FMEDA and Proven-in-use Assessment

Project:
Temperature Transmitter Type 9182/*0-5*-*4
(contact output)

Customer:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 07/07-23
Report No.: STAHL 07/07-23 R017
Version V2, Revision R1; January 2010
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 with proven-in-use consideration carried out on the Temperature Transmitter Type 9182/*0-5*-*4 with hardware version Rev. B and software version V01-09. Table 1 gives an overview of the different versions that belong to the considered Temperature Transmitter Type 9182/*0-5*-*4.

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

Table 1: Version overview

9182/10-50-14	1 channel, contact output 1x2 contacts	I.S. [1]
9182/10-50-64	1 channel, contact output 1x2 contacts	non I.S.
9182/20-50-14	2 channels, contact output 2x2 contacts	I.S.
9182/20-50-64	2 channels, contact output 2x2 contacts	non I.S.
9182/10-51-14	channel 1, 4..20mA current output active channel 2, contact output 1x2 contacts	I.S.
9182/10-51-64	channel 1, 4..20mA current output active channel 2, contact output 1x2 contacts	non I.S.
9182/10-59-14	channel 1, 4..20mA current output passive channel 2, contact output 1x2 contacts	I.S.
9182/10-59-64	channel 1, 4..20mA current output passive channel 2, contact output 1x2 contacts	non I.S.

For safety applications only the described contact output versions were considered. All other possible output variants or electronics are not covered by this report. The 4..20mA current output versions are covered by the report "STAHL 9182-x3-x4 4-20mA 07-07-23 R016".

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1. The analysis has also been 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 only the results based on 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 contact outputs can be connected in series. Therefore the Temperature Transmitter Type 9182/*0-5*-*4 could be split into two separate subsystems; one representing the input and logic part having a hardware fault tolerance of 0 and one representing the output part having a hardware fault tolerance of 1.

[1] I.S. Intrinsic Safety

For simplicity reasons the analysis was done by considering one of the outputs to be the "diagnostics" for the “primary” output. A diagnostic coverage (DC) of 90% was considered to account for possible common cause failures (this is equivalent to a beta factor of 10%).

The Temperature Transmitter Type 9182/*0-5*-*4 is considered to be 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 shall be > 90% for SIL 2 subsystems according to table 3 of IEC 61508-2.

As the Temperature Transmitter Type 9182/*0-5*-*4 is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by R. STAHL Schaltgeräte GmbH.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the ***exida*** proven-in-use assessment described in section 6, the Temperature Transmitter Type 9182/*0-5*-*4 with a SFF of < 90% might also be used for a SIL 2 safety function. The decision on the usage of proven-in-use devices, however, is always with the end-user.

A user of the Temperature Transmitter Type 9182/*0-5*-*4 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates for different operating conditions is presented in section 4.4.1 along with all assumptions.

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

The following table shows how the above stated requirements are fulfilled.

[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 – Failure rates for 9182/*0-5*-*4 with contact output

	exida **Profile 1**
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**299**
Fail safe undetected	150
No effect	130
Annunciation undetected (95%)	19
Fail Dangerous Detected (λ_{DD})	**232**
Fail dangerous detected	232
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**146**
Fail dangerous undetected	145
Annunciation undetected (5%)	1
No part	323

Total failure rate (safety function)	**677 FIT**
SFF [3]	**78.4%**
DC_D	**61%**
MTBF	**114 years**

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

Table 3: Summary – Failure rates for 9182/*0-5*-*4 with two contact outputs in series

	exida **Profile 1**
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**308**
Fail safe undetected	150
No effect	130
Annunciation undetected (95%)	28
Fail Dangerous Detected (λ_{DD})	**241**
Fail dangerous detected	241
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**128**
Fail dangerous undetected	126
Annunciation undetected (5%)	2
No part	323

Total failure rate (safety function)	**677 FIT**
SFF [4]	**81.1%**
DC_D	**65%**
MTBF	**114 years**

The failure rates are valid for the useful life of the Temperature Transmitter Type 9182/*0-5*-*4 (see Appendix 2).

