that a connected device can detect the output state within a time that allows reacting within the process safety time.

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

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply 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) 9113 Temperature / mA 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 is displayed in section 4.3.1. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 2.

For SIL2 applications, the PFD_{AVG} value needs to be < 1.00E-02.

Table 2: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.96E-04	PFD_{AVG} = 6.5E-04	PFD_{AVG} = 1.41E-03

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 4% of the allowed range.

Figure 2 shows the time dependent curve of PFD_{AVG}.

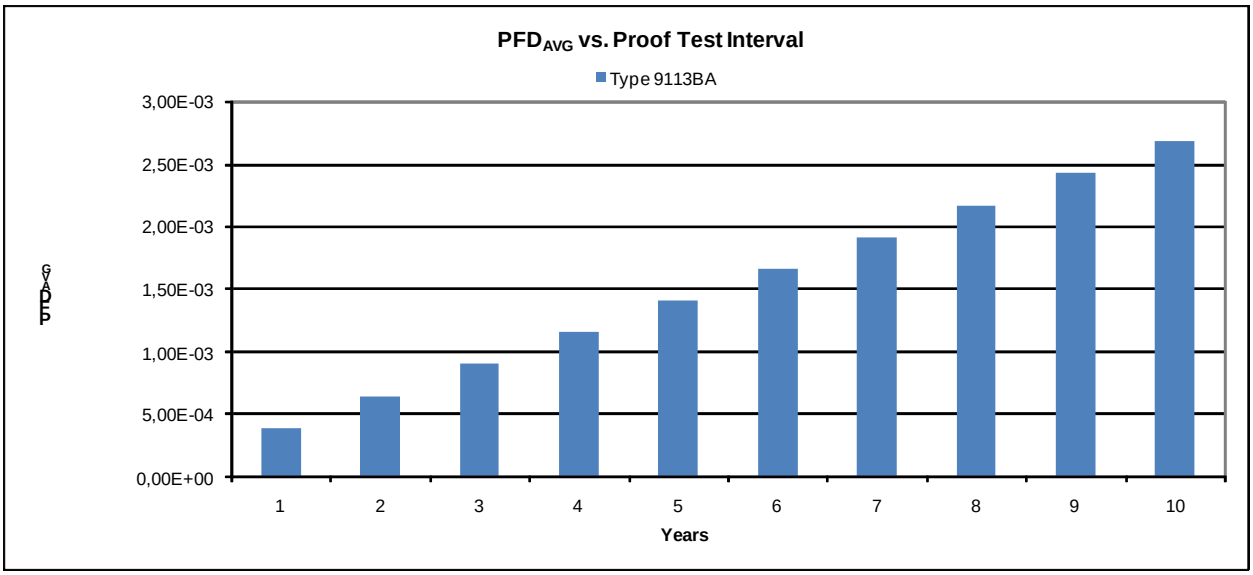

Figure 2: $PFD_{AVG}(t)$

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:	Editorial changes; July 10, 2014
	V2R0:	Non-Ex versions added; July 8, 2014
	V1R1:	Purpose and Scope section modified; September 27, 2010
	V1R0:	Review comments incorporated; October 19, 2009
	V0R1:	Initial version; October 2, 2009
Authors:	Stephan Aschenbrenner, Alexander Dimov	
Review:	V2R0:	Flemming Svanholm Sørensen (PR electronics A/S); July 10, 2012
	V0R1:	Rachel Amkreutz (*exida*); October 13, 2009
		Hans Jørgen Eriksen (PR electronics A/S); October 13, 2009
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 the 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 which have been noted during the FMEDA can be detected during proof testing.

