



FMEDA and Proven-in-use Assessment

Project:

Solenoid Valve Drivers ED2-VM-Ex*.3**

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 03/3-25

Report No.: P+F 03/3-25 R011

Version V1, Revision R1.0, July 2003

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / FDIS IEC 61511 carried out on the Solenoid Valve Drivers ED2-VM-Ex*.3**. '*' and '**' stand for the different versions that are available.

Table 1 gives an overview and explains the differences.

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

Type	Channels	Input not isolated	Input isolated	Separate power
ED2-VM-Ex4.3*	4	X		X
ED2-VM-Ex2.3*	2	X		X
ED2-VM-Ex4.3*.O	4		X	X
ED2-VM-Ex2.3*.O	2		X	X

The “*” stands for several options regarding the output voltage and output current. Mostly used are “32” and “35”. The “O” stands for opto-coupler isolated inputs.

The failure rates used in this analysis are based on the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-4}$ to $< 10^{-3}$ for SIL 3 safety functions and $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 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 for SIL 3 and better than or equal to 1,00E-03 for SIL 2.

The Solenoid Valve Drivers ED2-VM-Ex*.3** are considered to be Type A¹ components having a hardware fault tolerance of 0.

For Type A components the SFF has to be between 90% and 99% for SIL 3 (sub-) systems and between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

As the Solenoid Valve Drivers ED2-VM-Ex*.3** are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the devices was carried out. According to the requirements of IEC 61511-1 FDIS Ed.1 27-09-02 section 11.4.4 and the assessment described in section 5.1 the devices are suitable to be used, as a single device, for SIL 2 safety functions.

The following table shows which boards (considering one input and one output being part of the safety function) fulfill this requirement.

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

1. Switch-off path via logic input

Table 2: Summary of all considered boards with regard to SIL 2 requirements – PFD_{AVG} values

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
ED2-VM-Ex4.3*	PFD _{AVG} = 2,72E-05	PFD _{AVG} = 1,36E-04	PFD _{AVG} = 2,72E-04
ED2-VM-Ex2.3*	PFD _{AVG} = 2,72E-05	PFD _{AVG} = 1,36E-04	PFD _{AVG} = 2,72E-04
ED2-VM-Ex4.3*.O	PFD _{AVG} = 5,08E-05	PFD _{AVG} = 2,54E-04	PFD _{AVG} = 5,07E-04
ED2-VM-Ex2.3*.O	PFD _{AVG} = 5,08E-05	PFD _{AVG} = 2,54E-04	PFD _{AVG} = 5,07E-04

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 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-03.

Table 3: Summary of all considered boards with regard to SIL 3 requirements – PFD_{AVG} values

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
ED2-VM-Ex4.3*	PFD _{AVG} = 2,72E-05	PFD _{AVG} = 1,36E-04	PFD _{AVG} = 2,72E-04
ED2-VM-Ex2.3*	PFD _{AVG} = 2,72E-05	PFD _{AVG} = 1,36E-04	PFD _{AVG} = 2,72E-04
ED2-VM-Ex4.3*.O	PFD _{AVG} = 5,08E-05	PFD _{AVG} = 2,54E-04	PFD _{AVG} = 5,07E-04
ED2-VM-Ex2.3*.O	PFD _{AVG} = 5,08E-05	PFD _{AVG} = 2,54E-04	PFD _{AVG} = 5,07E-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 table 3.1 of ANSI/ISA–84.01–1996 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.

Table 4: Summary of all considered boards – Failure rates

Name	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
ED2-VM-Ex4.3*	0,00E-00 1/h	1,53E-07 1/h	0,00E-00 1/h	6,22E-09 1/h	> 96 %
ED2-VM-Ex2.3*	0,00E-00 1/h	1,53E-07 1/h	0,00E-00 1/h	6,22E-09 1/h	> 96 %
ED2-VM-Ex4.3*.O	0,00E-00 1/h	1,62E-07 1/h	0,00E-00 1/h	1,16E-08 1/h	> 93 %
ED2-VM-Ex2.3*.O	0,00E-00 1/h	1,62E-07 1/h	0,00E-00 1/h	1,16E-08 1/h	> 93 %

2. Switch-off path via common power supply

Table 5: Summary of all considered boards with regard to SIL 3 requirements – PFD_{AVG} values

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
ED2-VM-Ex4.3*	PFD _{AVG} = 2,80E-06	PFD _{AVG} = 1,40E-05	PFD _{AVG} = 2,80E-05
ED2-VM-Ex2.3*	PFD _{AVG} = 2,80E-06	PFD _{AVG} = 1,40E-05	PFD _{AVG} = 2,80E-05
ED2-VM-Ex4.3*.O	PFD _{AVG} = 2,80E-06	PFD _{AVG} = 1,40E-05	PFD _{AVG} = 2,80E-05
ED2-VM-Ex2.3*.O	PFD _{AVG} = 2,80E-06	PFD _{AVG} = 1,40E-05	PFD _{AVG} = 2,80E-05

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 table 3.1 of ANSI/ISA–84.01–1996 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.