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

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 2.

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the Temperature Transmitter Type 9182/*0-5*-*4 with hardware version Rev. B and software version V01-09. Table 1 gives an overview of the different versions that belong to the considered Temperature Transmitter Type 9182/*0-5*-*4.

The information in this report can be used to evaluate whether a sensor subsystem, including the Temperature Transmitter Type 9182/*0-5*-*4 meets the average Probability of Failure on Demand (PFD_{AVG}) 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 of the parties involved

R. STAHL Schaltgeräte GmbH	Manufacturer of the Temperature Transmitter Type 9182/*0-5*-*4.
exida	Performed the hardware assessment according to option 1 (see section 1).

R. STAHL Schaltgeräte GmbH contracted *exida* in October 2008 with the FMEDA of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	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]	9182_Temperaturmessumformer_CD60_E.pdf	Technical Information of the Temperature Transmitter Type 9182
[D2]	91 826 01 20 0_04.pdf	Circuit diagram "Temperature Transmitter Type 9182/*0-5*-**" 91 826 01 20 0 Index 04 of 21.12.09
[D3]	91 826 02 20 0_04.pdf	Table for circuit diagram "Temperature Transmitter Type 9182/*0-5*-**" 91 826 01 20 0 Index 04 of 21.12.09
[D4]	Stueckliste 9182 10-51-x4.pdf	Parts list for 9182
[D5]	Cadstar - 9182_Var_IX2.pdf	Mounting list for the different configurations of 9182
[D6]	1_1_de_matrix_reklamationsabwicklung.pdf	Field data evaluation process
[D7]	1_1_de_checkliste_fuer_qualitaetskreise.pdf	Checklist for the field data evaluation process

[D8]	ISpac HW FW Revisions 9182.pdf	History of hardware and software revisions
[D9]	Kunden_Referenz_Liste_Typ 9182_Jahr 06_07.xlsx of 28.07.08	List of applications
[D10]	stückzahlen 9182__für SIL Betrachtung5.xls of 14.08.2009	Field data evaluation (sold devices; operating hours)
[D11]	9182 Abfrage 09.10.09.xls 02.11.2009	Field data evaluation (returned devices, evaluation process)
[D12]	Checkliste_Impact analyse.zip of 01.08.08	Impact analyses for modifications from V01-04 to V01-08
[D13]	Zuordnung_ MANTIS zu TESTS_04.pdf	Reference between modification and executed tests
[D14]	V_V test plan_Specification.zip of 01.08.08	Test specifications and reports for the modifications from V01-04 to V01-08
[D15]	Version V01-04 zu V01-05.zip	Highlighted software changes from version V01-04 to V01-05
[D16]	Version V01-05 zu V01-06.zip	Highlighted software changes from version V01-05 to V01-06
[D17]	Version V01-06 zu V01-07.zip	Highlighted software changes from version V01-06 to V01-07
[D18]	Version V01-07 zu V01-08.zip	Highlighted software changes from version V01-07 to V01-08
[D19]	MANTIS_ID000007.pdf MANTIS_ID000008.pdf MANTIS_ID000009.pdf	Impact analyses for modifications from V01-08 to V01-09
[D20]	INT-009_00.pdf INT-010_00.pdf INT-011_00.pdf	Test specifications and reports for the modifications from V01-08 to V01-09
[D21]	COR-001_01.pdf	Results of code review for function compose_output_data()
[D22]	Zuordnungsatabelle Modultyp-moduloption und Funktion compose_output_data( ).pdf	Comparison table for modifications from V01-08 to V01-09
[D23]	9182_SIL2_08.07.07.eap of 21.07.08	Software Architecture Specification
[D24]	Entwicklungshandbuch SM aktuell_auszug.zip	Development handbook
[D25]	1_1_de_aenderungsprozess1.pdf	Flow diagram “Modification Process” according to the new development process
[D26]	1_1_de_aenderungsprozess2.pdf	Flow diagram “Modification Process” according to the new development process
[D27]	NF V01-31 V02-31.zip	Examples of the modification process

