



Failure Modes, Effects and Diagnostic Analysis

Project:
Digital Output Type 9175

Company:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 07/10-01
Report No.: STAHL 07/10-01 R012
Version V3, Revision R1, March 2011
Stephan Aschenbrenner

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Digital Output Type 9175, Revision B. Table 1 gives an overview of the different variants that belong to the Digital Output Type 9175. The FMEDA was done by the customer R. STAHL Schaltgeräte GmbH and reviewed by *exida*.

A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Digital Output Type 9175. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

Devices of the Digital Output Type 9175 are used for intrinsically safe operation of solenoid valves, LED signal lights etc. The variant 9175/10-1*-12 LFT (Line Fault Transparent) reports a detected line fault to the control equipment via the signal channel itself.

Table 1 gives an overview of the different variants that were considered in the FMEDA of the Digital Output Type 9175.

Table 1: Variant Overview

Type	No-load voltage U_A	Max. output current $I_{A \max}$	Internal resistance R_i
9175/a0-12-11	10 V	60 mA / 120 mA ^{*)}	150 Ω / 75 Ω ^{*)}
9175/a0-14-11	17,5 V	45 mA / 90 mA ^{*)}	130 Ω / 65 Ω ^{*)}
9175/a0-16-11	25 V	35 mA / 70 mA ^{*)}	250 Ω / 125 Ω ^{*)}
9175/10-12-12	10 V	60 mA	150 Ω
9175/10-14-12	17,5 V	45 mA	130 Ω
9175/10-16-12	25 V	35 mA	250 Ω

a = 1, one channel variant; a = 2, two channel variant
^{*)} By two channel variant parallel connection of the outputs possible (doubling of the output current).

For safety applications only the described variants were considered. All other possible output variants or electronics are not covered by this report. Lead breakage detection and short circuit detection can be activated or de-activated.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1 (for details see Appendix C). The analysis has 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 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 Digital Output Type 9175 is classified as a Type A¹ element according to IEC 61508, having a hardware fault tolerance of 0. The worst-case failure rates according to IEC 61508:2010 for the Digital Output Type 9175 are listed in the following tables.

¹ Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Table 2: Digital Output Type 9175/10-1*-12

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	210
Fail Dangerous Detected	0
Fail Dangerous Undetected	14
No Effect	335
No part	132
SFF ²	93%
SIL AC ³	SIL 3

Table 3: Digital Output Type 9175/a0-1*-11

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	166
Fail Dangerous Detected	0
Fail Dangerous Undetected	9
No Effect	243
No part	212
SFF ²	94%
SIL AC ³	SIL 3

Table 4: Digital Output Type 9175/20-1*-11 with parallel output connection

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	266
Fail Dangerous Detected	0
Fail Dangerous Undetected	18
No Effect	429
No part	417
SFF ²	93%
SIL AC ³	SIL 3

² The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³ 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. The complete final element subsystem will need to be taken into account when determining the corresponding SIL.



At type 9175/*0-1*-11 the control input cannot supply the output. In case of a missing power supply the outputs are de-energized. Type 9175/10-1*-12 is different. At this type the outputs are also supplied via the control input.

These failure rates are valid for the useful lifetime of the Digital Output Type 9175, see Appendix B.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

A user of the Digital Output Type 9175 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 4.3 along with all assumptions.

Table of Contents

Management Summary	2
1 Purpose and Scope.....	6
2 Project Management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards and Literature used	7
2.4 Reference documents	8
2.4.1 Documentation provided by R. STAHL Schaltgeräte GmbH	8
2.4.2 Documentation generated by <i>exida</i>	8
3 Product Description.....	9
4 Failure Modes, Effects, and Diagnostic Analysis.....	10
4.1 Description of the failure categories	10
4.2 Methodology – FMEDA, Failure Rates	11
4.2.1 FMEDA	11
4.2.2 Failure Rates	11
4.2.3 Assumptions	12
4.3 Results.....	12
4.3.1 Digital Output Type 9175.....	13
5 Using the FMEDA Results	15
5.1 Example PFD _{AVG} calculation.....	15
6 Terms and Definitions	16
7 Status of the Document.....	17
7.1 Liability.....	17
7.2 Releases.....	17
7.3 Release Signatures	17
Appendix A: Possibilities to reveal dangerous undetected faults during the proof test..	18
Appendix A.1: Possible proof tests to detect dangerous undetected faults	18
Appendix B: Lifetime of Critical Components.....	19
Appendix C: Description of the considered profiles	20
Appendix C.1: <i>exida</i> electronic database	20

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 per 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 1.