Table 6: Summary of all considered boards – Failure rates

Name	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
ED2-VM-Ex4.3*	0,00E-00 1/h	1,59E-07 1/h	0,00E-00 1/h	6,40E-10 1/h	> 99 %
ED2-VM-Ex2.3*	0,00E-00 1/h	1,59E-07 1/h	0,00E-00 1/h	6,40E-10 1/h	> 99 %
ED2-VM-Ex4.3*.O	0,00E-00 1/h	1,73E-07 1/h	0,00E-00 1/h	6,40E-10 1/h	> 99 %
ED2-VM-Ex2.3*.O	0,00E-00 1/h	1,73E-07 1/h	0,00E-00 1/h	6,40E-10 1/h	> 99 %

A user of the Solenoid Valve Drivers ED2-VM-Ex*.3** 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). The complete list of failure rates is presented in section 5.2 to 5.3 along with all assumptions.

Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida.com</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards / Literature used.....	7
2.4 Reference documents.....	8
2.4.1 Documentation provided by the customer.....	8
2.4.2 Documentation generated by <i>exida.com</i>	8
3 Description of the analyzed modules	9
4 Failure Modes, Effects, and Diagnostics 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 Assumption	11
5 Results of the assessment.....	12
5.1 Assessment of ED2-VM-Ex*.3**	13
5.2 ED2-VM-Ex4.3* - switch-off path via logic input	15
5.3 ED2-VM-Ex4.3*.O - switch-off path via logic input.....	16
5.4 ED2-VM-Ex4.3* - switch-off path via common power supply.....	17
5.5 ED2-VM-Ex4.3*.O - switch-off path via common power supply.....	18
6 Terms and Definitions	19
7 Status of the document.....	20
7.1 Liability.....	20
7.2 Releases	20
7.3 Release Signatures.....	20
Appendix 1: Prior use Proof according to IEC 61511-1 FDIS Ed.1 27-09-02	21
Appendix 1.1 Section 11.5.3 of IEC 61511-1 FDIS Ed.1 27-09-02.....	21
Appendix 1.2 Section 11.5.4 of IEC 61511-1 FDIS Ed.1 27-09-02.....	21
Appendix 1.3 Section 11.5.2 of IEC 61511-1 FDIS Ed.1 27-09-02.....	21
Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test.....	23
Appendix 3: Impact of lifetime of critical components on the failure rate.....	24

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.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not contain any software assessment.

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

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}). In addition this option consists of an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of draft 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.com* according to the relevant application standard(s) like draft IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, 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 is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 2.

This document shall describe the results of the assessment carried out on the Solenoid Valve Drivers ED2-VM-Ex*.3**.

It shall be assessed whether the solenoid valve drivers meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

Pepperl+Fuchs GmbH contracted *exida.com* in April 2003 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* 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.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl+Fuchs	Manufacturer of the Solenoid Valve Drivers ED2-VM-Ex*.3**.
<i>exida.com</i>	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	IEC 61511-1 FDIS Ed.1; 27-09-02	Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
[N3]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N4]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N5]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N6]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N7]	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	1-3247 Ind. B	Circuit diagram "Ex-Modul KM/V 030-036"
[D2]	1-3935 Ind. 0	Circuit diagram "ED2-VM-Ex4..."
[D3]	1-3413 Ind. A	Circuit diagram "ED2-VM-4.30.O ... ED2-VM-4.35.O"
[D4]	EG_ED.xls of 07.05.03	Field data evaluation (operating hours, sold devices, returned devices)
[D5]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D6]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D7]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D8]	Email of 18.06.03	Examples of applications

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V5 R0.1 VM logic input V1 R1.0.xls of 23.04.03
[R2]	FMEDA V5 R0.1 VM logic input with opto-coupler V1 R1.0.xls of 26.06.03
[R3]	FMEDA V5 R0.1 VM PS input V1 R1.0.xls of 18.05.03
[R4]	FMEDA V5 R0.1 VM PS input with opto-coupler V1 R1.0.xls of 26.06.03

3 Description of the analyzed modules

- Common or separate power supply for the 4 channels
- 1-logic input per channel for on / off switching
- Outputs galvanically isolated from the power supply and inputs