[D28]	9475 30.7.03.pdf	Modification request DOM
[D29]	Checkliste SM Phase 2 Änderung SW1.xls	Checklist phase 2 “software modification”
[D30]	rpt_PrüfBericht3027.pdf	Example of a repair report
[D31]	Safety Manual 9182GW_en_20091217.docx	Draft safety manual
[D32]	Fehlerversuche_9182-GW_20091222.xlsx	Fault insertion tests
[D33]	9182-GrenzwertAusgang_B.docx of 23.12.09	Description of additional versions
[D34]	FMEDA V7.1.5 9182-10-51-X4 binary output V1R3.efm of 23.12.09	
[D35]	FMEDA V7.1.5 9182-10-51-X4 binary output-outputs in series V1R0.efm of 23.12.09	

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V7.1.5 9182-10-51-X4 binary output V1R2.efm of 09.10.08

3 Description of the analyzed subsystem

The Temperature Transmitter Type 9182/*0-5*-*4 is considered to be a Type B subsystem with a hardware fault tolerance of 0.

The FMEDA of the Temperature Transmitter Type 9182/*0-5*-*4 has been carried out on the parts within the red rectangular indicated in Figure 1.

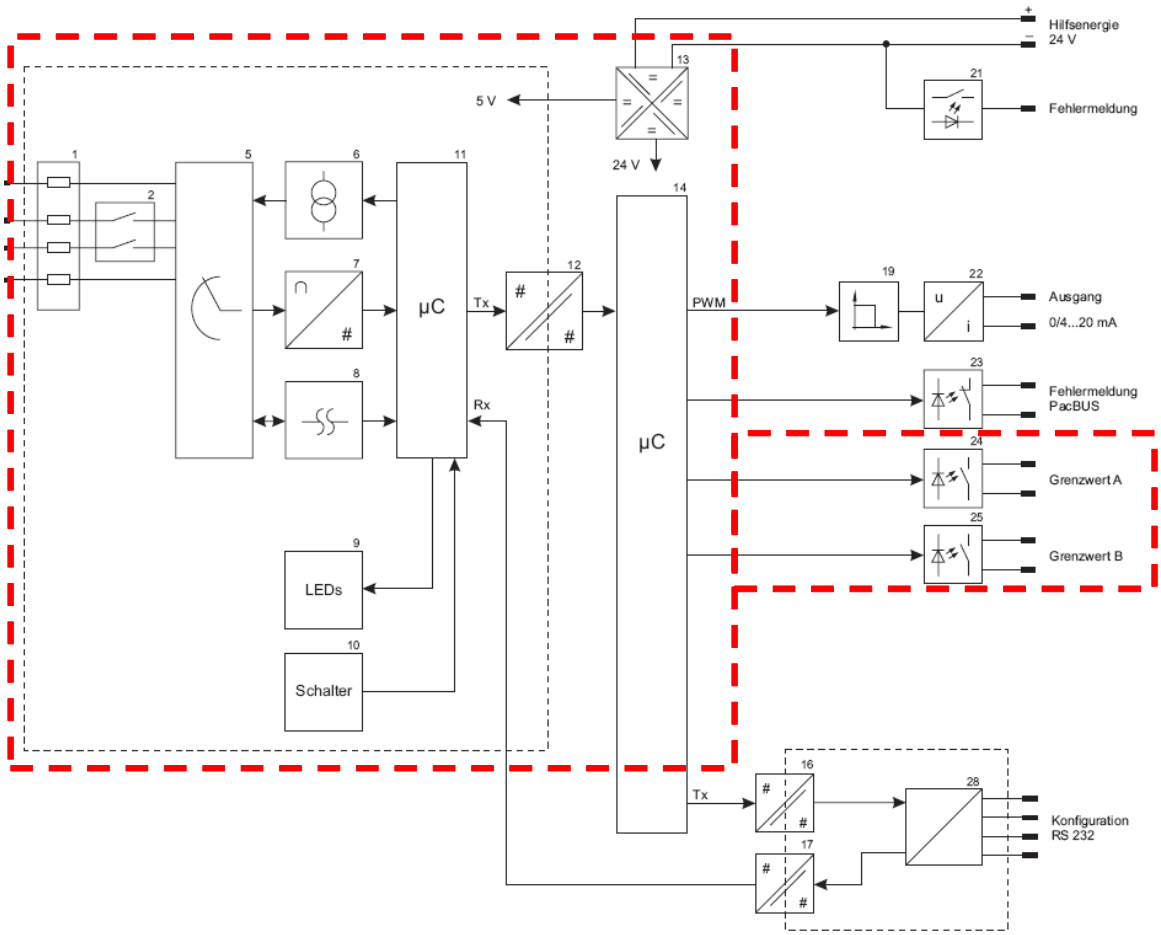


Figure 1: Block diagram of the Temperature Transmitter Type 9182/10-5*-*4

Figure 1 is representative for all Temperature Transmitter Type 9182/*0-5*-*4 listed in Table 1.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with R. STAHL Schaltgeräte GmbH and is documented in [D34] and [D35].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level, see fault insertion test report [D32].

4.1 Description of the failure categories

In order to judge the failure behavior of the Temperature Transmitter Type 9182/*0-5*-*4, the following definitions for the failure of the product were considered.

Fail-Safe State	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	Failure that 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.
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 failure and to 95% as a no effect failure.
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. For the calculation of the SFF it is treated like a safe undetected 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 “No effect” and “Annunciation” 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, physical abuse, or problems due to intermittent instrument air quality.

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”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Temperature Transmitter Type 9182/*0-5*-*4.

- 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.
- For safety applications only the described outputs are considered, i.e. relay output.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- The worst-case internal fault detection time is 60 seconds.
- All modules are operated in the low demand mode of operation.
