FMEDA and Proven-in-use Assessment

Project:
Inductive NAMUR sensors

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 03/11-10
Report No.: P+F 03/11-10 R015
Version V1, Revision R1.1, July 2004

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the inductive NAMUR sensors listed in Table 1. Table 1 gives an overview of the different versions that belong to the considered sensors. The compliance of individual products with the sensors covered by this report has to be confirmed by the manufacturer.

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

Version	Type	Circuit diagram	Sensors
V1	NJ 5-30GK-S1N***	01-2320	1
V2	NJ 6S1+U*+N1***	01-2362	1
V3	NJ 5-18GK-SN***	01-2363A	1
	NJ 8-18GK-SN***		
	NJ 10-30GK-SN***		
	NJ 15-30GK-SN***		
	NJ 15S+U*+N***		
	NJ 20S+U*+N***		
	NJ 40-FP-SN***		
	NJ 6-22-SN***		
	NJ 6-22-SN-G***		
V4	SJ 2-SN***	01-2525A	1
	SJ 3,5-SN***		
V5	SJ 3,5-S1N***	01-2628B	1
V6	NJ 2-11-SN***	01-3312A	1
	NJ 2-11-SN-G***		
	NJ 2-12GK-SN***		
	NJ 4-12GK-SN***		
V7	NJ 3-18GK-S1N***	01-3348A	1
V8	SJ 2-S1N***	01-3778	1
V9[1]	NCN3-F25*-SN4***	01-4326C	2

Failure rates used in this analysis are basic failure rates from 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 $\geq 10^{-3}$ 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-03.

[1] Because this sensor is not on the market yet, no operating experience can be demonstrated.

The sensors of Table 1 are considered to be Type A[2] components with a hardware fault tolerance of 0.

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

As the above described NAMUR sensors 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. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1.2 the devices are suitable to be used, as a single device, for SIL 2 safety functions.

Application with standard NAMUR amplifier[3] according to EN 60947-5-6:

Table 2: Summary of all considered NAMUR sensors[4]– Failure rates according to IEC 61508

Type	λ_{safe}	$\lambda_{dangerous}$	SFF
NJ 5-30GK-S1N***	15,4 FIT	9,63 FIT	61,48%
NJ 6S1+U*+N1***	15,4 FIT	9,63 FIT	61,48%
NJ 5-18GK-SN*** **NJ 8-18GK-SN***** **NJ 10-30GK-SN***** **NJ 15-30GK-SN***** **NJ 15S+U*+N***** **NJ 20S+U*+N***** **NJ 40-FP-SN***** **NJ 6-22-SN***** **NJ 6-22-SN-G*****	15,4 FIT	9,63 FIT	61,48%
SJ 2-SN*** **SJ 3,5-SN*****	15,2 FIT	9,61 FIT	61,25%
SJ 3,5-S1N***	15,4 FIT	9,63 FIT	61,48%
NJ 2-11-SN*** **NJ 2-11-SN-G***** **NJ 2-12GK-SN***** **NJ 4-12GK-SN*****	19,1 FIT	10,7 FIT	64,14%
NJ 3-18GK-S1N***	19,1 FIT	10,7 FIT	64,14%
SJ 2-S1N***	15,4 FIT	9,63 FIT	61,48%
NCN3-F25*-SN4***	19,1 FIT	10,7 FIT	64,14%

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

[3] Failure rates of the standard NAMUR amplifier are not included in the failure rates listed in Table 2.

[4] Some results are based on FMEDAs carried out on the “two channel” versions but are considered to be the same for the “one channel” versions as also for the “two channel” versions only one channel was considered.

Table 3: Summary of all considered NAMUR sensors – PFD_{AVG} values

Type	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
NJ 5-30GK-S1N***	PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-04
NJ 6S1+U*+N1***	PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-04
NJ 5-18GK-SN*** NJ 8-18GK-SN*** NJ 10-30GK-SN*** NJ 15-30GK-SN*** NJ 15S+U*+N*** NJ 20S+U*+N*** NJ 40-FP-SN*** NJ 6-22-SN*** NJ 6-22-SN-G***	PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-04
SJ 2-SN*** SJ 3,5-SN***	PFD_{AVG} = 4.21E-05	PFD_{AVG} = 8.42E-05	PFD_{AVG} = 2.10E-04
SJ 3,5-S1N***	PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-04
NJ 2-11-SN*** NJ 2-11-SN-G*** NJ 2-12GK-SN*** NJ 4-12GK-SN***	PFD_{AVG} = 4.66E-05	PFD_{AVG} = 9.33E-05	PFD_{AVG} = 2.33E-04
NJ 3-18GK-S1N***	PFD_{AVG} = 4.66E-05	PFD_{AVG} = 9.33E-05	PFD_{AVG} = 2.33E-04
SJ 2-S1N***	PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-04
NCN3-F25*-SN4***	PFD_{AVG} = 4.66E-05	PFD_{AVG} = 9.33E-05	PFD_{AVG} = 2.33E-04

Application with (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1[5]:

Table 4: Summary of all considered NAMUR sensors – Failure rates according to IEC 61508

Type	λ_{safe}	$\lambda_{dangerous}$	SFF
NJ 5-30GK-S1N* **	24,9 FIT	0,09 FIT	99,64%
NJ 6S1+U*+N1* **	24,9 FIT	0,09 FIT	99,64%
NJ 5-18GK-SN* ** **NJ 8-18GK-SN*** ** **NJ 10-30GK-SN*** ** **NJ 15-30GK-SN*** ** **NJ 15S+U*+N*** ** **NJ 20S+U*+N*** ** **NJ 40-FP-SN*** ** **NJ 6-22-SN*** ** **NJ 6-22-SN-G*** **	24,9 FIT	0,09 FIT	99,64%
SJ 2-SN* ** **SJ 3,5-SN*** **	24,7 FIT	0,07 FIT	99,72%
SJ 3,5-S1N* **	24,9 FIT	0,09 FIT	99,64%
NJ 2-11-SN* ** **NJ 2-11-SN-G*** ** **NJ 2-12GK-SN*** ** **NJ 4-12GK-SN*** **	29,6 FIT	0,09 FIT	99,70%
NJ 3-18GK-S1N* **	29,6 FIT	0,09 FIT	99,70%
SJ 2-S1N* **	24,9 FIT	0,09 FIT	99,64%
NCN3-F25*-SN4* **	29,6 FIT	0,09 FIT	99,70%

[5] Failure rates of the amplifier KFD2-SH-Ex1 are not included in the failure rates listed in Table 4.

Table 5: Summary of all considered NAMUR sensors – PFD_{AVG} values

Type	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
NJ 5-30GK-S1N***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
NJ 6S1+U*+N1***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
NJ 5-18GK-SN*** NJ 8-18GK-SN*** NJ 10-30GK-SN*** NJ 15-30GK-SN*** NJ 15S+U*+N*** NJ 20S+U*+N*** NJ 40-FP-SN*** NJ 6-22-SN*** NJ 6-22-SN-G***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
SJ 2-SN*** SJ 3,5-SN***	PFD_{AVG} = 3.07E-07	PFD_{AVG} = 6.13E-07	PFD_{AVG} = 1.53E-06
SJ 3,5-S1N***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
NJ 2-11-SN*** NJ 2-11-SN-G*** NJ 2-12GK-SN*** NJ 4-12GK-SN***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
NJ 3-18GK-S1N***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
SJ 2-S1N***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06
NCN3-F25*-SN4***	PFD_{AVG} = 3.94E-07	PFD_{AVG} = 7.88E-07	PFD_{AVG} = 1.97E-06

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 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.

The functional assessment has shown that the NAMUR sensors have a PFD_{AVG} 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 a Safe Failure Fraction (SFF) of more than 61% for applications with standard NAMUR amplifier according to EN 60947-5-6 and a SFF of more than 99% for applications with (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to "prior-use" of IEC 61511-1 they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

Although the PFD_{AVG} values and the SFF of the NAMUR sensors for applications with (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1 are within the allowed range for SIL 3 according to IEC 61508 it depends on the failure rates of the fail safe interface whether they can also be used for SIL 3 safety functions.

A user of the NAMUR sensors can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates for different operating conditions is presented in section 5.1 to 5.9 along with all assumptions.

It is important to realize that the “don’t care” 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

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 consist of an assessment of the software development process

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

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 and its software 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 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 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 FMEDAs carried out on the inductive NAMUR sensors listed in Table 1. Table 1 gives an overview and explains the differences.

It shall be assessed whether these NAMUR sensors 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.

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 NAMUR sensors.
exida.com	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

Pepperl+Fuchs GmbH contracted *exida.com* in January 2004 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	IEC 61511-1 First Edition 2003-01	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	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	01-2320 Index 0 of 24.01.86	Circuit diagram for NJ 5-30GK-S1N
[D1.1]	Product No. 106649	Bill of material for NJ 5-30GK-S1N
[D2]	01-2362 Index 0 of 17.04.86	Circuit diagram for NJ 6 S1+…
[D2.1]	Product No. 106661	Bill of material for NJ 6 S1+…
[D3]	01-2363 Index A of 06.06.89	Circuit diagram
[D3.1]	Product No. 106643	Bill of material for NJ 5-18GK-SN
[D3.2]	Product No. 106662	Bill of material for NJ 8-18GK-SN
[D3.3]	Product No. 106667	Bill of material for NJ 10-30GK-SN
[D3.4]	Product No. 106676	Bill of material for NJ 15-30GK-SN
[D3.5]	Product No. 106679	Bill of material for NJ 15S+U1+N
[D3.6]	Product No. 106683	Bill of material for NJ 20S+U1+N
[D3.7]	Product No. 106696	Bill of material for NJ 40-FP-SN-P1
[D3.8]	Product No. 106654	Bill of material for NJ 6-22-SN
[D3.9]	Product No. 106656	Bill of material for NJ 6-22-SN-G
[D4]	01-2525 Index A of 14.09.99	Circuit diagram
[D4.1]	Product No. 106718	Bill of material for SJ 2-SN
[D4.2]	Product No. 106710	Bill of material for SJ 3,5-SN
[D5]	01-2628 Index B of 15.12.99	Circuit diagram for SJ 3,5-S1N
[D5.1]	Product No. 106709	Bill of material for SJ 3,5-S1N
[D6]	01-3312 Index A of 15.07.92	Circuit diagram for NJ 2/4-12GK-SN
[D6.1]	Product No. 106633 / 106641	Bill of material for NJ 2/4-12GK-SN
[D7]	01-3348 Index A of 21.12.92	Circuit diagram for NJ 3-18GK-S1N
[D7.1]	Product No. 106639 / 028409	Bill of material for NJ 3-18GK-S1N
[D8]	01-3778 Index 0 of 13.07.94	Circuit diagram for SJ2-S1N
[D8.1]	Product No. 106704	Bill of material for SJ2-S1N
[D9]	01-4326 Index C of 24.07.01	Circuit diagram for NCN3-…-SN4..
[D9.1]	Product No. 044989	Bill of material for NCN3-F25-SN4-V1
[D10]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D11]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D12]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D13]	Betriebsbewährung SN-Sensoren.xls	Statistics of field-feed-back tracking; sold devices

[D14]	Auswertung SJ_PPM- Raten.xls	Statistics of field-feed-back tracking; returned devises
[D15]	exida Applikationsbeispiele 2.doc	Document about the applications the operating experience is based on
[D16]	Email of 07.04.04	Description of the different working principles of SN and S1N sensors

