



Failure Modes, Effects and Diagnostic Analysis

Project:

Loop Powered Isolating Repeater 9167

Customer:

R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 04/04-03

Report No.: STAHL 04/04-03 R005

Version V2, Revision R1, November 2008

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the Loop Powered Isolating Repeater 9167 revision Rev. A. Table 1 gives an overview of the different configurations that belong to the considered Loop Powered Isolating Repeater 9167.

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: Configuration overview

9167/11-11-00	1 channel	15.7 V, 60 mA, 233 mW, 360 Ω	I.S. ¹ output
9167/13-11-00	1 channel	25 V, 99 mA, 613 mW, 800 Ω	I.S. output
9167/13-11-50	1 channel	25 V, 99 mA, 613 mW, 800 Ω	non I.S. output
9167/23-11-50	2 channels	25 V, 99 mA, 613 mW, 800 Ω	non I.S. output
9167/14-11-00	1 channel	18.8 V, 107 mA, 503 mW, 590 Ω	I.S. output
9167/21-11-00	2 channels	15.7 V, 60 mA, 233 mW, 360 Ω	I.S. output
9167/23-11-00	2 channels	25 V, 99 mA, 613 mW, 800 Ω	I.S. output
9167/24-11-00	2 channels	18.8 V, 107 mA, 503 mW, 590 Ω	I.S. output

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

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $< 10^{-3}$ for SIL 3 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to 1,00E-04.

The Loop Powered Isolating Repeater 9167 is considered to be a Type A² subsystem with a hardware fault tolerance of 0.

For Type A subsystems the SFF has to be $> 90\%$ according to table 2 of IEC 61508-2 for SIL 3 subsystems with a hardware fault tolerance of 0.

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

¹ I.S. Intrinsic Safety

² Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

Failure rates according to IEC 61508

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
94 FIT	3 FIT	97%

PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,17E-05	PFD_{AVG} = 5,87E-05	PFD_{AVG} = 1,17E-04

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04.

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

A user of the Loop Powered Isolating Repeater 9167 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 along with all assumptions.

The failure rates are valid for the useful life of the Loop Powered Isolating Repeater 9167, which is estimated to be between 8 and 12 years (see Appendix 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.



Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved.....	6
2.3 Standards / Literature used.....	6
2.4 Reference documents.....	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida</i>	7
3 Description of the analyzed module	8
3.1 Loop Powered Isolating Repeater 9167.....	8
4 Failure Modes, Effects, and Diagnostic Analysis	9
4.1 Description of the failure categories.....	9
4.2 Methodology – FMEDA, Failure rates	9
4.2.1 FMEDA.....	10
4.2.2 Failure rates	10
4.2.3 Assumption	10
5 Results of the assessment.....	11
5.1 Loop Powered Isolating Repeater 9167.....	12
6 Terms and Definitions	14
7 Status of the document.....	15
7.1 Liability.....	15
7.2 Releases	15
7.3 Release Signatures.....	15
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	16
Appendix 1.1: Possible proof tests to detect dangerous undetected faults.....	17
Appendix 2: Impact of lifetime of critical components on the failure rate	18

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 EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). 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 EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option 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 1.

This document shall describe the results of the hardware assessment carried out on the Loop Powered Isolating Repeater 9167 revision Rev. A. Table 1 gives an overview of the different configurations that belong to the considered Loop Powered Isolating Repeater 9167.

It shall be assessed whether the Loop Powered Isolating Repeater 9167 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 3 sub-systems according to 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 Loop Powered Isolating Repeater 9167.

exida Performed the hardware assessment according to option 1 (see section 1).

R. STAHL Schaltgeräte GmbH contracted *exida* in May 2004 with 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]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	91 676 01 20 0_02_20041109.pdf	Circuit diagram „Trennübertrager/Isolating Repeater Typ 9167/..-11-00“ 91 676 01 20 0 Index 02 of 09.11.04
[D2]	Stueli 9167_02_20041109.xls	Parts list for Loop Powered Isolating Repeater 9167
[D3]	Email of 29.06.04	Information about the base material used
[D4]	B9167_de_en.doc	Operating instructions S-BA-9167-00-de/en-01/2004 - Entwurf 1
[D5]	FMEDA V5 9167 V1 R2.0.xls of 06.10.08	

2.4.2 Documentation generated by exida

[R1]	FMEDA V5 9167 V1 R1.0.xls of 09.07.04	
------	---------------------------------------	--

3 Description of the analyzed module

3.1 Loop Powered Isolating Repeater 9167

The Loop Powered Isolating Repeater 9167 is used for the operation of control valves, I/P converters, analog or digital indicators and fire & gas detectors.