- Only one input and one output are part of the considered safety function.
- 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.
- The output signal is fed to a SIL 2 compliant input board of a safety PLC.
- Lead breakage detection is activated.

4.4 Results

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

λ_{total} consists of the sum of all component failure rates. This means:

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

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

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

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

4.4.1 Type 9182/*0-5*-*4 with one contact output

The FMEDA carried out on the Temperature Transmitter Type 9182/*0-5*-*4 with one contact output leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 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})	**299**
Fail safe undetected	150
No effect	130
Annunciation undetected (95%)	19
Fail Dangerous Detected (λ_{DD})	**232**
Fail dangerous detected	232
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**146**
Fail dangerous undetected	145
Annunciation undetected (5%)	1
No part	323

Total failure rate (safety function)	**677 FIT**
SFF [5]	**78.4%**
DC_D	**61%**
MTBF	**114 years**

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the ***exida*** proven-in-use assessment described in section 6, the Temperature Transmitter Type 9182/*0-5*-*4 with a SFF of 78% might also be used for a SIL 2 safety function. The decision on the usage of proven-in-use devices, however, is always with the end-user.

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

4.4.2 9182/*0-5*-*4 with two contact outputs in series

The FMEDA carried out on the Temperature Transmitter Type 9182/*0-5*-*4 with two contact outputs in series leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 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})	**308**
Fail safe undetected	150
No effect	130
Annunciation undetected (95%)	28
Fail Dangerous Detected (λ_{DD})	**241**
Fail dangerous detected	241
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**128**
Fail dangerous undetected	126
Annunciation undetected (5%)	2
No part	323

Total failure rate (safety function)	**677 FIT**
SFF [6]	**81.1%**
DC_D	**65%**
MTBF	**114 years**

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the ***exida*** proven-in-use assessment described in section 6, the Temperature Transmitter Type 9182/*0-5*-*4 with a SFF of 81% might also be used for a SIL 2 safety function. The decision on the usage of proven-in-use devices, however, is always with the end-user.