2.4.2 Documentation generated by *exida.com*

R1	FMEDA V5 R0.2 1-2320 Standard V0 R1.0.xls of 29.01.04
R2	FMEDA V5 R0.2 1-2320 V0 R1.0.xls of 29.01.04
R3	FMEDA V5 R0.2 1-2362 Standard V0 R1.0.xls of 29.01.04
R4	FMEDA V5 R0.2 1-2362 V0 R1.0.xls of 29.01.04
R5	FMEDA V5 R0.2 1-2363A Standard V0 R1.0.xls of 29.01.04
R6	FMEDA V5 R0.2 1-2363A V0 R1.0.xls of 29.01.04
R7	FMEDA V5 R0.2 1-2525A Standard V0 R1.0.xls of 17.03.04
R8	FMEDA V5 R0.2 1-2525A V0 R1.0.xls of 29.01.04
R9	FMEDA V5 R0.2 1-2628B Standard V0 R1.0.xls of 29.01.04
R10	FMEDA V5 R0.2 1-2628B V0 R1.0.xls of 29.01.04
R11	FMEDA V5 R0.2 01-3312A Standard V0 R1.0.xls of 29.01.04
R12	FMEDA V5 R0.2 01-3312A V0 R1.0.xls of 29.01.04
R13	FMEDA V5 R0.2 1-3348A Standard V0 R1.0.xls of 29.01.04
R14	FMEDA V5 R0.2 1-3348A V0 R1.0.xls of 29.01.04
R15	FMEDA V5 R0.2 01-3778 Standard V0 R1.0.xls of 17.03.04
R16	FMEDA V5 R0.2 01-3778 V0 R1.0.xls of 29.01.04
R17	FMEDA V5 R0.2 01-4326C Standard V0 R1.0.xls of 29.01.04
R18	FMEDA V5 R0.2 01-4326C V0 R1.0.xls of 29.01.04
R19	Betriebsbewährung SN-Sensoren – exida.xls of 06.04.04
R20	Auswertung SJ_PPM- Raten – exida.xls of 16.03.04

3 Functional Description

3.1 Analyzed sensors

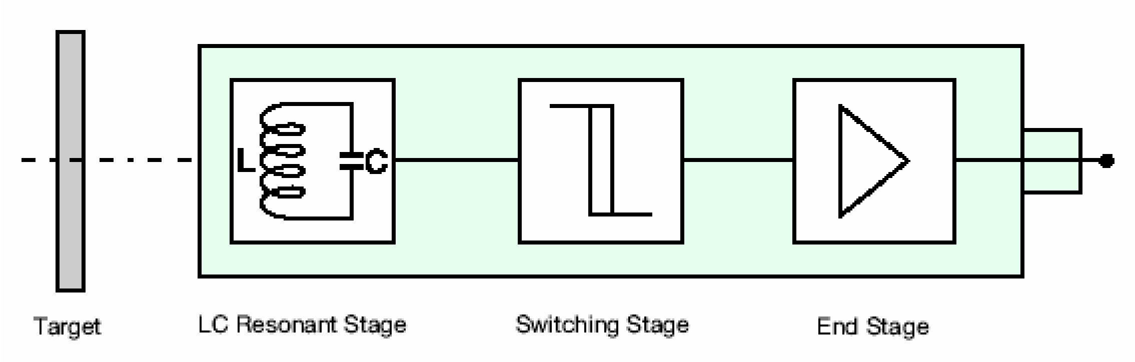


Figure 1: General description of the inductive sensors

The most important component of the inductive sensors is the LC resonant circuit. The coil L of this resonant circuit generates a magnetic field. This magnetic field generates eddy currents in a metallic target and losses due to magnetic reversal.

These eddy currents and magnetic reversal losses damp the resonant circuit.

The smaller the distance from the target, the greater is the damping. The greater the damping, the smaller is the sensor current. This functional behavior is shown in Figure 2.

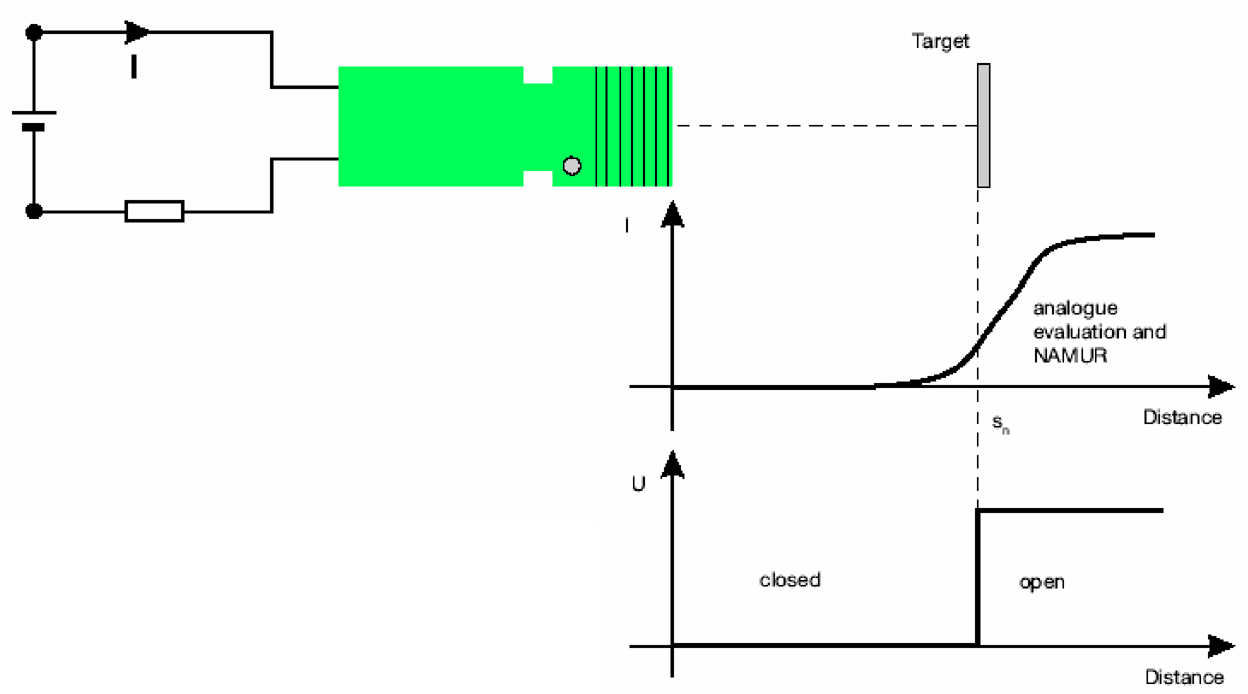


Figure 2: Functional behavior of the inductive sensors

The current consumption of an inductive sensor reduces as the separation from a metal object reduces.

3.2 Connection between analyzed sensors and for example KFD2-SH-Ex1

The Pepperl+Fuchs fail safe interface KFD2-SH-Ex1 is controlled with an SN- and/or S1N-series intrinsic safety proximity sensor. Figure 3 shows how sensor and amplifier are connected.

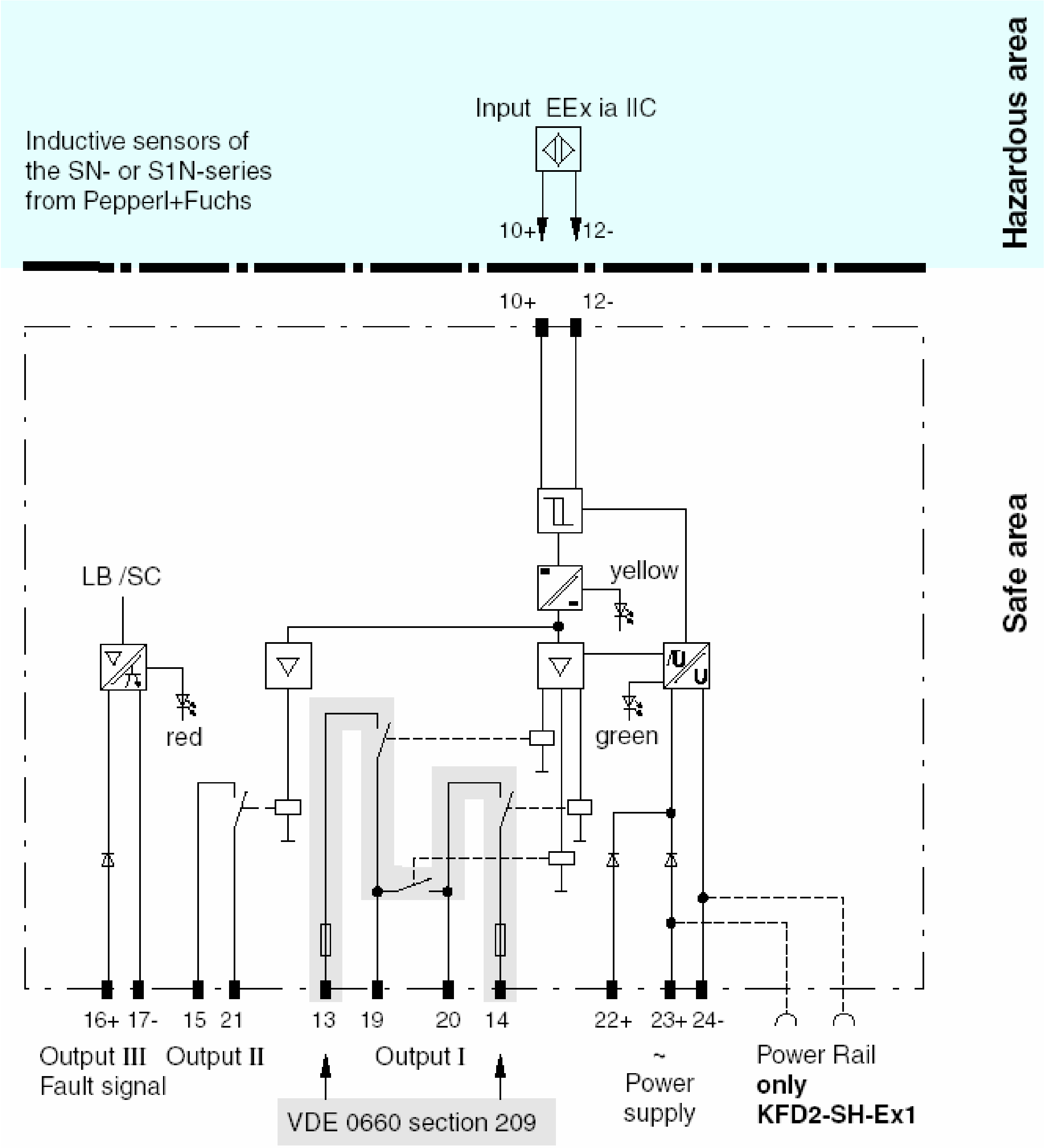


Figure 3: Connection between analyzed sensors and KFD2-SH-Ex1

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs GmbH and is documented in R1 to R18.

4.1 Description of the failure categories

In order to judge the failure behavior of the NAMUR sensors, the following definitions for the failure of the product were considered.

Application with standard NAMUR amplifier according to EN 60947-5-6:

Fail-Safe State — The fail-safe state is defined as the output being below 1.2 mA.

Fail Dangerous — Failure leading to an output current above 1.2 mA (i.e. being unable to go to the defined fail-safe state).