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Digital Output Type 9175. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a final element subsystem, including the Digital Output Type 9175 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 product certification and 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, detailed 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 Digital Output Type 9175.

exida Reviewed the provided FMEDA and issued this report according to Option 1 (see Section 1).

R. STAHL Schaltgeräte GmbH contracted *exida* in December 2010 to review the provided FMEDA and issue the report.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; 2nd edition
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	<i>exida</i> 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 R. STAHL Schaltgeräte GmbH

[D1]	91 756 02 20 0_00.pdf	Circuit diagram "Binary Output Typ 9175/10-1.-12" 91 756 02 20 0; of 18.01.08
[D2]	B9175_de_en_einreichung 2008.pdf	Instruction Manual / Safety Manual; Date: Feb. 2008
[D3]	Bauteile 9175 SIL.xls	Bill of Material of 17.07.07
[D4]	91 756 01 20 0_04_20060926.pdf	Circuit diagram "Binary Output Typ 9175/.0-1.-11" 91 756 01 20 0; version 04 of 26.09.06
[D5]	STL_9175_x0-1x-11-20101214.xlsx	Bill of Material of 14.12.10
[D6]	Useful lifetime 9175.pdf	Useful lifetime evaluation of 15.12.10
[D7]	FMEDA V 6_5_7_9175-11_V1R2.xls	Failure Modes, Effects, and Diagnostic Analysis – Digital Output Type 9175/a0-1*-11 of 09.02.11
[D8]	9175_x0-1x-11_NeuBew_C.docx	Description of changes "Binärausgabe Typ 9175/**-**-11 Neubewertung" of 15.03.11
[D9]	FMEDA V 6_5_7_9175-11_V3R1.xls	Failure Modes, Effects, and Diagnostic Analysis – Digital Output Type 9175/10-1*-12 of 14.03.11

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V 6_5_7_9175-11_parallel_V1R2.xls	Failure Modes, Effects, and Diagnostic Analysis – Digital Output Type 9175/a0-1*-11 of 10.02.11
------	---	---

3 Product Description

Digital Output Type 9175 are used for intrinsically safe operation of solenoid valves, LED signal lights etc. The version LFT (Line Fault Transparent) reports a detected line fault to the control equipment via the signal channel itself.

The FMEDA was done on the Digital Output Type 9175 as shown in the blue shaded area of Figure 1. There were no connected parts like valves etc., neither in the safe nor in the hazardous area, used in the FMEDA.