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

5 Using the FMEDA results

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

5.1 Temperature sensing devices

The Temperature Transmitter Type 9182/*0-5*-*4 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. Typical failure rates for thermocouples and RTDs with extension wires are listed in the following table.

Table 4 Typical failure rates of thermocouples and RTDs with extension wire

Temperature Sensing Device	Failure rate (FIT)
Thermocouple low stress environment	1000
Thermocouple high stress environment	20000
4-wire RTD low stress environment	500
4-wire RTD high stress environment	10000

5.1.1 Temperature Transmitter Type 9182/*0-5*-*4 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 the following table when thermocouples with extension wires are supplied with the Temperature Transmitter Type 9182/*0-5*-*4. The drift failure mode is primarily due to T/C aging. The Temperature Transmitter Type 9182/*0-5*-*4 will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 5 Typical failure mode distributions for thermocouples

TC Failure Modes – Device with extension wires	Percentage
Open Circuit (Burn-out)	90%
Wire Short (Temperature measurement in error)	5%
Drift (Temperature measurement in error)	5%

A complete temperature sensor assembly consisting of the Temperature Transmitter Type 9182/*0-5*-*4 and a thermocouple with extension wires supplied with the Temperature Transmitter Type 9182/*0-5*-*4 can be modeled by considering a series subsystem where failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the Temperature Transmitter Type 9182/*0-5*-*4 is programmed to drive its output to the specified failure state on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

λ^{DD} = 1000 FIT * 90% = 900 FIT
λ^{DU} = 1000 FIT * 10% = 100 FIT

The total failure rate for the temperature sensor assembly with the Temperature Transmitter Type 9182/*0-5*-*4 with one contact output is:

λ^{SD} = 0 FIT
λ^{SU} = 299 FIT
λ^{DD} = 900 FIT + 232 FIT = 1132 FIT
λ^{DU} = 100 FIT + 146 FIT = 246 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. For these circumstances, the Safe Failure Fraction of this temperature sensor assembly is 85%.

5.1.2 Temperature Transmitter Type 9182/*0-5*-*4 with 4-wire RTD

The failure mode distribution for an RTD also depends on the application with 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. Typical failure rate distributions are shown in Table 17. The Temperature Transmitter Type 9182/*0-5*-*4 will detect open circuit and short circuit RTD failures and drive its output to the alarm state on detected failures of the RTD.

Table 6 Failure mode distribution for 4-wire RTD, low stress environment

RTD Failure Modes – Device with extension wires	Percentage
Open Circuit	82%
Short Circuit	4%
Drift (Temperature measurement in error)	14%

A complete temperature sensor assembly consisting of the Temperature Transmitter Type 9182/*0-5*-*4 and a 4-wire RTD with extension wires supplied with the Temperature Transmitter Type 9182/*0-5*-*4 can be modeled by considering a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Assuming that the Temperature Transmitter Type 9182/*0-5*-*4 is programmed to drive its output to the alarm state on detected failures of the RTD, the failure rate contribution for a 4-wire RTD with extension wires in a low stress environment is:

λ^{DD} = 500 FIT * (82% + 4%) = 430 FIT
λ^{DU} = 500 FIT * 14% = 70 FIT

The total failure rate for the temperature sensor assembly with the Temperature Transmitter Type 9182/*0-5*-*4 with one contact output is:

λ^{SD} = 0 FIT
λ^{SU} = 299 FIT
λ^{DD} = 430 FIT + 232 FIT = 662 FIT
λ^{DU} = 70 FIT + 146 FIT = 216 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature subsystem, given the assumptions, is 81%.

5.2 Example PFD_{AVG} calculation

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).