Application with (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1:

Fail-Safe State — The fail-safe state is defined as the output being below 1.8 mA or above 6 mA.

Fail Dangerous — Failure leading to an output current between 1.8 mA and 6 mA (i.e. being unable to go to the defined fail-safe state).

General failure categories:

Fail Safe — Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.

Fail No Effect — Failure of a component that is part of the safety function but that has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous.

In IEC 61508 the “No Effect” failures are defined as safe 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.

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 the basic failure rates 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 IEC 645-1, 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 sensors.

- 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 of the logic solver 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 Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 645-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1 is also suitable to be used for SIL 3 safety function.
- Short circuit (SC) and lead breakage (LB) detection of the (Pepperl+Fuchs) fail safe interface, for example KFD2-SH-Ex1 are activated and lead to a safe state of the interface.
- Sufficient damping is considered; i.e. max. 0,6 x sn[6] (SN sensors) and min. 1,4 x sn (S1N sensors).

[6] sn := rated operating distances.

5 Results of the assessment

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

The two channels on certain modules should not be used for one safety function as they contain common components.

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:

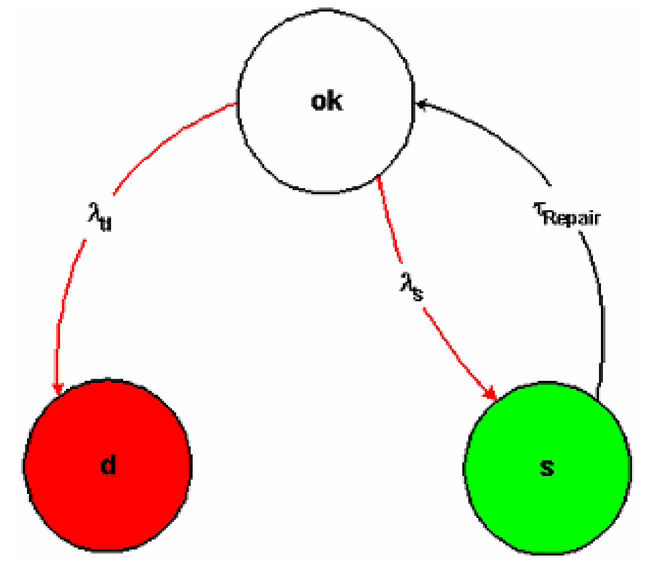
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care}$.

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

For the FMEDAs failure modes and distributions were used based on information gained from N3 and N4.

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1 system was used. As there are no explicit on-line diagnostics, no state “dd” – dangerous detected is required. 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.



Abbreviations:

d	The system has failed dangerous
s	The system has failed safe
λ_d	Failure rate of dangerous failures
λ_s	Failure rate of safe failures
T_{Repair}	Repair time
τ_{Repair}	Repair rate ($1 / T_{Repair}$)

Figure 4: Markov model

5.1 Version V1

5.1.1 Standard application

The FMEDA carried out on the sensors called version V1 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,28E-08 1/h + 2,56E-09 1/h = 1,54E-08 1/h

$\lambda_{dangerous}$ = 9,63E-09 1/h

λ_{total} = 2,50E-08 1/h

SFF = 61,48%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.22E-05	**PFD_{AVG} = 8.44E-05**	**PFD_{AVG} = 2.11E-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 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 5 shows the time dependent curve of PFD_{AVG}.

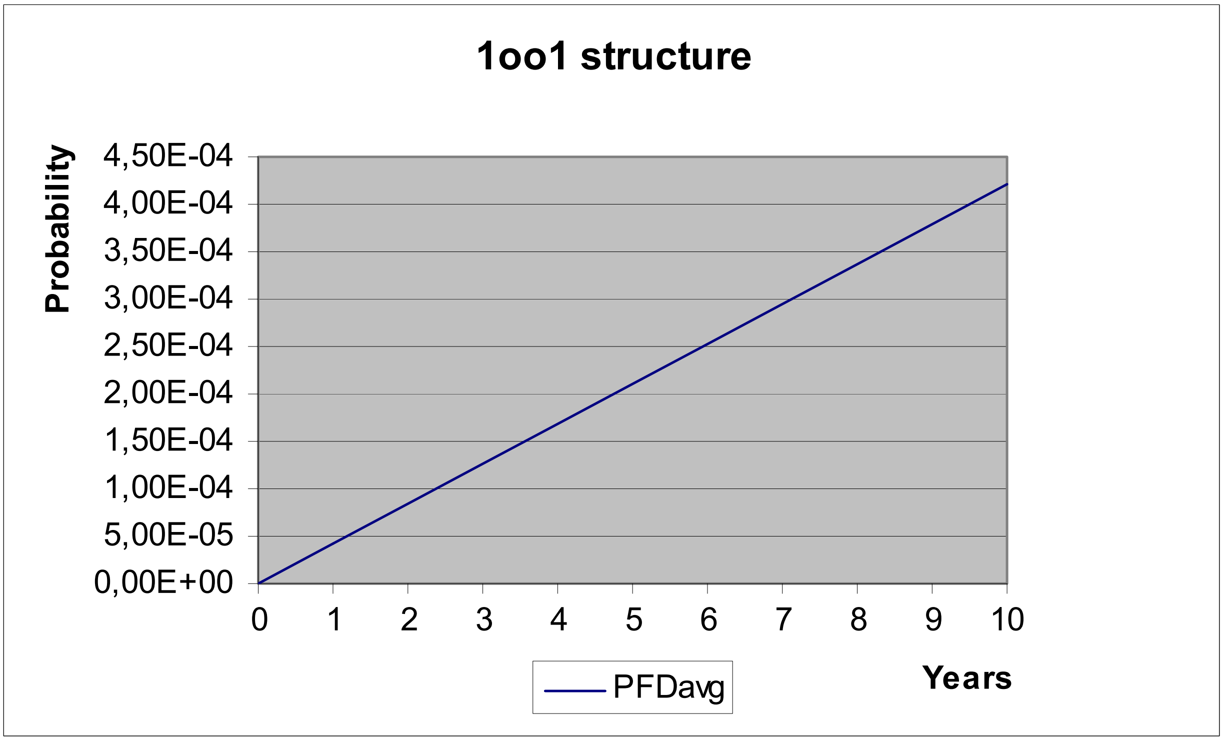


Figure 5: PFD_{AVG}(t) of V1 in standard application

5.1.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V1 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,24E-08 1/h + 2,56E-09 1/h = 2,49E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,50E-08 1/h

SFF = 99,64%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 6 shows the time dependent curve of PFD_{AVG}.

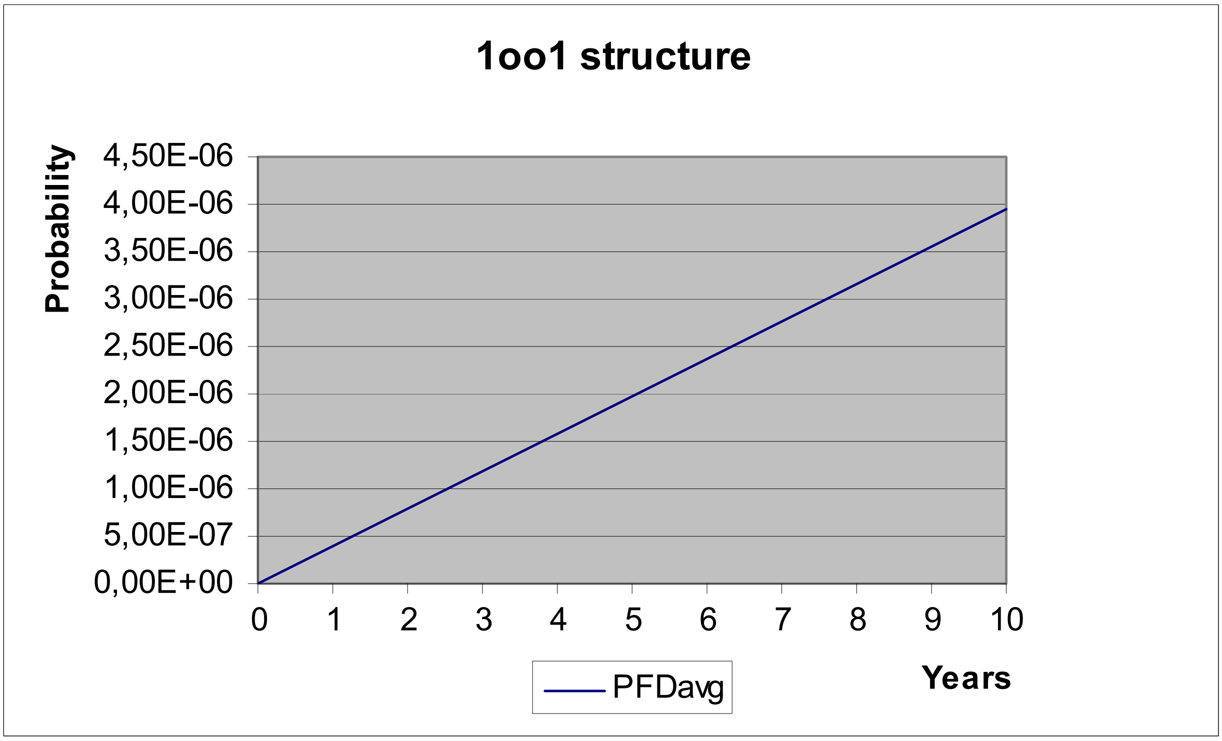


Figure 6: PFD_{AVG}(t) of V1 in applications with (Pepperl+Fuchs) fail safe interface

5.2 Version V2

5.2.1 Standard application

The FMEDA carried out on the sensors called version V2 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,28E-08 1/h + 2,56E-09 1/h = 1,54E-08 1/h

$\lambda_{dangerous}$ = 9,63E-09 1/h

λ_{total} = 2,50E-08 1/h

SFF = 61,48%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.22E-05	**PFD_{AVG} = 8.44E-05**	**PFD_{AVG} = 2.11E-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 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 7 shows the time dependent curve of PFD_{AVG}.