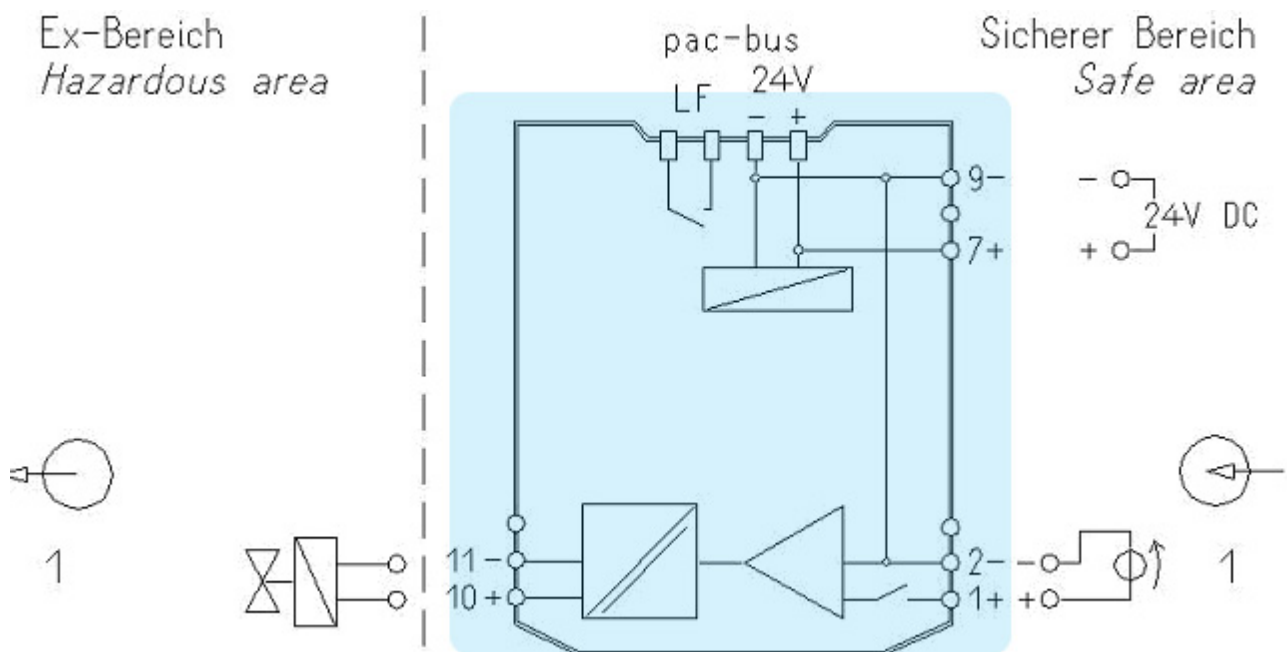


Figure 1: Digital Output Type 9175/10-1*-12

Figure 1 is representative for all Digital Output Type 9175 listed in Table 5.

Table 5 gives an overview of the different variants that were considered in the FMEDA of the Digital Output Type 9175. The Digital Output Type 9175 is classified as a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

Table 5: Variant Overview

Type	No-load voltage U_A	Max. output current $I_{A \max}$	Internal resistance R_i
9175/a0-12-11	10 V	60 mA / 120 mA ^{*)}	150 Ω / 75 Ω ^{*)}
9175/a0-14-11	17,5 V	45 mA / 90 mA ^{*)}	130 Ω / 65 Ω ^{*)}
9175/a0-16-11	25 V	35 mA / 70 mA ^{*)}	250 Ω / 125 Ω ^{*)}
9175/10-12-12	10 V	60 mA	150 Ω
9175/10-14-12	17,5 V	45 mA	130 Ω
9175/10-16-12	25 V	35 mA	250 Ω

a = 1, one channel variant; a = 2, two channel variant
^{*)} By two channel variant parallel connection of the outputs possible (doubling of the output current).

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented in [D7] and [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the Digital Output Type 9175, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized or the output current is less than 3mA.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
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.
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. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.
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.

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 Digital Output Type 9175.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- 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.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- For safety applications only the described variants are considered.
- Short circuit and lead breakage detection are either activated or de-activated.

4.3 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:

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

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

$$\text{DC}_D = \lambda_{\text{DD}} / (\lambda_{\text{DD}} + \lambda_{\text{DU}})$$

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

4.3.1 Digital Output Type 9175

Table 6: Digital Output Type 9175/10-1*-12

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	210
Fail Dangerous Detected	0
Fail Dangerous Undetected	14
No Effect	335
No part	132

SFF ⁴	93%
SIL AC ⁵	SIL 3

Table 7: Digital Output Type 9175/a0-1*-11

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	166
Fail Dangerous Detected	0
Fail Dangerous Undetected	9
No Effect	243
No part	212

SFF ⁶	94%
SIL AC ⁷	SIL 3

⁴ The complete final element 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. The complete final element subsystem will need to be taken into account when determining the corresponding SIL.

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

⁷ 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. The complete final element subsystem will need to be taken into account when determining the corresponding SIL.

Table 8: Digital Output Type 9175/20-1*-11 with parallel output connection

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	266
Fail Dangerous Detected	0
Fail Dangerous Undetected	18
No Effect	429
No part	417
SFF ²	93%
SIL AC ³	SIL 3

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

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 (1oo1D) Digital Output Type 9175 considering a proof test coverage of 99% (see Appendix A.1) and a mission time of 10 years. The failure rate data used in this calculation is displayed in section 4.3. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 9.

For SIL 3 applications, the PFD_{AVG} value needs to be $< 1.00E-03$.