Table 3 shows an 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 3: Importance analysis of dangerous undetected faults

Component	% of total λ_{du}	Detection through
IC106-FLASH	16,44%	100% functional test with different expected output signals over the entire range
IC104	11,67%	100% functional test with different expected output signals over the entire range
Z201	9,75%	100% functional test with different expected output signals over the entire range
Z102	9,54%	100% functional test with different expected output signals over the entire range
Z103	9,54%	100% functional test with different expected output signals over the entire range
IC203-RAM	6,16%	100% functional test with different expected output signals over the entire range
IC106-CPU	4,17%	100% functional test with different expected output signals over the entire range
Z104	3,21%	100% functional test with different expected output signals over the entire range
D205	2,57%	100% functional test with different expected output signals over the entire range
C220	2,57%	100% functional test with different expected output signals over the entire range

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 4.

Table 4: Suggested proof test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	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. 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	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. This tests for possible quiescent current related failures
4	Perform a two-point calibration of the transmitter.
5	Restore the loop to full operation.
6	Remove the bypass from the safety PLC or otherwise restore normal operation.

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[10] 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 which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

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

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

Appendix 3: Description of the considered profiles

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 9113 Temperature / mA 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: 9113 Temperature / mA converter 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 5 and Table 6 when thermocouples are supplied with the 9113 Temperature / mA converter. The drift failure mode is primarily due to T/C aging. The 9113 Temperature / mA converter will detect a thermocouple burn-out failure and drive its output to the specified failure state.

Table 5 Typical failure rates for thermocouples (with extension wire)

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

Table 6 Typical failure rates for thermocouples (close coupled)

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

A complete temperature sensor assembly consisting of the 9113 Temperature / mA 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. Assuming that the 9113 Temperature / mA converter will go to the pre-defined alarm state on detected failures of the thermocouple, the failure rate contribution for the thermocouple is:

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

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

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

Table 7: 9113 Temperature / mA converter with thermocouple (low tress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	1267 FIT	161 FIT	90.3 %

Table 8: 9113 Temperature / mA converter with thermocouple (low tress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	462 FIT	66 FIT	91.3 %

Table 9: 9113 Temperature / mA converter with thermocouple (high tress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	18367 FIT	2061 FIT	90.0 %

Table 10: 9113 Temperature / mA converter with thermocouple (high tress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	2267 FIT	161 FIT	93.9 %

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

Appendix 4.2: 9113 Temperature / mA converter 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 are shown in Table 11 to Table 14. The 9113 Temperature / mA 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 11 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 [11]	1400 FIT [12]

Table 12 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 [13]	120 FIT [14]

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

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

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

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

Table 13 Typical failure rates for 2/3-Wire RTDs (with extension wire)

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

Table 14 Typical failure rates for 2/3-Wire RTDs (close coupled)

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

A complete temperature sensor assembly consisting of the 9113 Temperature / mA 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. Assuming that the 9113 Temperature / mA converter will go to the pre-defined alarm state on a detected failure of the RTD, the failure rate contribution for the RTD is:

4-wire RTD 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

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

2/3-wire RTD with extension wire:

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

2/3-wire RTD close coupled:

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

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

Table 15: 9113 Temperature / mA converter with 4-wire RTD (low stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	862 FIT	66 FIT	94.3 %

Table 16: 9113 Temperature / mA converter with 4-wire RTD (low stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	414.5 FIT	63.5 FIT	91.0 %

Table 17: 9113 Temperature / mA converter with 4-wire RTD (high stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	7967 FIT	1961 FIT	93.9 %

Table 18: 9113 Temperature / mA converter with 4-wire RTD (high stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	1317 FIT	111 FIT	93.3 %

Table 19: 9113 Temperature / mA converter with 2/3-wire RTD (low stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	747 FIT	156 FIT	86.3 %

Table 20: 9113 Temperature / mA converter with 2/3-wire RTD (low stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	406.36 FIT	69.64 FIT	81.6 %

Table 21: 9113 Temperature / mA converter with 2/3-wire RTD (high stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	7967 FIT	1961 FIT	80.7 %

Table 22: 9113 Temperature / mA converter with 2/3-wire RTD (high stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
0 FIT	234 FIT	1154.2 FIT	233.8 FIT	85.6 %

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