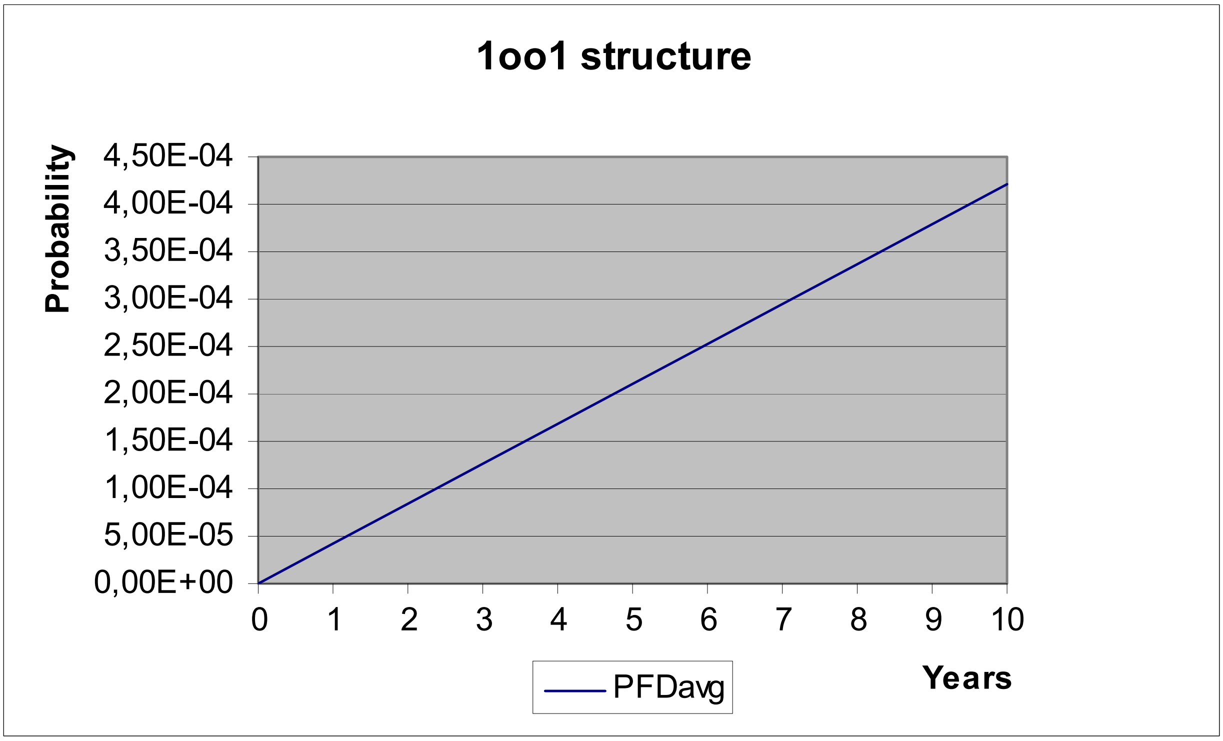


Figure 7: PFD_{AVG}(t) of V2 in standard application

5.2.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V2 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,24E-08 1/h + 2,56E-09 1/h = 2,49E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,50E-08 1/h

SFF = 99,64%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 8 shows the time dependent curve of PFD_{AVG}.

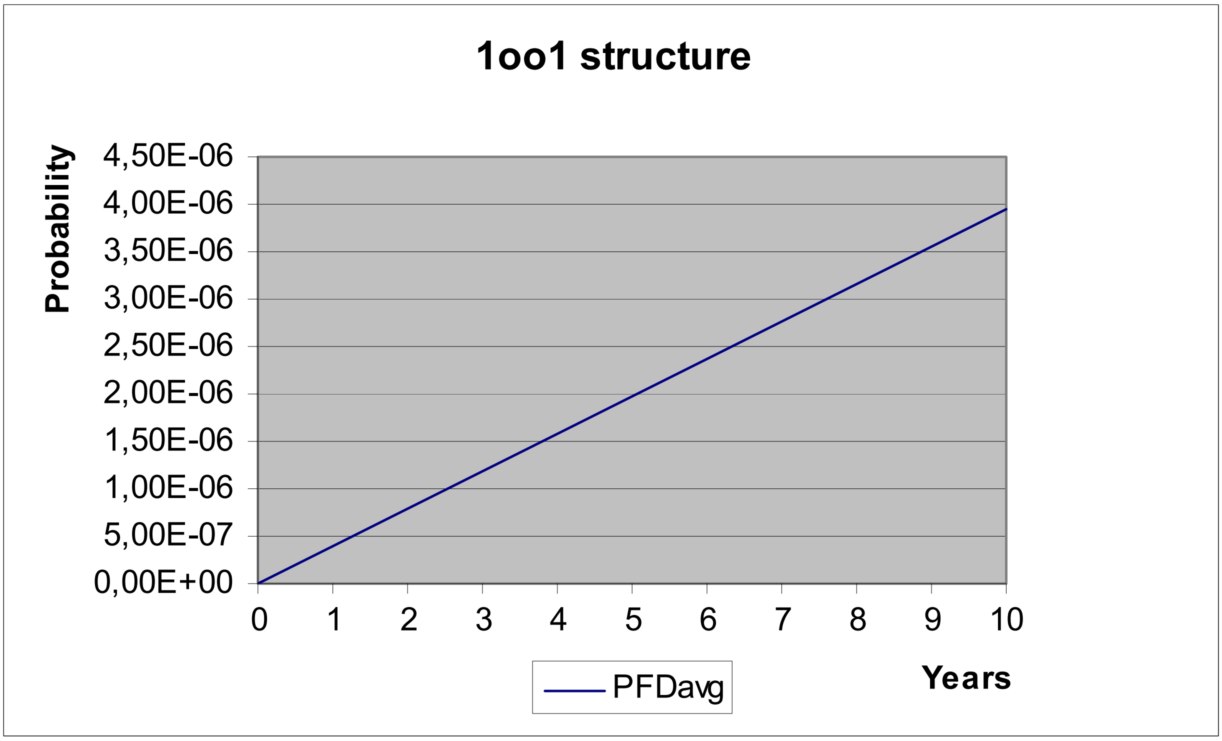


Figure 8: $PFD_{AVG}(t)$ of V2 in applications with (Pepperl+Fuchs) fail safe interface

5.3 Version V3

5.3.1 Standard application

The FMEDA carried out on the sensors called version V3 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,28E-08 1/h + 2,56E-09 1/h = 1,54E-08 1/h

$\lambda_{dangerous}$ = 9,63E-09 1/h

λ_{total} = 2,50E-08 1/h

SFF = 61,48%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-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 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 9 shows the time dependent curve of PFD_{AVG}.

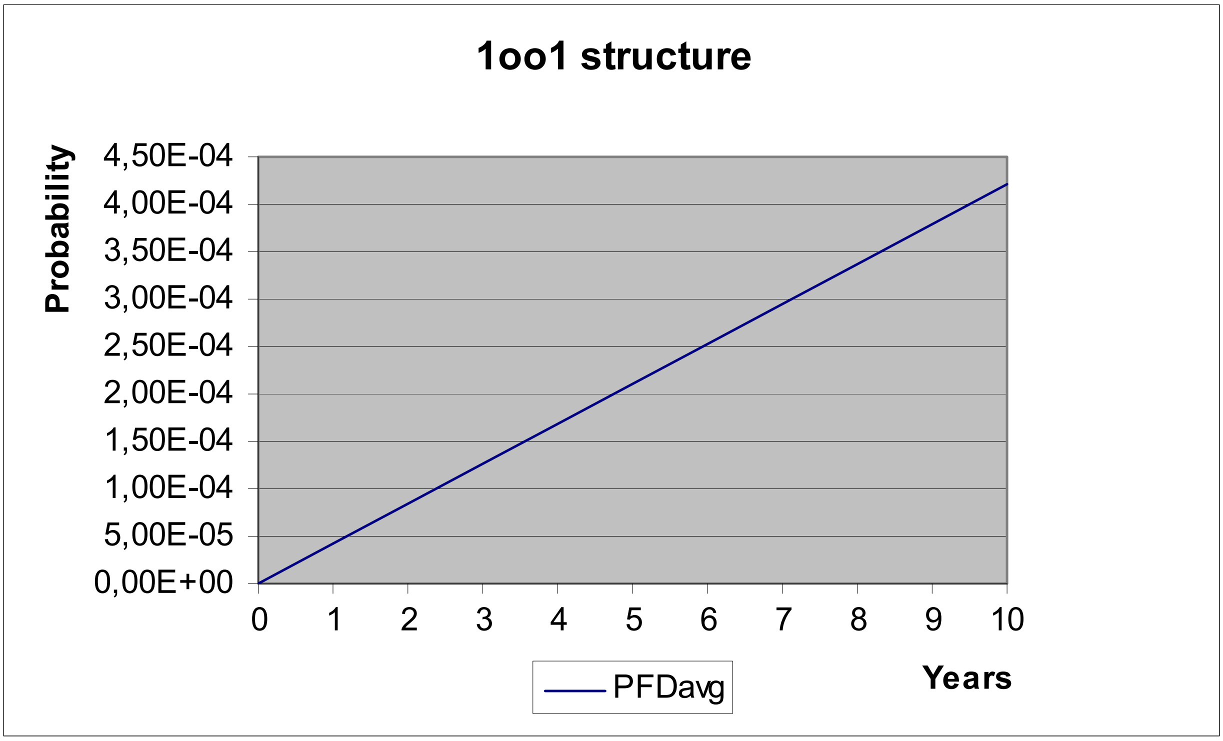


Figure 9: PFD_{AVG}(t) of V3 in standard application

5.3.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V3 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,24E-08 1/h + 2,56E-09 1/h = 2,49E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,50E-08 1/h

SFF = 99,64%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 10 shows the time dependent curve of PFD_{AVG}.

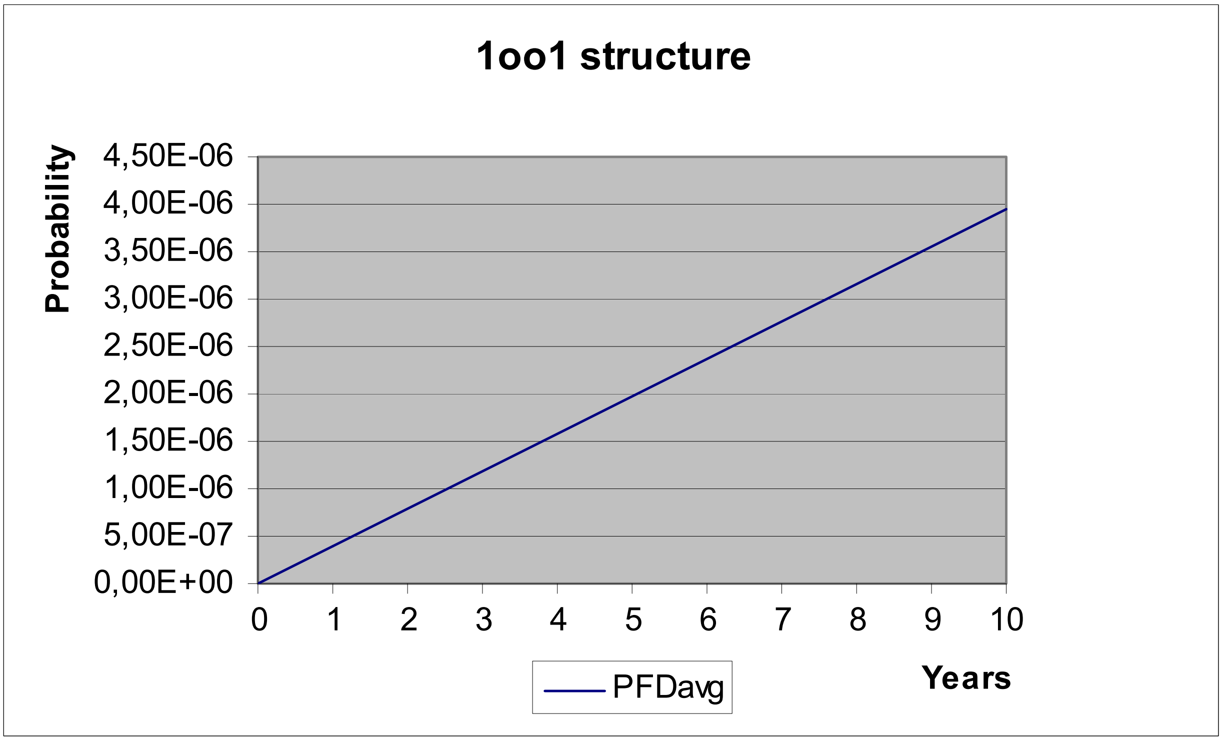


Figure 10: PFD_{AVG}(t) of V3 in applications with (Pepperl+Fuchs) fail safe interface

5.4 Version V4

5.4.1 Standard application

The FMEDA carried out on the sensors called version V4 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,27E-08 1/h + 2,50E-09 1/h = 1,52E-08 1/h

$\lambda_{dangerous}$ = 9,61E-09 1/h

λ_{total} = 2,48E-08 1/h

SFF = 61,25%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.21E-05	**PFD_{AVG} = 8.42E-05**	**PFD_{AVG} = 2.10E-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 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 11 shows the time dependent curve of PFD_{AVG}.