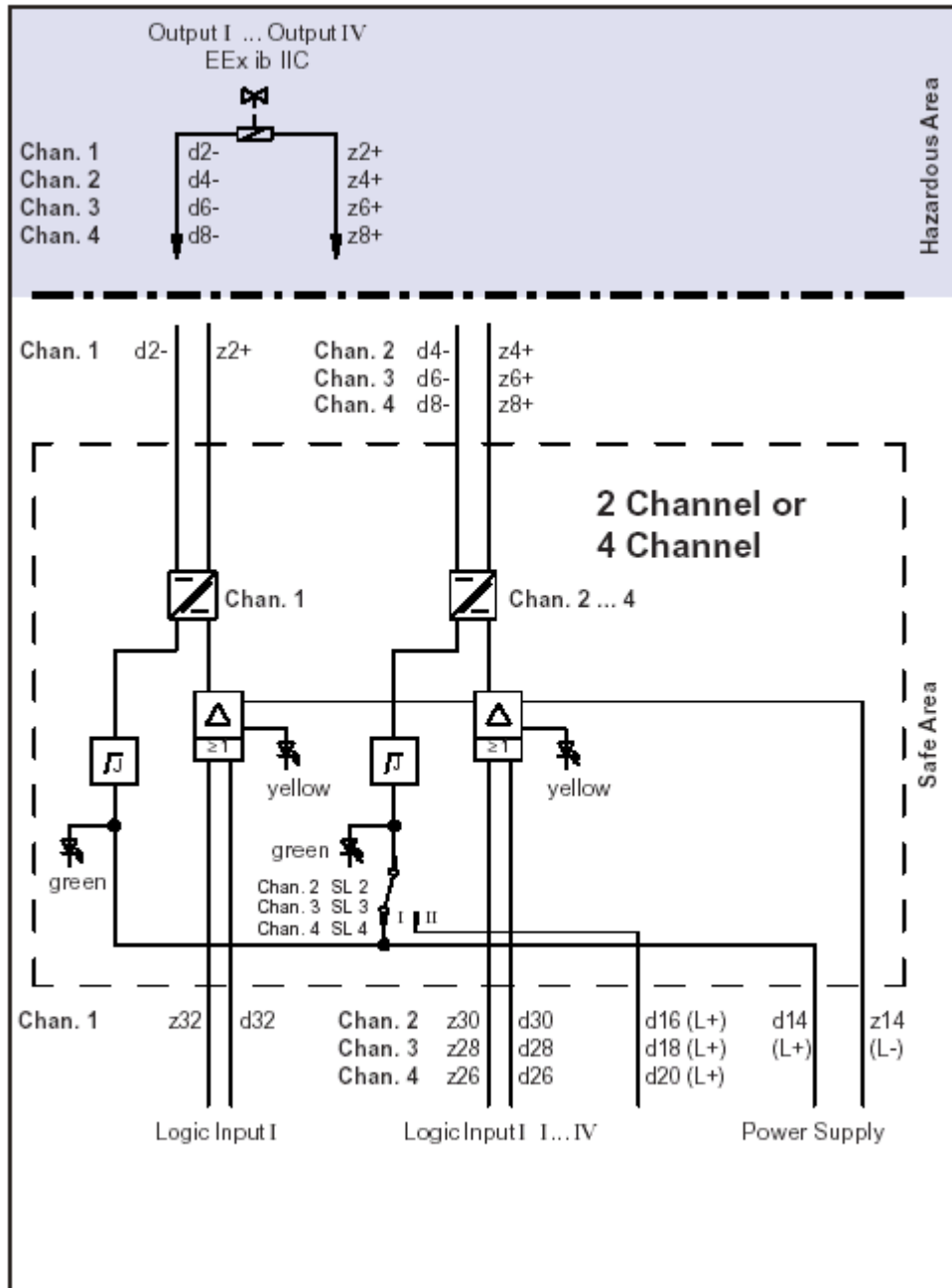


Figure 1: Block diagram of the solenoid valve drivers

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs and is documented in [R1] to [R4].

4.1 Description of the failure categories

The **fail-safe state** is defined as the output being de-energized.

Failures are categorized and defined as follows:

A **safe** failure (S) is defined as a failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.

A **dangerous undetected** failure (DU) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

A **dangerous detected** failure (DD) is defined as a failure that is dangerous but is detected by the device itself.

An annunciation failure (A) is defined as a 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). For the calculation of the SFF it is treated like a safe undetected failure.

A don't care failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function or deviates the output current by not more than 1% of the actual value. For the calculation of the SFF it is treated like a safe undetected failure.

"not part" (-) means that this component 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.

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.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an 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.com* in this FMEDA are from the Siemens SN 29500 failure rate database. 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 ISA 71.01 class D. 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 Solenoid Valve Drivers ED2-VM-Ex*.3**.

- Bridges SL2, SL3 and SL4 are wired in such a way that each channel is separately powered.
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The repair time after a safe failure is 8 hours.
- The test time to react on a dangerous detected failure is 1 hour.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment and can be compared to the Ground Benign classification.
- All modules are operated in the low demand mode of operation.

5 Results of the assessment

exida.com did the FMEDAs together with Pepperl+Fuchs.

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:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care} + \lambda_{annunciation}$$

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

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 1oo1D 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.com as a simulation tool. The results are documented in the following sections.