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) Temperature Transmitter Type 9182/*0-5*-*4 considering a proof test coverage of 99% (see Appendix 1.2) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 4.4.1. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 7.

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

Table 7: PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
One contact output	PFD_{AVG} = 7.03E-04	PFD_{AVG} = 1.34E-03	PFD_{AVG} = 3.23E-03
Two contact outputs in series	PFD_{AVG} = 6.17E-04	PFD_{AVG} = 1.17E-03	PFD_{AVG} = 2.84E-03

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval considering profile 1 data is approximately equal to 7% of the range.

Figure 2 shows PFD_{AVG} as a function of the proof test interval.

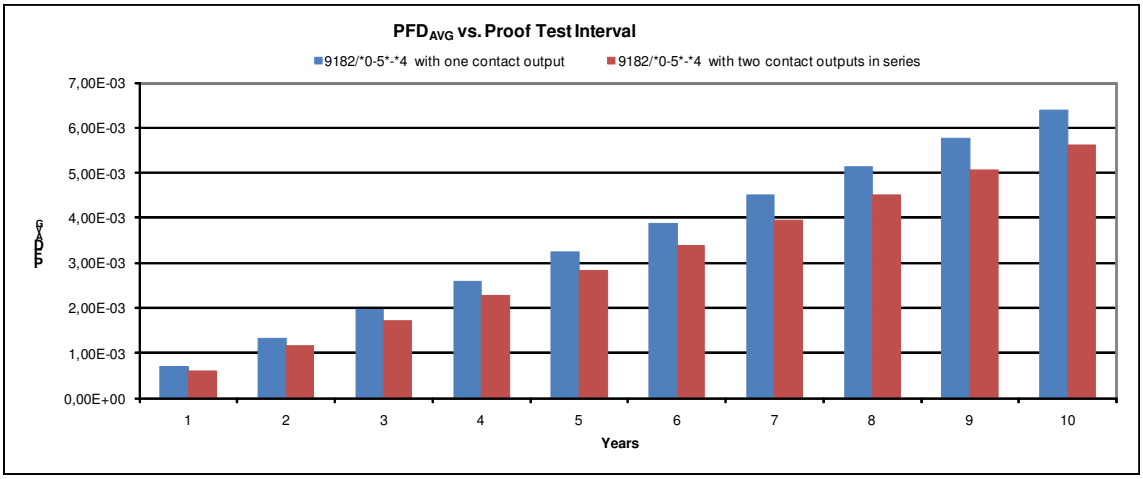


Figure 2: $PFD_{AVG}(t)$

6 *exida* Proven-in-use Assessment

6.1 Supplemental information to assist in prior-use justification

According to IEC 61511-1 First Edition 2003-01 section 11.4.4 for all subsystems (e.g., sensor, final elements and non-PE logic solvers) except PE logic solvers the minimum fault tolerance specified in Table 6 of this standard may be reduced by one if the devices under consideration comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3)
- the device allows adjustment of process-related parameters only, e.g., measuring range, upscale or downscale failure direction, etc.;
- the adjustment of the process-related parameters of the device is protected, e.g., jumper, password;
- the function has a SIL requirement less than 4.

The following information can be used to assist an end user with prior-use justification of the Temperature Transmitter Type 9182/*0-5*-*4.

Requirement	**Argumentation**
Prove of quality management and operating experience	1. R. STAHL Schaltgeräte GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D24] to [D30]. The assessed subsystem is clearly identified and specified. The field feedback tracking database of R. STAHL Schaltgeräte GmbH together with the explanations given in [D10] to [D11] provide evidence that the field failures are used as design feedback. 2. Operating experience of the Temperature Transmitter Type 9182/10-51-*4 exists of more than 31.000.000 operating hours for devices with hardware version Rev. B and software version V01-04 to V01-09. The software modifications (see [D12] to [D23]) were carried out in accordance with a SIL 2 compliant modification process.
Adjustment of process-related parameters only	The device only allows the adjustment of process-related parameters.
Adjustment of process-related parameters is protected	The adjustment of process-related parameters is protected as an external device with special software and cable has to be connected to change the parameterization.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Temperature Transmitter Type 9182/*0-5*-*4 with a SFF of < 90% and a HFT = 0 can considered to be a proven-in-use device and therefore might also be used for a SIL 2 safety function according to IEC 61511-1 First Edition 2003-01.