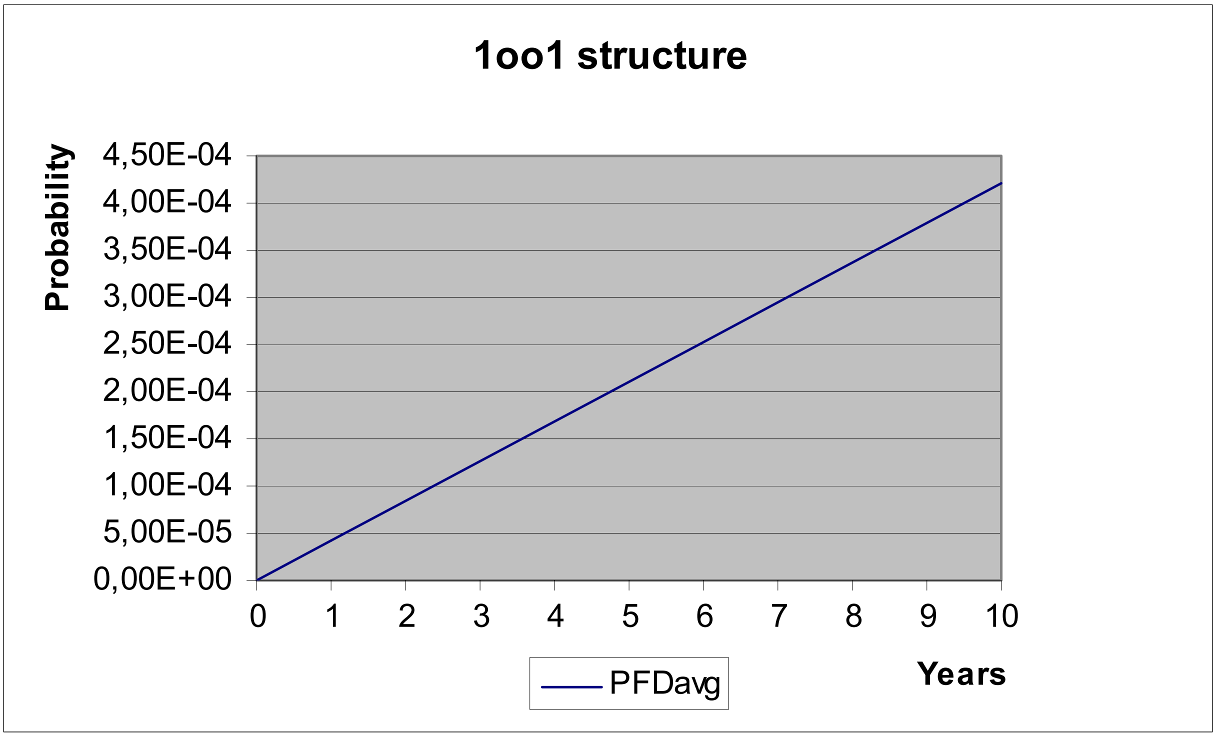


Figure 11: PFD_{AVG}(t) of V4 in standard application

5.4.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V4 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,22E-08 1/h + 2,50E-09 1/h = 2,47E-08 1/h

$\lambda_{dangerous}$ = 7,00E-11 1/h

λ_{total} = 2,48E-08 1/h

SFF = 99,72%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.07E-07	**PFD_{AVG} = 6.13E-07**	**PFD_{AVG} = 1.53E-06**

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 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 12 shows the time dependent curve of PFD_{AVG}.

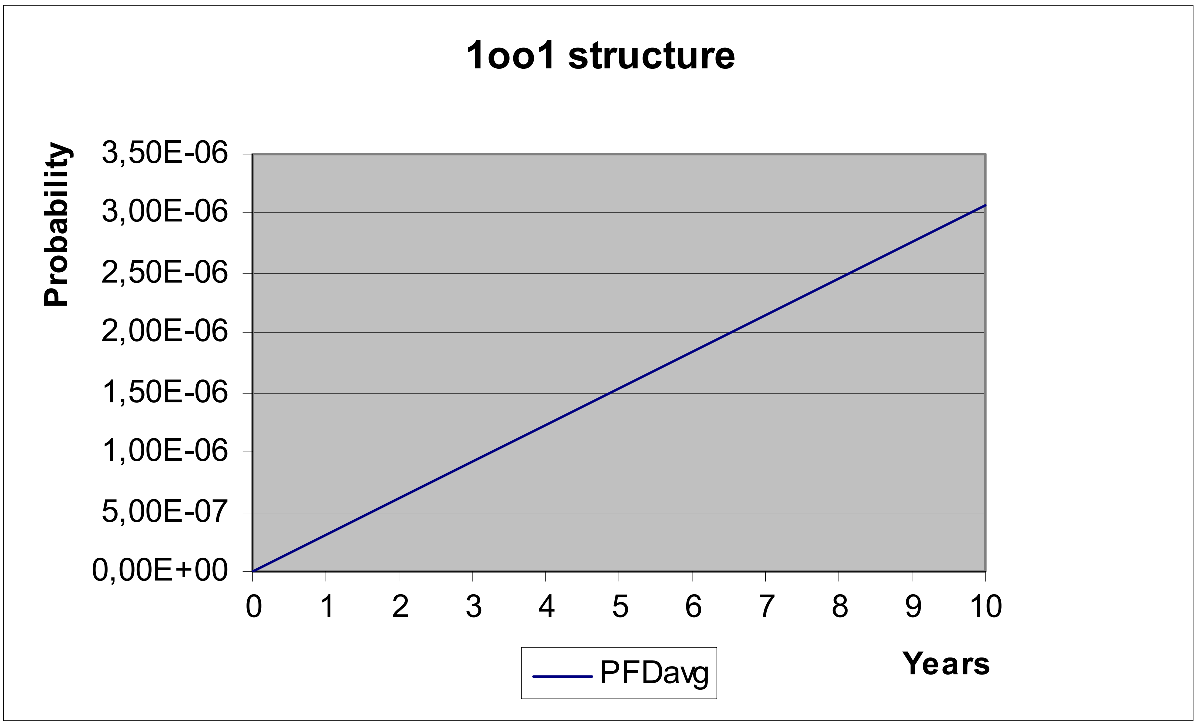


Figure 12: PFD_{AVG}(t) of V4 in applications with (Pepperl+Fuchs) fail safe interface

5.5 Version V5

5.5.1 Standard application

The FMEDA carried out on the sensors called version V5 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,28E-08 1/h + 2,56E-09 1/h = 1,54E-08 1/h

$\lambda_{dangerous}$ = 9,63E-09 1/h

λ_{total} = 2,50E-08 1/h

SFF = 61,48%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.22E-05	**PFD_{AVG} = 8.44E-05**	**PFD_{AVG} = 2.11E-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 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 13 shows the time dependent curve of PFD_{AVG}.

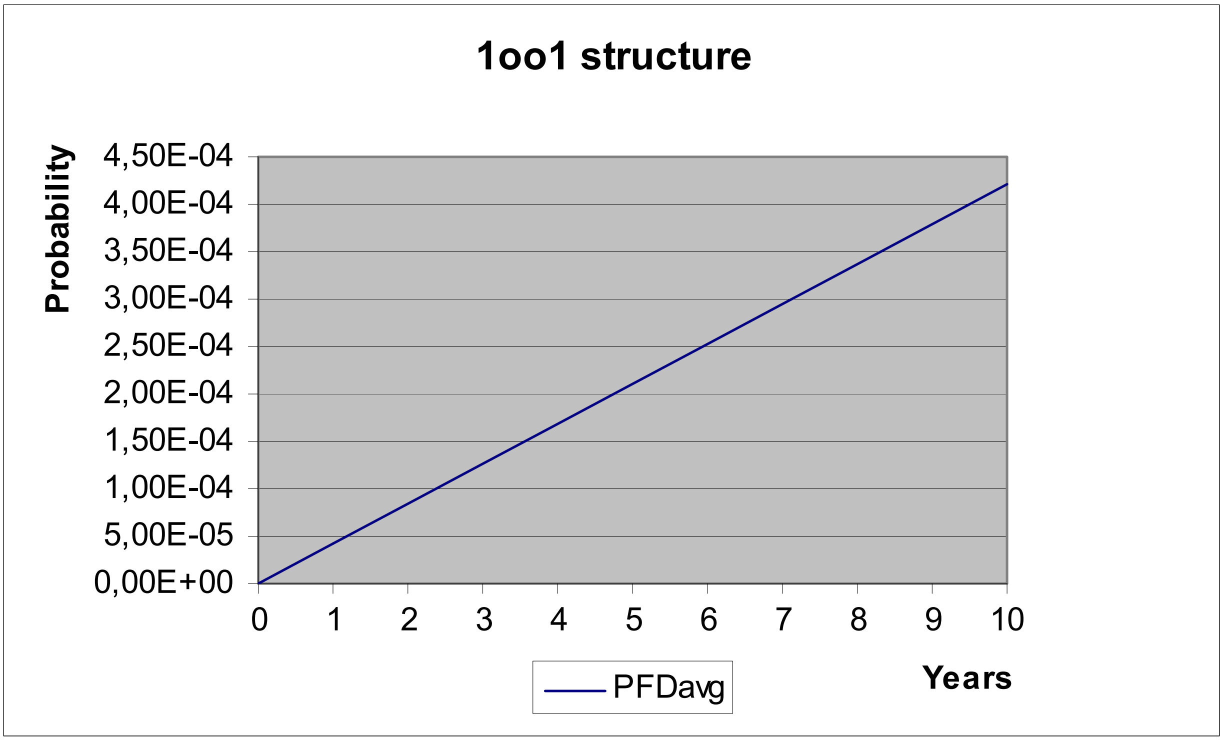


Figure 13: PFD_{AVG}(t) of V5 in standard application

5.5.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V5 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,24E-08 1/h + 2,56E-09 1/h = 2,49E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,50E-08 1/h

SFF = 99,64%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 14 shows the time dependent curve of PFD_{AVG}.