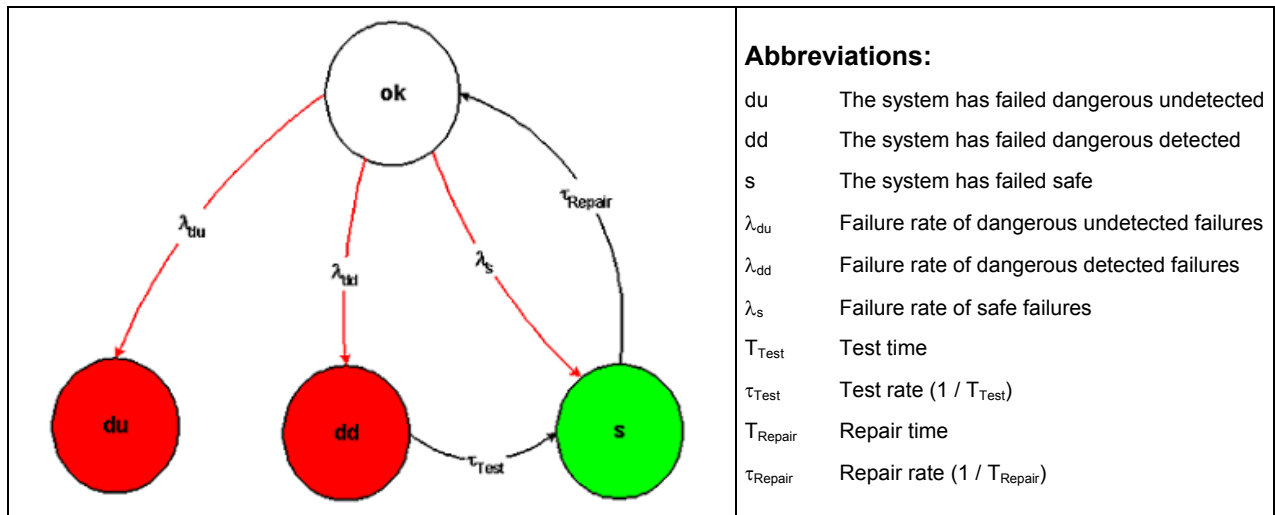


Figure 2: Markov model for a 1oo1D structure

5.1 Assessment of ED2-VM-Ex*.3**

According to IEC 61511-1 FDIS Ed.1 27-09-02 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.

Table 6 of IEC 61511-1 FDIS Ed.1 27-09-02
(Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers):

SIL	Minimum Hardware Fault Tolerance	
	Does not meet 11.4.4 requirements	Meets 11.4.4 requirements
1	0	0
2	1	0
3	2	1
4	Special requirements apply - See IEC 61508	

This means that if the requirements of section 11.4.4 of IEC 61511-1 FDIS Ed.1 27-09-02 are fulfilled a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with a SFF of 60% to < 90%².

This is identical to the requirements on Type A (sub)-systems. The Solenoid Valve Drivers ED2-VM-Ex*.3** have been developed before IEC 61508 was published, however, and so IEC 61511-1 FDIS Ed.1 27-09-02 section 11.4.4 is used as a basis for arguing that prior use shows the unlikelihood of systematic failures.

The assessment of the Solenoid Valve Drivers ED2-VM-Ex*.3** has shown that the requirements of IEC 61511-1 FDIS Ed.1 27-09-02 section 11.4.4 are fulfilled based on the following argumentation:

² IEC 61511-1 FDIS Ed.1 27-09-02 explicitly says "...provided that the dominant failure mode is to the safe state or dangerous failures are detected...".

Requirement	Argumentation ³
See Appendix 1: Prior use Proof according to IEC 61511-1 FDIS Ed.1 27-09-02	<ol style="list-style-type: none"> 1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 6 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail⁴ is very low (< 0.5%). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D4] to [D7]. The assessed sub-systems are clearly identified and specified (see Table 1). The field feedback tracking database of Pepperl+Fuchs GmbH together with the explanations given in [D8] demonstrated the performance of the sub-system in similar operating profiles and physical environments and the operating experience (Operating experience of more than 40.500.000 operating hours exists. This is considered to be sufficient taking into account the low complexity of the sub-system and the use in SIL 2 safety functions only). 3. 11.5.2 is under the responsibility of the manufacturer → no argumentation. 11.5.3 see bullet items before. 4. N/A 5. Under the responsibility of the manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D8].
Adjustment of process-related parameters only	N/A
Adjustment of process-related parameters is protected	N/A
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Solenoid Valve Drivers ED2-VM-Ex*.3** with a SFF of 60% - < 90% and HFT = 0 can be considered to be proven-in-use according to IEC 61511-1 FDIS Ed.1 27-09-02.

³ The numbering is based on the requirements detailed in appendix 1.

⁴ The probability of failure is the percentage of all returned devices of the ED2-VM-Ex*.3** family to all sold devices of the ED2-VM-Ex*.3** family based on the assumption that all returned devices from the field failed.