The device can transfer bi-directionally a superimposed HART communication signal.

The Loop Powered Isolating Repeater 9167 is considered to be a Type A subsystem with a hardware fault tolerance of 0.

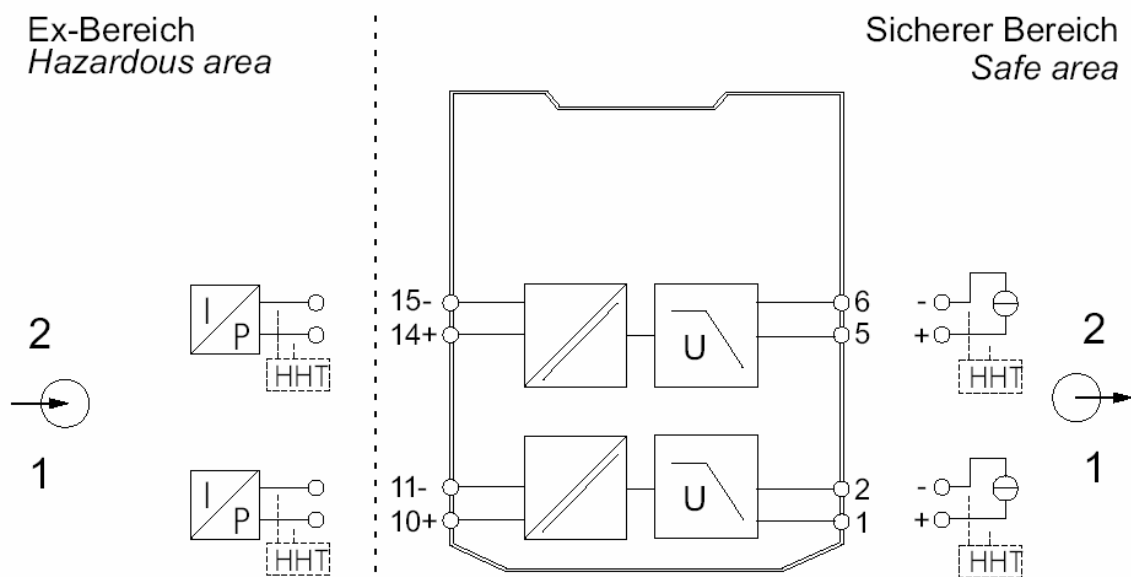


Figure 1: Block diagram of the Loop Powered Isolating Repeater 9167

Figure 1 is representative for all Loop Powered Isolating Repeater 9167 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 [D5].

4.1 Description of the failure categories

In order to judge the failure behavior of the Loop Powered Isolating Repeater 9167, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output going to "fail-low".
Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process or has no effect on the safety function.
Fail Dangerous	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 scale (+/-0.32mA).
Fail High	Failure that causes the output signal to go to the maximum output current (> 20.5 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.8 mA)
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output current by not more than 2% full scale. For the calculation of the SFF it is treated like a safe undetected failure.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The "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" and "Annunciation Undetected" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates are considered to be appropriate for safety integrity level verification calculations. The rates match operating stress conditions typical of an industrial field environment similar to IEC 60645-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.2.3 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Loop Powered Isolating Repeater 9167.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not during normal operation.
- For safety applications only the 4..20 mA output is considered.
- Only one input and one output are part of the safety function.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HDBK-217F. Alternatively, the assumed environment is similar to:
 - IEC 60645-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.

5 Results of the assessment

exida did the FMEDAs together with R. STAHL Schaltgeräte GmbH.