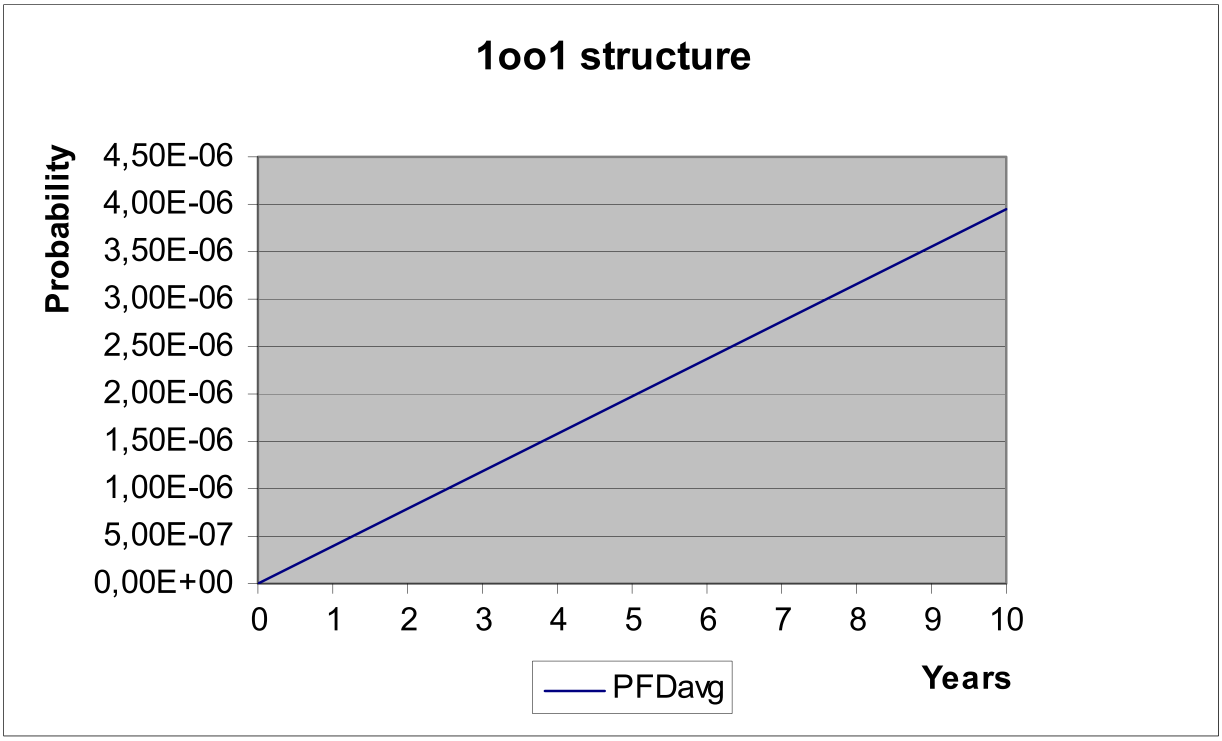


Figure 14: PFD_{AVG}(t) of V5 in applications with (Pepperl+Fuchs) fail safe interface

5.6 Version V6

5.6.1 Standard application

The FMEDA carried out on the sensors called version V6 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{safe} = λ_{safe} + $\lambda_{don't\ care}$ = 1,43E-08 1/h + 4,74E-09 1/h = 1,91E-08 1/h

$\lambda_{dangerous}$ = 1,07E-08 1/h

λ_{total} = 2,97E-08 1/h

SFF = 64,14%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.66E-05	**PFD_{AVG} = 9.33E-05**	**PFD_{AVG} = 2.33E-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 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 15 shows the time dependent curve of PFD_{AVG}.

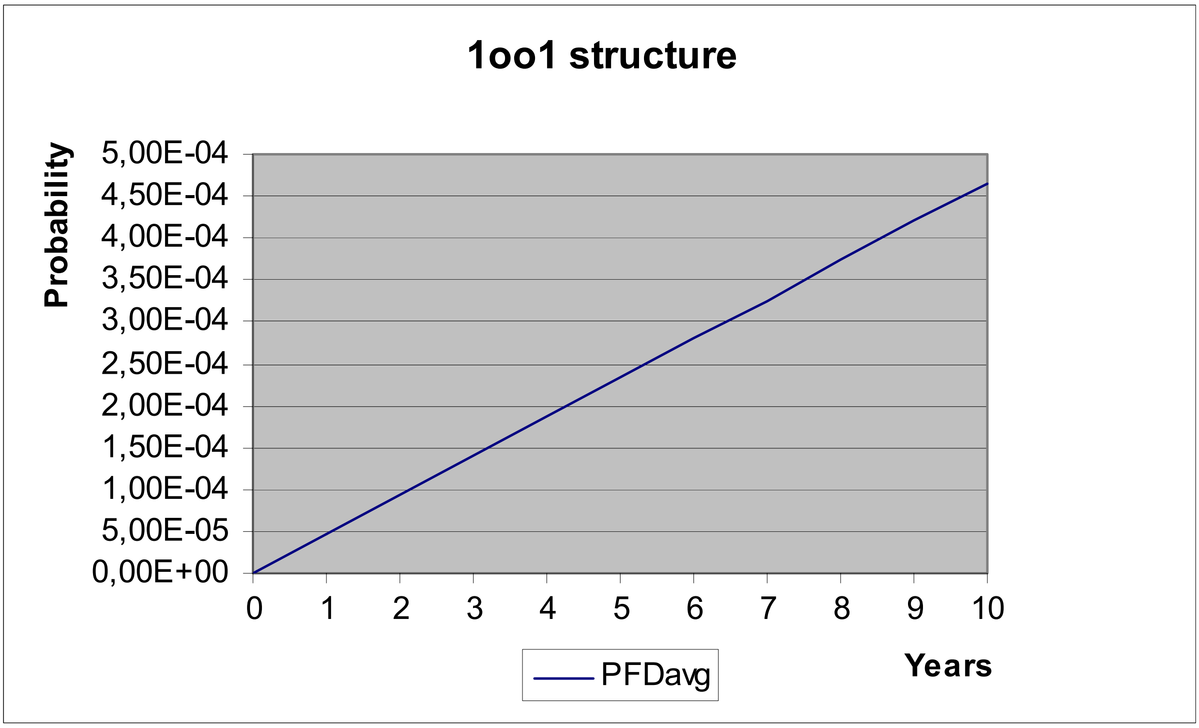


Figure 15: PFD_{AVG}(t) of V6 in standard application

5.6.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V6 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,49E-08 1/h + 4,74E-09 1/h = 2,96E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,97E-08 1/h

SFF = 99,70%

The PFD$_{AVG}$ was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD$_{AVG}$ = 3.94E-07	**PFD$_{AVG}$ = 7.88E-07**	**PFD$_{AVG}$ = 1.97E-06**

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 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 16 shows the time dependent curve of PFD$_{AVG}$.

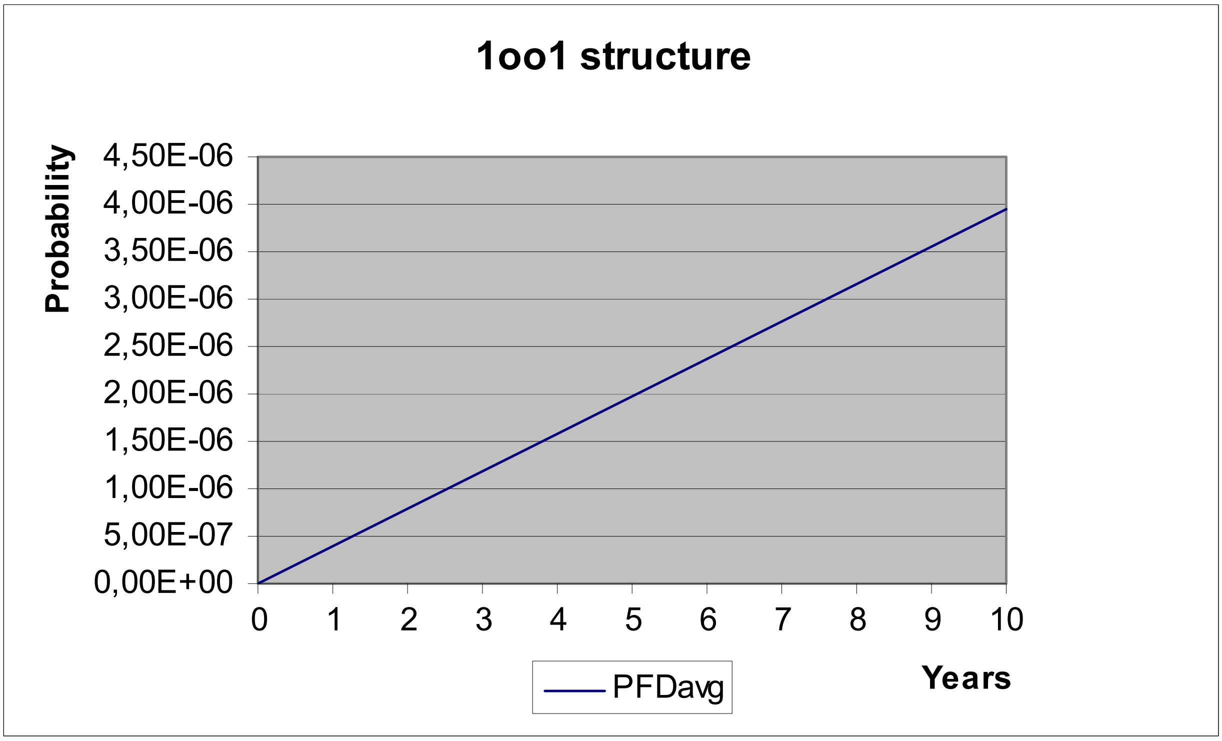


Figure 16: PFD$_{AVG}$(t) of V6 in applications with (Pepperl+Fuchs) fail safe interface

5.7 Version V7

5.7.1 Standard application

The FMEDA carried out on the sensors called version V7 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,43E-08 1/h + 4,74E-09 1/h = 1,91E-08 1/h

$\lambda_{dangerous}$ = 1,07E-08 1/h

λ_{total} = 2,97E-08 1/h

SFF = 64,14%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.66E-05	**PFD_{AVG} = 9.33E-05**	**PFD_{AVG} = 2.33E-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 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 17 shows the time dependent curve of PFD_{AVG}.

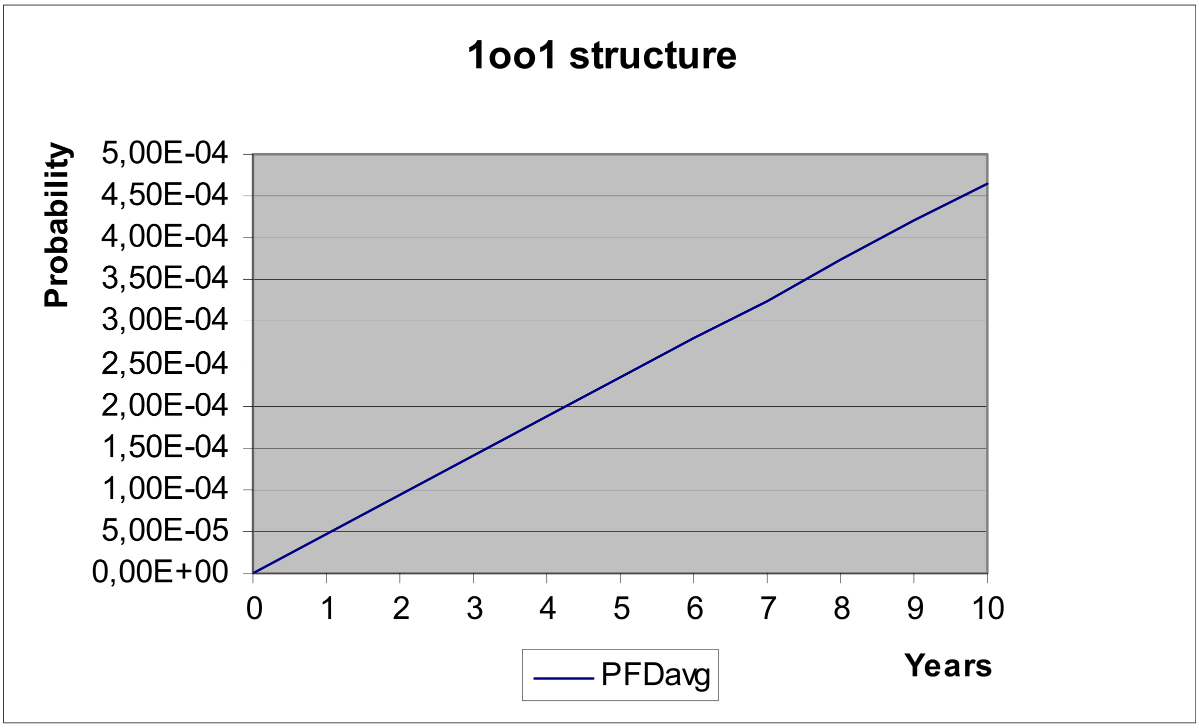


Figure 17: PFD_{AVG}(t) of V7 in standard application

5.7.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V7 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,49E-08 1/h + 4,74E-09 1/h = 2,96E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,97E-08 1/h

SFF = 99,70%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 18 shows the time dependent curve of PFD_{AVG}.