5.2 ED2-VM-Ex4.3* - switch-off path via logic input

The FMEDA carried out on the Solenoid Valve Driver ED2-VM-Ex4.3* with a common power supply and independent power supplies for the 4 channels leads under the assumptions described in section 4.2.3 and 5 and the consideration of the switch-off path via D32 (D30, D28, D26) or Z32 (Z30, Z28, Z26) to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 6,83E-08 \text{ 1/h} + 8,32E-08 \text{ 1/h} + 1,45E-09 \text{ 1/h} = 1,53E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 6,22E-09 \text{ 1/h}$$

$$\lambda_{\text{total}} = 1,59E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 5,20E-09 \text{ 1/h}$$

$$\text{SFF} = 96,09\%$$

The PFD_{AVG} for the solenoid valve driver with switch-off path via logic input 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
$\text{PFD}_{\text{AVG}} = 2,72E-05$	$\text{PFD}_{\text{AVG}} = 1,36E-04$	$\text{PFD}_{\text{AVG}} = 2,72E-04$

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$. Figure 3 shows the time dependent curve of PFD_{AVG} .

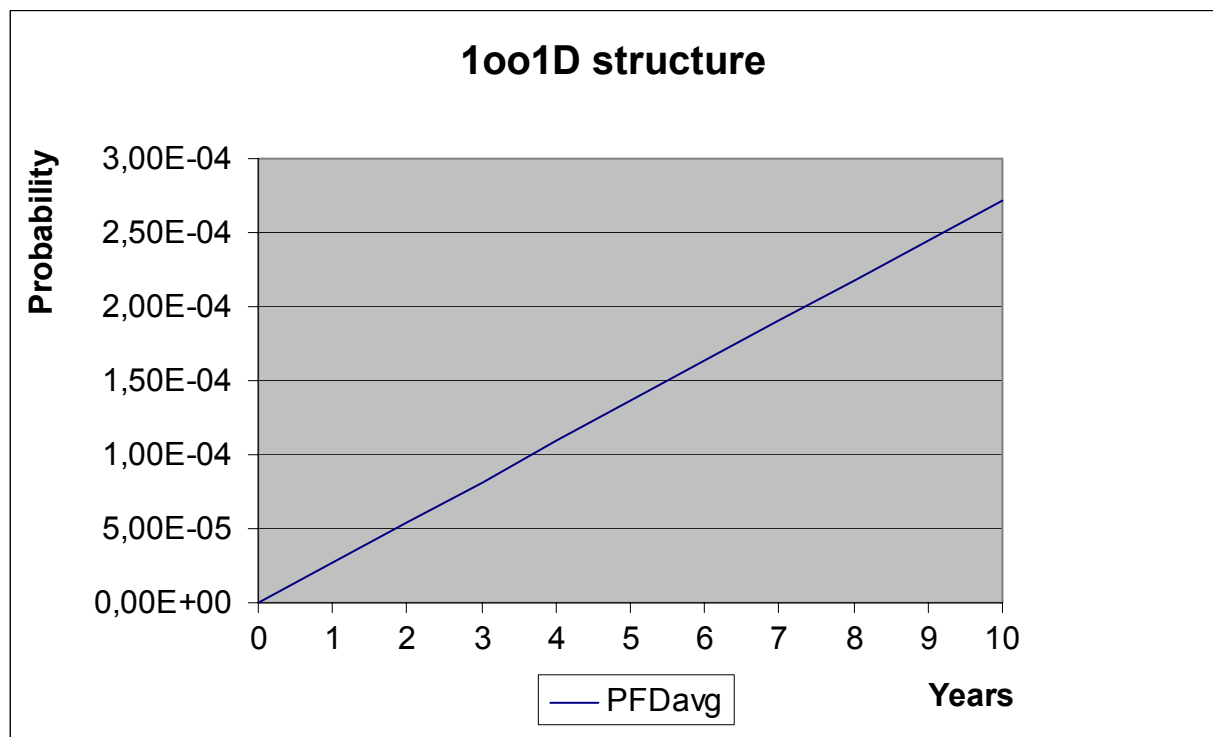


Figure 3: $\text{PFD}_{\text{AVG}}(t)$ - switch-off path via logic input

5.3 ED2-VM-Ex4.3*.O - switch-off path via logic input

The FMEDA carried out on the Solenoid Valve Driver ED2-VM-Ex4.3*.O... with a common power supply and independent power supplies for the 4 channels leads under the assumptions described in section 4.2.3 and 5 and the consideration of the switch-off path via D32 (D30, D28, D26) or Z32 (Z30, Z28, Z26) to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 7,78E-08 \text{ 1/h} + 8,27E-08 \text{ 1/h} + 1,45E-09 \text{ 1/h} = 1,62E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 1,16E-08 \text{ 1/h}$$

$$\lambda_{\text{total}} = 1,74E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 5,20E-09 \text{ 1/h}$$

$$\text{SFF} = 93,32\%$$

The PFD_{AVG} for the solenoid valve driver with switch-off path via logic input 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
$\text{PFD}_{\text{AVG}} = 5,08E-05$	$\text{PFD}_{\text{AVG}} = 2,54E-04$	$\text{PFD}_{\text{AVG}} = 5,07E-04$

The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$. Figure 3 shows the time dependent curve of PFD_{AVG} .