7 Terms and Definitions

DC_D	Diagnostic Coverage of dangerous failures
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.
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

8 Status of the document

8.1 Liability

exida prepares 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.

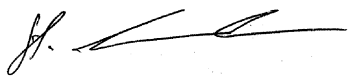
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market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

8.2 Releases

Version History:	V2R1:	Editorial changes; January 29, 2010
	V2R0:	Proven-in-use investigation and additional devices added; January 28, 2010
	V1R0:	Review comments incorporated; January 8, 2009
	V0R1:	Initial version; December 11, 2008
Author:	Stephan Aschenbrenner	
Review:	V0R1:	Andreas Bagusch (R. STAHL); January 8, 2008
	V0R1:	Rachel Amkreutz (*exida*); January 6, 2009
Release status:	Released to R. STAHL Schaltgeräte GmbH	

8.3 Release Signatures



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

Rachel Amkreutz, Safety Engineer

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 8 shows an importance analysis according to the ***exida*** database (profile 1) of the ten most critical dangerous undetected faults and indicate 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 8: Importance Analysis for 9182/*0-5*-*4 with one contact output

Component	% of total λ_{du}	Detection through
I302-D	22,61%	100% functional test with different input signals and monitoring of the output signals
O106, O107	13,99%	100% functional test with different input signals and monitoring of the output signals
I303	9,30%	100% functional test with different input signals and monitoring of the output signals
I309	8,60%	100% functional test with different input signals and monitoring of the output signals
I308-A	4,76%	100% functional test with different input signals and monitoring of the output signals
I306-CPU	3,79%	100% functional test with different input signals and monitoring of the output signals
I101-CPU	3,79%	100% functional test with different input signals and monitoring of the output signals
I107	3,72%	100% functional test with different input signals and monitoring of the output signals
I301-D	3,43%	100% functional test with different input signals and monitoring of the output signals
Q302	2,84%	100% functional test with different input signals and monitoring of the output signals

Table 9: Importance Analysis for 9182/*0-5*-*4 with two contact outputs in series

Component	% of total λ_{du}	Detection through
I302-D	26,07%	100% functional test with different input signals and monitoring of the output signals
I303	10,73%	100% functional test with different input signals and monitoring of the output signals
I309	9,92%	100% functional test with different input signals and monitoring of the output signals
I308-A	5,49%	100% functional test with different input signals and monitoring of the output signals
I306-CPU	4,37%	100% functional test with different input signals and monitoring of the output signals
I101-CPU	4,37%	100% functional test with different input signals and monitoring of the output signals
I107	4,29%	100% functional test with different input signals and monitoring of the output signals
I301-D	3,96%	100% functional test with different input signals and monitoring of the output signals
Q302	3,28%	100% functional test with different input signals and monitoring of the output signals
I304	2,76%	100% functional test with different input signals and monitoring of the output signals

Appendix 1.2: Proof test to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 10.

Table 10 Steps for a possible proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Force the Temperature Transmitter Type 9182/*0-5*-*4 to reach several defined “MAX” threshold value over the entire range and verify that the output goes into the safe state.
3	Force the Temperature Transmitter Type 9182/*0-5*-*4 to reach several defined “MIN” threshold value over the entire range and verify that the output goes into the safe state.
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures of the Temperature Transmitter Type 9182/*0-5*-*4.

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 4.3) this only applies provided that the useful lifetime[7] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

The Temperature Transmitter Type 9182/*0-5*-*4 does not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation. Therefore there is no limiting factor to 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.