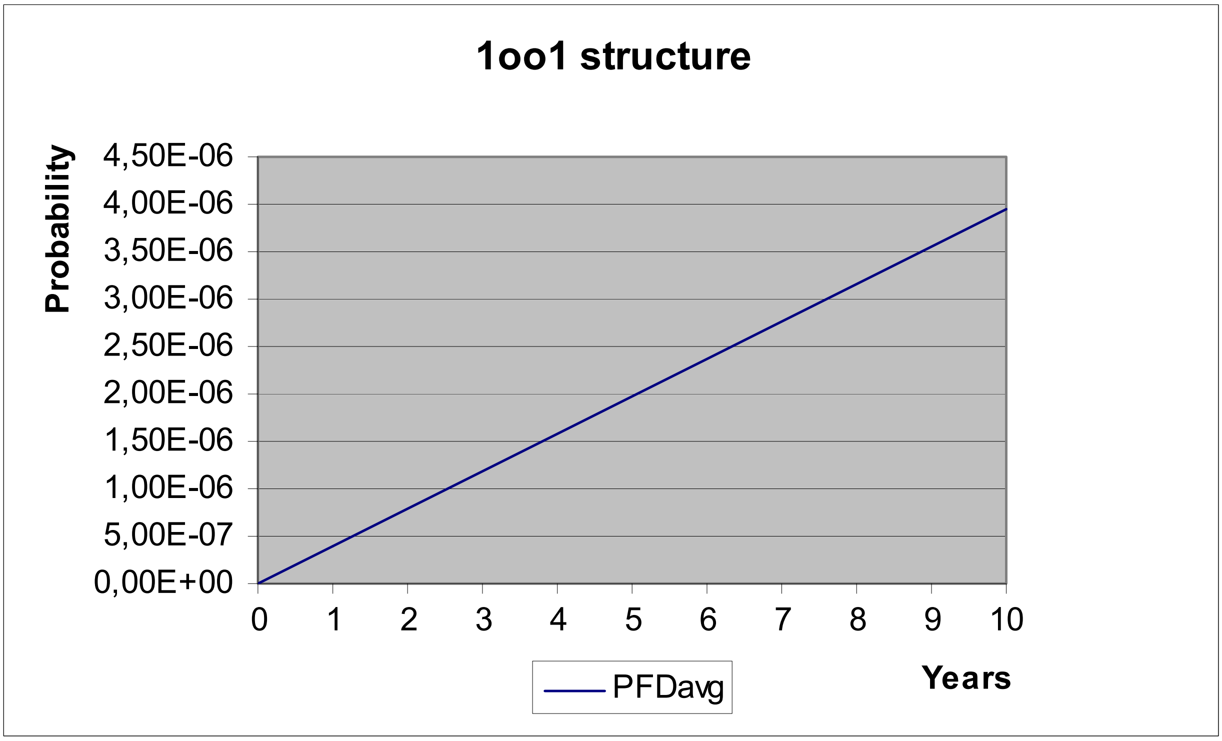


Figure 18: PFD_{AVG}(t) of V7 in applications with (Pepperl+Fuchs) fail safe interface

5.8 Version V8

5.8.1 Standard application

The FMEDA carried out on the sensors called version V8 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,28E-08 1/h + 2,56E-09 1/h = 1,54E-08 1/h

$\lambda_{dangerous}$ = 9,63E-09 1/h

λ_{total} = 2,50E-08 1/h

SFF = 61,48%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.22E-05	PFD_{AVG} = 8.44E-05	PFD_{AVG} = 2.11E-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 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 19 shows the time dependent curve of PFD_{AVG}.

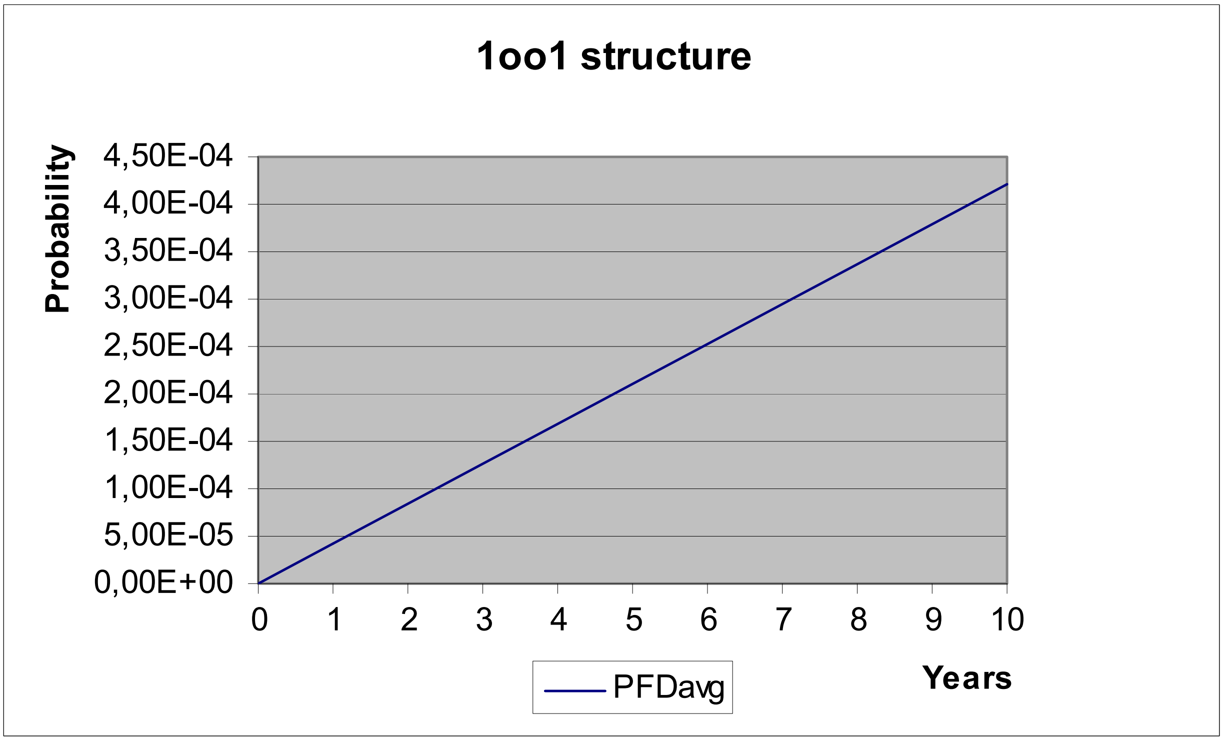


Figure 19: PFD_{AVG}(t) of V8 in standard application

5.8.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V8 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,24E-08 1/h + 2,56E-09 1/h = 2,49E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,50E-08 1/h

SFF = 99,64%

The PFD$_{AVG}$ was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD$_{AVG}$ = 3.94E-07	**PFD$_{AVG}$ = 7.88E-07**	**PFD$_{AVG}$ = 1.97E-06**

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 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 20 shows the time dependent curve of PFD$_{AVG}$.

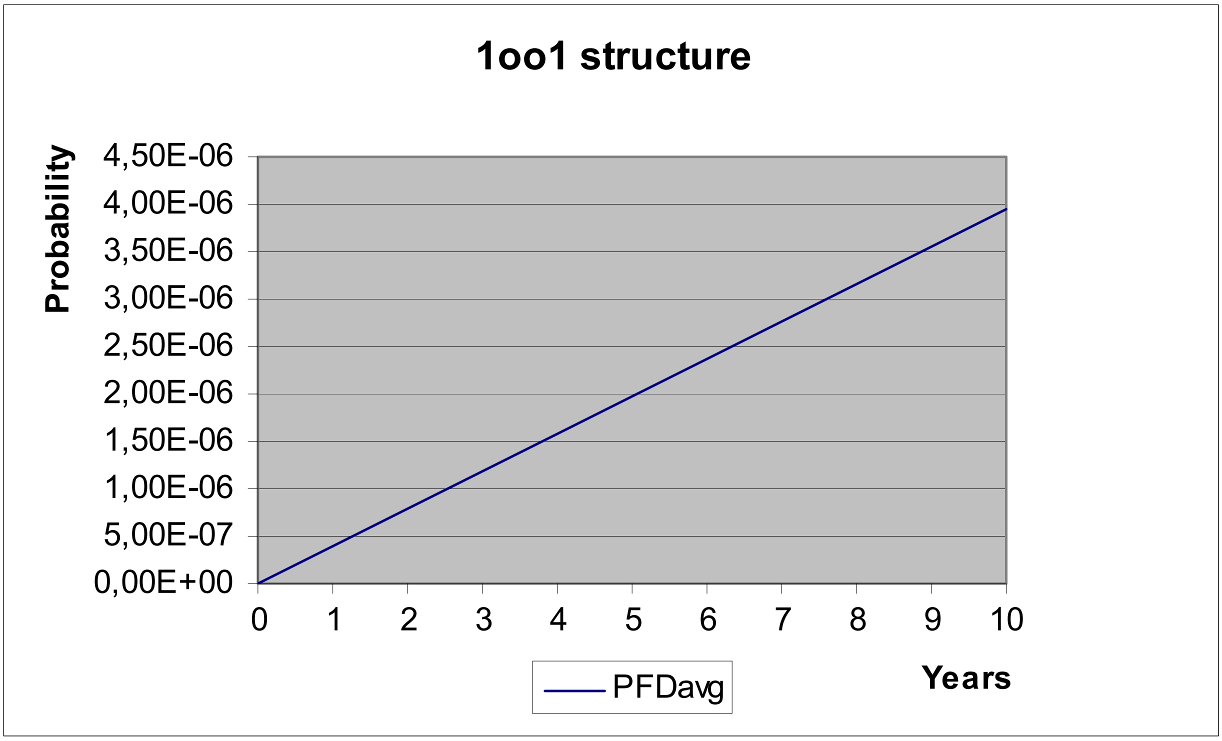


Figure 20: PFD$_{AVG}$(t) of V8 in applications with (Pepperl+Fuchs) fail safe interface

5.9 Version V9

5.9.1 Standard application

The FMEDA carried out on the sensors called version V9 in standard applications, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 1,43E-08 1/h + 4,74E-09 1/h = 1,91E-08 1/h

$\lambda_{dangerous}$ = 1,07E-08 1/h

λ_{total} = 2,97E-08 1/h

SFF = 64,14%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.66E-05	PFD_{AVG} = 9.33E-05	PFD_{AVG} = 2.33E-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 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 21 shows the time dependent curve of PFD_{AVG}.