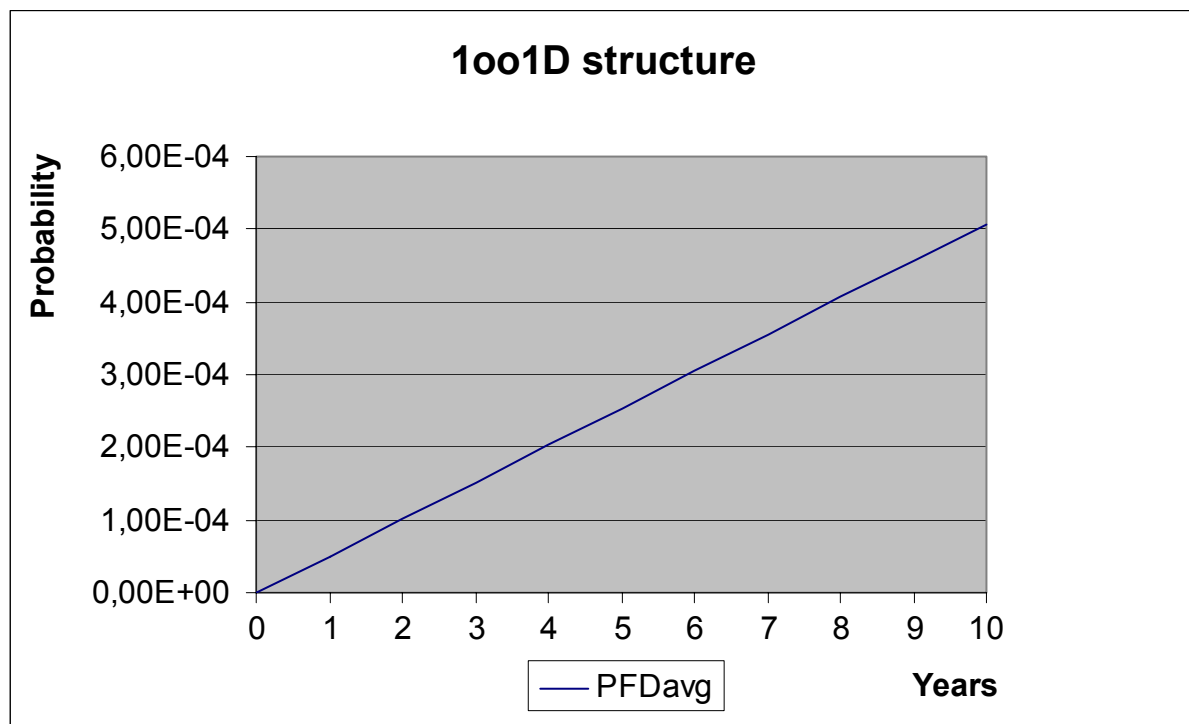


Figure 4: $\text{PFD}_{\text{AVG}}(t)$ - switch-off path via logic input

5.4 ED2-VM-Ex4.3* - switch-off path via common power supply

The FMEDA carried out on the Solenoid Valve Driver ED2-VM-Ex4.3.* with a common power supply and independent power supplies for the 4 channels leads under the assumptions described in section 4.2.3 and 5 and the consideration of the switch-off path via D14 (D16, D18, D20) to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 6,83E-08 \text{ 1/h} + 8,88E-08 \text{ 1/h} + 1,45E-09 \text{ 1/h} = 1,59E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 6,40E-10 \text{ 1/h}$$

$$\lambda_{\text{total}} = 1,59E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 5,20E-09 \text{ 1/h}$$

$$\text{SFF} = 99,60\%$$

The PFD_{AVG} for the solenoid valve driver with switch-off path via common power supply 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
$\text{PFD}_{\text{AVG}} = 2,80E-06$	$\text{PFD}_{\text{AVG}} = 1,40E-05$	$\text{PFD}_{\text{AVG}} = 2,80E-05$

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 table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-04$. Figure 3 shows the time dependent curve of PFD_{AVG} .