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

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

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous}$$

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

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

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1 system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

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

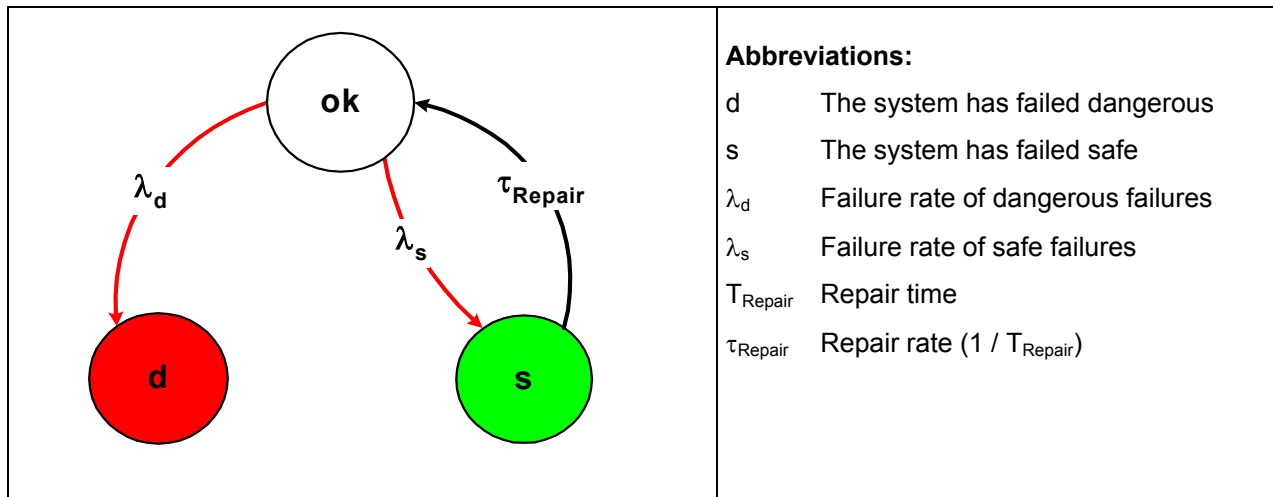


Figure 2: Markov model for a 1oo1 architecture

5.1 Loop Powered Isolating Repeater 9167

The FMEDA carried out on the Loop Powered Isolating Repeater 9167 leads under the assumptions described in section 4.2.3 to the following failure rates:

$$\lambda_{\text{safe}} = \lambda_{\text{low}} = 4,34\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = \lambda_{\text{dangerous}} + \lambda_{\text{high}} = 2,68\text{E-}09 \text{ 1/h} + 0,00\text{E-}00 \text{ 1/h} = 2,68\text{E-}09 \text{ 1/h}$$

$$\lambda_{\text{annunciation}} = 1,66\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{no effect}} = 3,36\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{total}} = 9,62\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 1,58\text{E-}08 \text{ 1/h}$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = 1 / (\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 1019 \text{ years}$$

Under the assumptions described in section 5 the following tables show the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{\text{dangerous}}$	SFF
94 FIT	3 FIT	97%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 1,17\text{E-}05$	$\text{PFD}_{\text{AVG}} = 5,87\text{E-}05$	$\text{PFD}_{\text{AVG}} = 1,17\text{E-}04$

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00\text{E-}04$. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00\text{E-}04$. Figure 3 shows the time dependent curve of PFD_{AVG} .