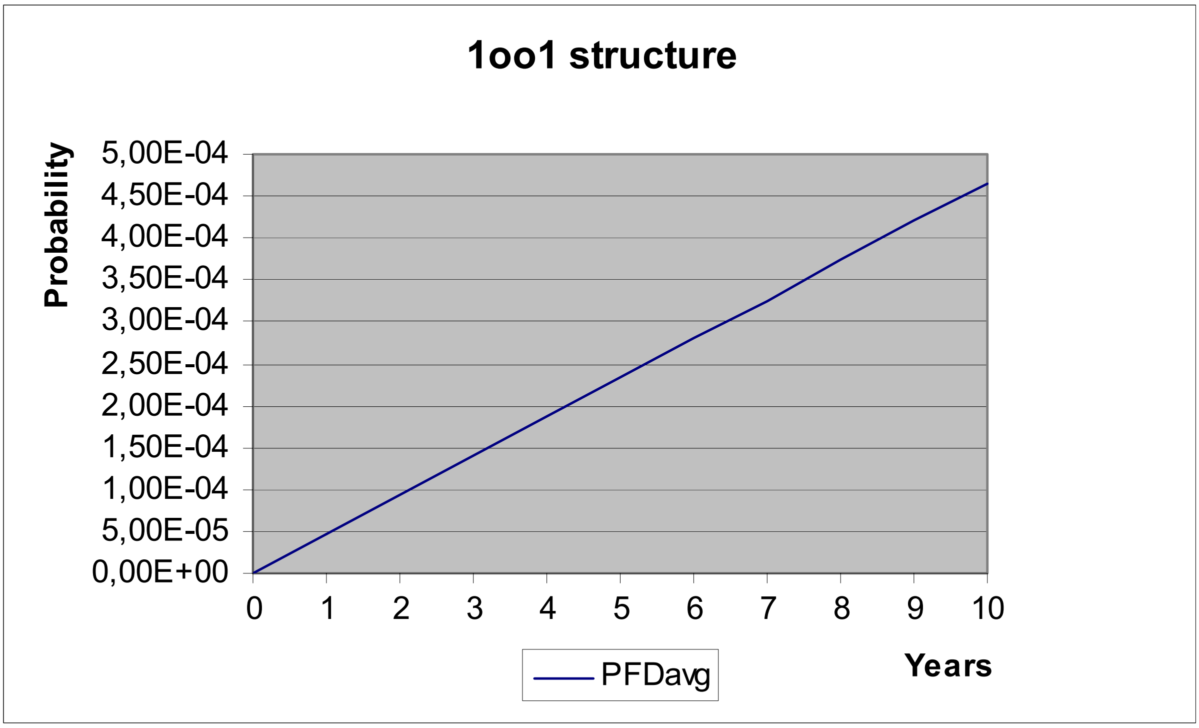


Figure 21: $PFD_{AVG}(t)$ of V9 in standard application

5.9.2 Application with (Pepperl+Fuchs) fail safe interface

The FMEDA carried out on the sensors called version V9 in applications with a (Pepperl+Fuchs) fail safe interface, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$\lambda_{safe} = \lambda_{safe} + \lambda_{don't\ care}$ = 2,49E-08 1/h + 4,74E-09 1/h = 2,96E-08 1/h

$\lambda_{dangerous}$ = 9,00E-11 1/h

λ_{total} = 2,97E-08 1/h

SFF = 99,70%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-07	**PFD_{AVG} = 7.88E-07**	**PFD_{AVG} = 1.97E-06**

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 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 22 shows the time dependent curve of PFD_{AVG}.

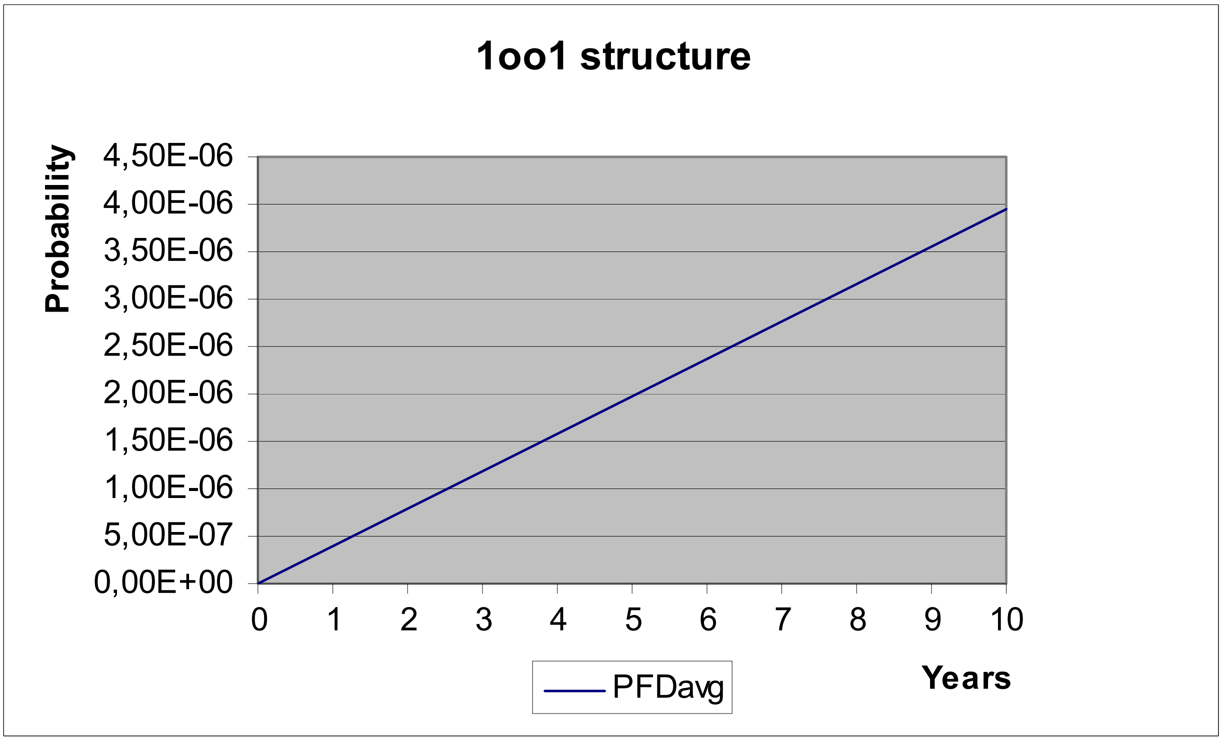


Figure 22: PFD_{AVG}(t) of V9 in applications with (Pepperl+Fuchs) fail safe interface

6 Proven-in-use Assessment

6.1 Definition of the term “Proven-in-use” according to IEC 61508

Reference: IEC 61508-7; B.5.4

Aim: To use field experience from different applications to prove that the safety-related system will work according to its specification.

Description: Use of components or subsystems, which have been shown by experience to have no, or only unimportant, faults when used, essentially unchanged, over a sufficient period of time in numerous different applications.

For proven by use to apply, the following requirements must have been fulfilled:

- unchanged specification;
- 10 systems in different applications;
- 10^5 operating hours and at least 1 year of service history.

The proof is given through documentation of the vendor and/or operating company. This documentation must contain at least the:

- exact designation of the system and its component, including version control for hardware;
- users and time of application;
- operating hours;
- procedures for the selection of the systems and applications procured to the proof;
- procedures for fault detection and fault registration as well as fault removal.

6.2 “Prior-use” requirements according to IEC 61511-1

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

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

Table 6 of IEC 61511-1 First Edition 2003-01
(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 First Edition 2003-01 are fulfilled a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with a SFF of 60% to < 90%[7].

This is identical to the requirements on Type A (sub)-systems. The NAMUR sensors have been developed without considering IEC 61508, however, and so IEC 61511-1 First Edition 2003-01 section 11.4.4 is used as a basis for arguing that proven-in-use shows the unlikelihood of systematic failures.

The assessment of the NAMUR sensors has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

[7] IEC 61511-1 First Edition 2003-01 explicitly says “…provided that the dominant failure mode is to the safe state or dangerous failures are detected…”.

Requirement	Argumentation[8]
See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 5 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail[9] is low (<0,3%). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See D10 to D12. The assessed sub-system are clearly identified and specified (see Table 1). The field feedback tracking database of Pepperl+Fuchs GmbH together with the explanations given in D13 to D15 demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience. The following operating experience exist: V1: More than 136.500.000 operating hours V2: More than 35.500.000 operating hours V3: More than 484.500.000 operating hours V4: More than 2.490.500.000 operating hours V5: More than 210.000.000 operating hours V6: More than 427.500.000 operating hours V7: More than 89.500.000 operating hours V8: More than 118.500.000 operating hours V9: No operating experience because new device This is considered to be sufficient taking into account the low complexity of the sub-systems and the use in SIL 2 safety functions only). 3. 11.5.2 is under the responsibility of the user / manufacturer –> no argumentation. 11.5.3 see bullet items before. 4. N/A 5. Under the responsibility of the user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see D15
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 NAMUR sensors with a SFF of 60% - < 90% and a HFT = 0 can considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

[8] The numbering is based on the requirements detailed in appendix 1.

[9] The probability of failure is the percentage of all returned devices with relevant repair reasons to all sold devices.

7 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 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 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

8 Status of the document

8.1 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.

8.2 Releases

Version:	V1	
Revision:	R1.1	
Version History:	V0, R1.0:	Initial version, Mar. 17, 2004
	V0, R1.1:	Additional information received from P+F added; Apr. 6, 2004
	V1, R1.0:	Review comments integrated; May 18, 2004
	V1, R1.1:	Review comments integrated; July 25, 2004
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com), April 12, 2004
	V0, R1.1:	Michael Wenglorz (Pepperl+Fuchs), May 12, 2004
	V1, R1.0:	Harald Eschelbach (Pepperl+Fuchs), July 20, 2004
Release status:	Released to Pepperl+Fuchs	

8.3 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 First Edition 2003-01

Appendix 1.1 Section 11.5.3 of IEC 61511-1 First Edition 2003-01

(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 First Edition 2003-01

(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 First Edition 2003-01

(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

Appendix 2 shall be considered when writing the safety manual as it contains important safety related information.

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 6 shows a sensitivity analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Table 6: Sensitivity Analysis of “du” failures of version V4 representing the worst case

Component	% of total λ_{du}	Detection through
L1	41,62%	100% functional test with different expected output signals over the entire range
P2	17,17%	100% functional test with different expected output signals over the entire range
P3	17,17%	100% functional test with different expected output signals over the entire range
C3	10,41%	100% functional test with different expected output signals over the entire range
P1	9,37%	100% functional test with different expected output signals over the entire range
Output teminal	2,08%	100% functional test with different expected output signals over the entire range
R3	1,25%	100% functional test with different expected output signals over the entire range
R2	0,52%	100% functional test with different expected output signals over the entire range
R1	0,21%	100% functional test with different expected output signals over the entire range
R4	0,21%	100% functional test with different expected output signals over the entire range

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, 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 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.

The circuits of the NAMUR sensors do 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.