[7] 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

Appendix 3.1: *exida* electronic database

Profile	Profile according to IEC60654-1	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 to
Report No.: STAHL 07/07-23 R017
Version V2, Revision R1; January 2010

Project:

Temperature Transmitter Type 9182/*0-5*-*4
(contact output)

Customer:

R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Jan Hettenbach

Appendix 4: Failure rates according to IEC 61508:2010

Table 1: Failure rates for 9182/*0-5*-*4 with contact output

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**150**
Fail Dangerous Detected (λ_{DD})	**232**
Fail Dangerous Detected (λ_{DD})	232
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**145**
Fail Annunciation Undetected (λ_{AU})	20
No effect	130
No part	323
Total failure rate (safety function)	**527**
SFF [1]	**72%**
SIL AC [2]	**SIL2**

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

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

Table 2: Failure rates for 9182/*0-5*-*4 with two contact outputs in series

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**150**
Fail Dangerous Detected (λ_{DD})	**241**
Fail Dangerous Detected (λ_{DD})	241
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**126**
Fail Annunciation Undetected (λ_{AU})	30
No effect	130
No part	323
Total failure rate (safety function)	**517**
SFF [3]	**75%**
SIL AC [4]	**SIL2**

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

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

Table 3: PFD_{AVG} Values

Configuration	T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 5 years	T[Proof] = 10 years
one contact output	PFD_{AVG} = 1,14E-03	PFD_{AVG} = 2,22E-03	PFD_{AVG} = 3,30E-03	PFD_{AVG} = 5,99E-03
two contact outputs in series	PFD_{AVG} = 9,72E-04	PFD_{AVG} = 1,89E-03	PFD_{AVG} = 2,80E-03	PFD_{AVG} = 5,09E-03

The listed PFD_{AVG} values are calculated for a proof test coverage of 90%.

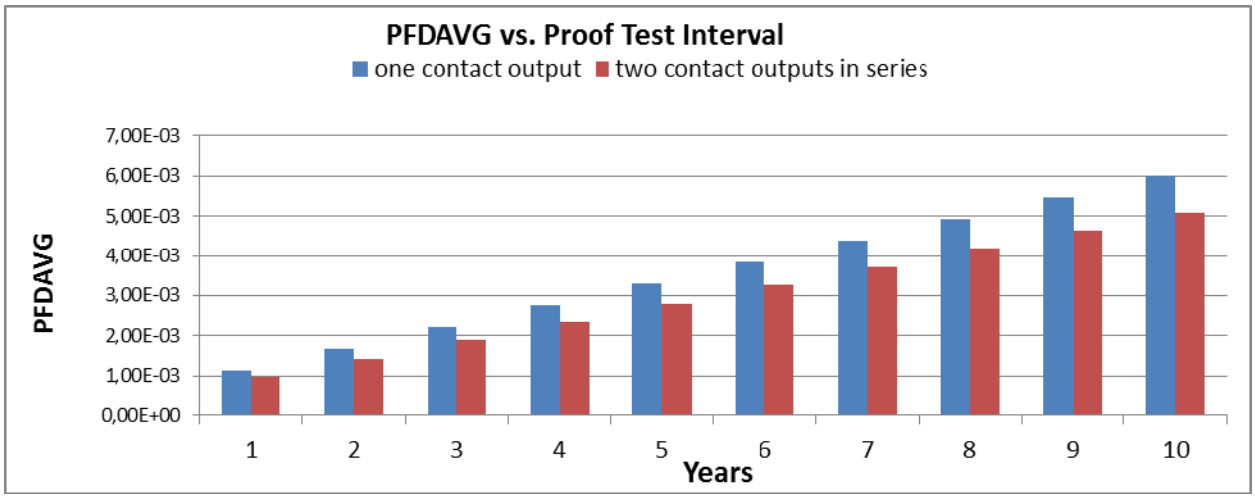


Figure 1: PFD_{AVG} (t)