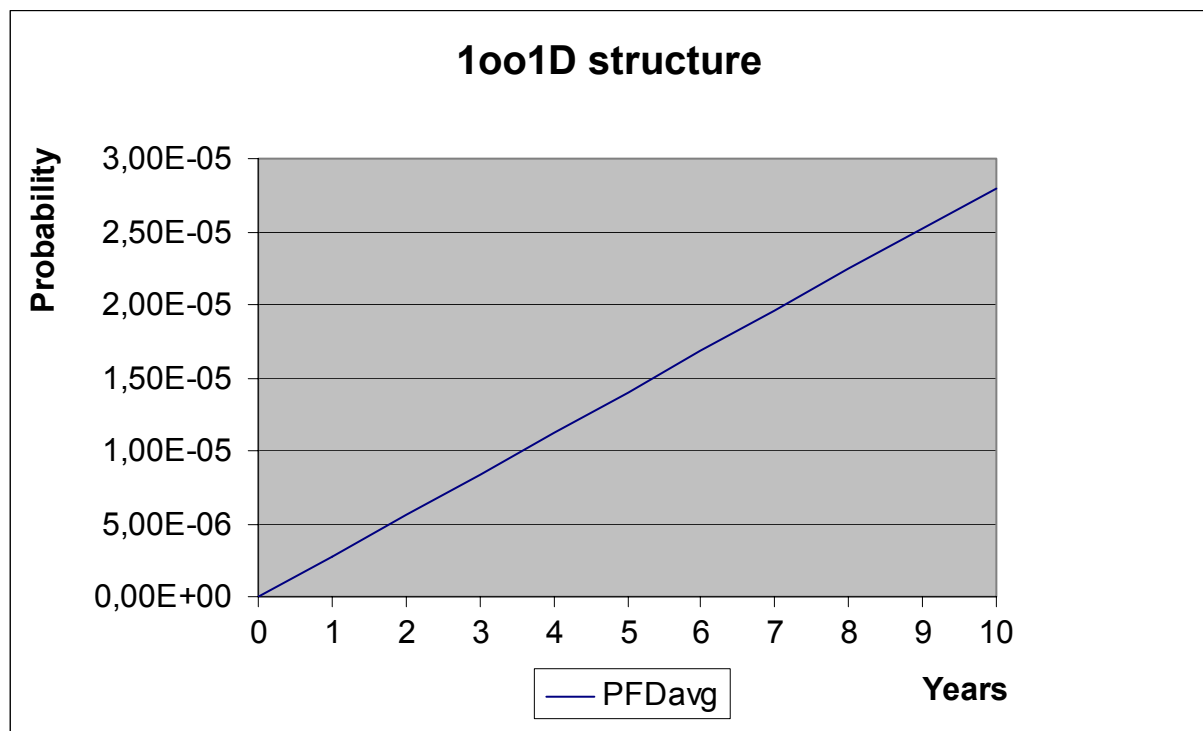


Figure 5: $\text{PFD}_{\text{AVG}}(t)$ - switch-off path via common power supply

5.5 ED2-VM-Ex4.3*.O - switch-off path via common power supply

The FMEDA carried out on the Solenoid Valve Driver ED2-VM-Ex4.3*.O with a common power supply and independent power supplies for the 4 channels leads under the assumptions described in section 4.2.3 and 5 and the consideration of the switch-off path via D14 (D16, D18, D20) to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 7,78E-08 \text{ 1/h} + 9,37E-08 \text{ 1/h} + 1,45E-09 \text{ 1/h} = 1,73E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 6,40E-10 \text{ 1/h}$$

$$\lambda_{\text{total}} = 1,74E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 5,20E-09 \text{ 1/h}$$

$$\text{SFF} = 99,63\%$$

The PFD_{AVG} for the solenoid valve driver with switch-off path via common power supply 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
$\text{PFD}_{\text{AVG}} = 2,80E-06$	$\text{PFD}_{\text{AVG}} = 1,40E-05$	$\text{PFD}_{\text{AVG}} = 2,80E-05$

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 table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-04$. Figure 3 shows the time dependent curve of PFD_{AVG} .