Table 9: PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
9175/10-1*-12	$PFD_{AVG} = 6.50E-05$	$PFD_{AVG} = 1.24E-04$	$PFD_{AVG} = 3.01E-04$
9175/a0-1*-11 (single)	$PFD_{AVG} = 4.25E-05$	$PFD_{AVG} = 8.12E-05$	$PFD_{AVG} = 1.97E-04$
9175/a0-1*-11 (parallel)	$PFD_{AVG} = 8.39E-05$	$PFD_{AVG} = 1.60E-04$	$PFD_{AVG} = 3.89E-04$

For the Digital Output Type 9175 this means that for a SIL3 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 7% of the range considering the single output and approximately equal to 8% of the range considering the parallel output.

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

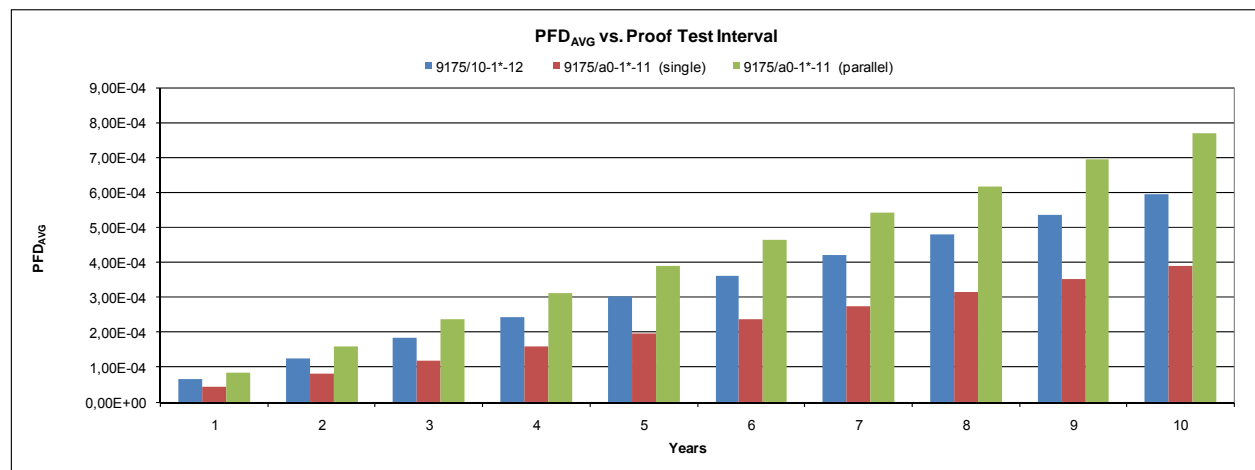


Figure 2: $PFD_{AVG}(t)$

6 Terms and Definitions

FIT	Failure In Time (1x10 ⁻⁹ failures per hour)
FMEDA	Failure Mode Effect 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 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
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

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: V3R1: Editorial changes; March 24, 2011
V3R0: Additional variants added; February 10, 2011
V2R0: Changes because of activation or de-activation of short circuit and lead breakage detection; Stephan Aschenbrenner; 13. March 2009
V1, R0: Review comments incorporated, Philipp Neumeier, 8. Aug. 2008
V0, R4: Review comments incorporated, Philipp Neumeier, 25. July 2008
V0, R3: Updated, Philipp Neumeier, 16. July 2008
V0, R2: Review comments incorporated, Otto Walch, 14. July 2008
V0, R1: initial Version, Otto Walch

Author(s): Stephan Aschenbrenner, Philipp Neumeier

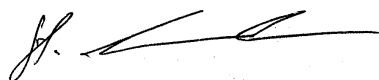
Review: V0, R3: Reviewed by Stephan Aschenbrenner; 17. July 2008
V0, R4: Reviewed by R. STAHL Schaltgeräte GmbH; 6. Aug. 2008

Release Status: Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures

A handwritten signature in blue ink, appearing to read "P. Neumeier".

Dipl.-Ing. (FH) Philipp Neumeier, Safety Engineer

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

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

Appendix A: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 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.

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

Appendix A.1: Possible proof tests to detect dangerous undetected faults

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

Table 10 Steps for Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Force the digital output 9175 to go to the safe state and verify that the safe state is reached.
3	Restore the loop to full operation.
4	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect more than 99% of possible “du” failures in the digital output 9175.

Appendix B: Lifetime of Critical Components

According to section 7.4.9.5 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 lifetime⁸ 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 subsystem itself and its operating conditions.

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

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

Table 11 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 11: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life
Opto-coupler	O20A, O20B	Approximately 10 years

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

⁸ 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 C: Description of the considered profiles

Appendix C.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.