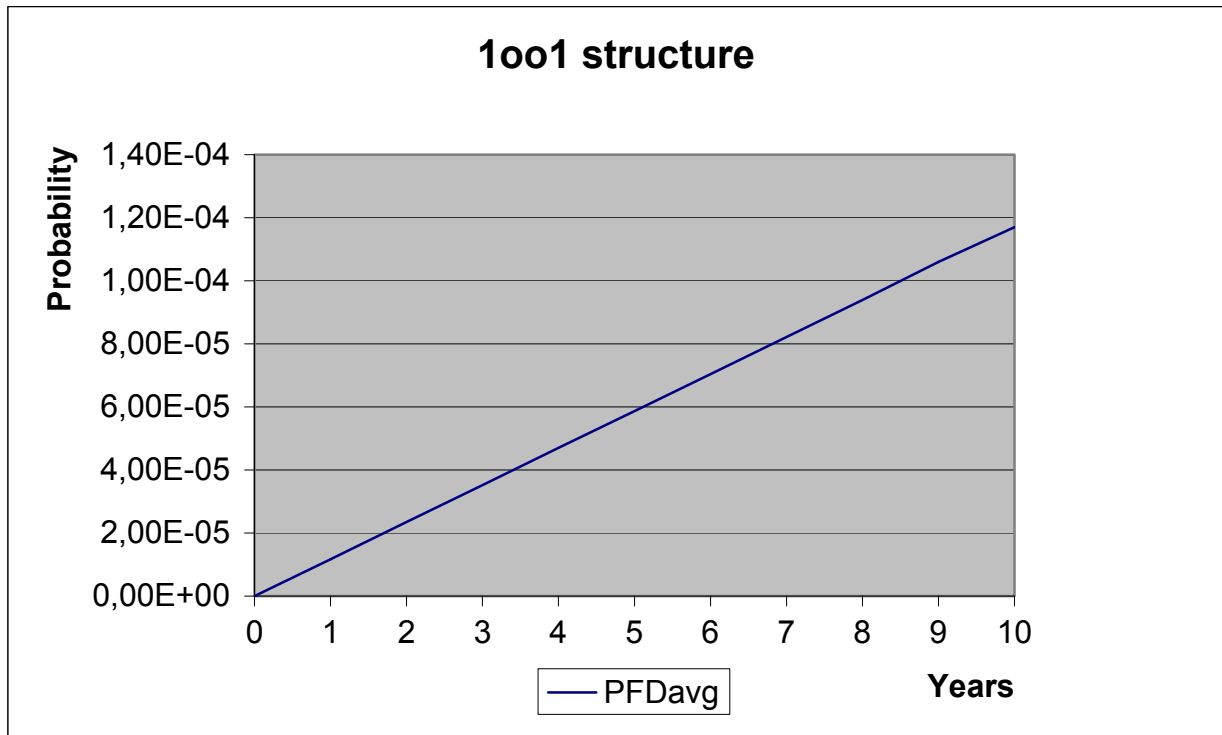


Figure 3: PFD_{AVG}(t)

6 Terms and Definitions

FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{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 A subsystem	“Non-complex” subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

7 Status of the document

7.1 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.

7.2 Releases

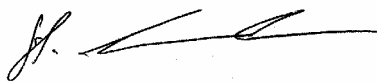
Version History: V2R1: Editorial changes; November 7, 2008
V2R0: Non I.S. devices added, editorial changes; November 5, 2008
V1, R1.0: Review comments integrated; August 6, 2004
V0, R1.0: Initial version; July 9, 2004

Authors: Stephan Aschenbrenner

Review: V2R0: Andreas Bagusch (R. STAHL); November 6, 2008
V0, R1.0: Rachel Amkreutz (*exida*); July 20, 2004

Release status: Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures

A handwritten signature in black ink, appearing to be "S. Aschenbrenner".

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

A handwritten signature in black ink, appearing to be "R. Faller".

Dipl.-Ing. (Univ.) Rainer Faller, Principal Partner

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 2 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 2: Importance analysis of dangerous undetected faults

Component	% of total λ_{du}	Detection through
W51A	22,39%	100% functional test with different expected output signals over the entire range
W52A	22,39%	100% functional test with different expected output signals over the entire range
C57A	11,20%	100% functional test with different expected output signals over the entire range
C59A	11,20%	100% functional test with different expected output signals over the entire range
D53A	11,20%	100% functional test with different expected output signals over the entire range
D54A	11,20%	100% functional test with different expected output signals over the entire range
R01A	5,22%	100% functional test with different expected output signals over the entire range
R07A	5,22%	100% functional test with different expected output signals over the entire range

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 3.

Table 3 Steps for Proof Test 1

Step	Action
1	Take appropriate action to avoid a false trip
2	Provide a 4mA control signal to the Loop Powered Isolating Repeater 9167 to open/close the driven output and verify that the driven output is open/closed. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures. It requires, however, that the driven output has already been tested without the repeater and does not contain any dangerous undetected faults anymore.
3	Restore the loop to full operation
4	Restore normal operation

This test will detect approximately 70% of possible “du” failures in the Loop Powered Isolating Repeater 9167.

Proof test 2 consists of the following steps, as described in Table 4.

Table 4 Steps for Proof Test 2

Step	Action
1	Take appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Provide a 4..20 mA control signal in steps of 1 mA to the Loop Powered Isolating Repeater 9167 to open/close the driven output and verify that the driven output opens/closes accordingly. This requires that the driven output has already been tested without the repeater and does not contain any dangerous undetected faults anymore.
4	Restore the loop to full operation
5	Restore normal operation

This test will detect approximately 95% of possible “du” failures in the Loop Powered Isolating Repeater 9167.

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

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

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components 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 circuit of the Loop Powered Isolating Repeater 9167 does not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

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