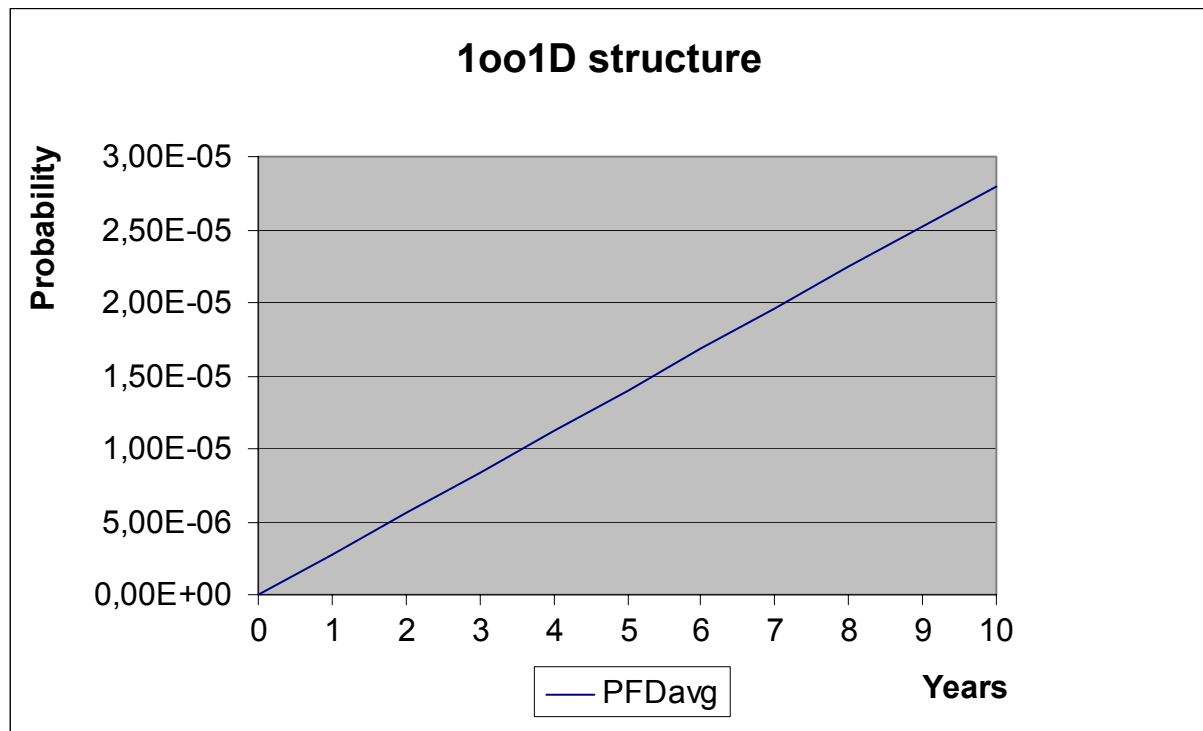


Figure 6: $\text{PFD}_{\text{AVG}}(t)$ - switch-off path via common power supply

6 Terms and Definitions

FIT	Failure In Time (1×10^{-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 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
SIS	Safety Instrumented System
Type A component	“Non-complex” component (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.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* 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.

7.2 Releases

Version: V1

Revision: R1.0

Version History: V0, R1.0: Initial version; May 18, 2003

V0, R1.1: Review comments integrated; June 26, 2003

V1, R1.0: First official release; July 1, 2003

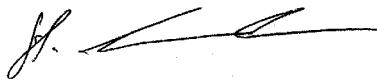
Authors: Stephan Aschenbrenner

Review: V0, R1.0 reviewed by P+F; June 18, 2003

V0, R1.1 reviewed by Rachel van Beurden-Amkreutz (*exida*); June 30, 2003

Release status: Released to Pepperl+Fuchs

7.3 Release Signatures



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



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

Appendix 1: Prior use Proof according to IEC 61511-1 FDIS Ed.1 27-09-02

Appendix 1.1 Section 11.5.3 of IEC 61511-1 FDIS Ed.1 27-09-02

(Requirements for the selection of components and subsystems based on prior use)

1. An assessment shall provide appropriate evidence that the components and sub-systems are suitable for use in the safety instrumented system.
2. The evidence of suitability shall include the following:
 - consideration of the manufacturer's quality management and configuration management systems;
 - adequate identification and specification of the components or sub-systems;
 - demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;
 - the volume of the operating experience.

Appendix 1.2 Section 11.5.4 of IEC 61511-1 FDIS Ed.1 27-09-02

(Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use)

3. The requirements of 11.5.2 and 11.5.3 apply.
4. Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.
5. For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider:
 - characteristics of input and output signals;
 - modes of use;
 - functions and configurations used;
 - previous use in similar applications and physical environments.

Appendix 1.3 Section 11.5.2 of IEC 61511-1 FDIS Ed.1 27-09-02

(General Requirements)

6. Components and sub-systems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with sub-clauses 11.4 and 11.5.3 to 11.5.6, as appropriate.

7. Components and sub-systems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.
8. The suitability of the selected components and sub-systems shall be demonstrated, through consideration of:
 - manufacturer hardware and embedded software documentation;
 - if applicable, appropriate application language and tool selection (see clause 12.4.4).
9. The components and sub-systems shall be consistent with the SIS safety requirements specifications.

Appendix 2: 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 7 shows a sensitivity analysis of the critical dangerous undetected faults of the Solenoid Valve Drivers ED2-VM-Ex4.3*.O and indicates how these faults can be detected during proof testing.

Table 7: Sensitivity Analysis of dangerous undetected faults

Component	% of total λ_{du}	Detection through
U1.1	45%	100% functional test
P1.1	22%	100% functional test
SL1	14%	100% functional test
IC1	13%	100% functional test
N9.1	4%	100% functional test
R15.1	1%	100% functional test
R20.1	1%	100% functional test

Appendix 3: 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 (i.e. as the probability of failure significantly increases with time) the results of the probabilistic calculation method is therefore meaningless. 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.

The circuit of the Solenoid Valve Drivers ED2-VM-Ex4... 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 life of the system.

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