



Failure Modes, Effects and Diagnostic Analysis

Project:

Solenoid Driver KFD2-SL-4 and Safety Relay KFD0-RSH-1(-Y2)

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 01/11-09

Report No.: P+F 01/11-09 R005

Version V3, Revision R1, May 2009

Stephan Aschenbrenner

Management summary

This report summarizes the results of the FMEDAs carried out on the solenoid driver KFD2-SL-4 and the safety relay KFD0-RSH-1(-Y2).

The safety relay KFD0-RSH-1-Y2 is a variant which can be connected to a control signal with periodically repeating High pulses during the OFF-state, Low pulses during the ON-state and a load impedance check.

The failure rates are based on the Siemens standard SN 29500.

According to table 2 / 3 of IEC 61508-1 the PFD_{AVG} / PFH has to be $< 1.00E-03$ / $< 1.00E-07$ 1/h for SIL 3 safety functions and $< 1.00E-02$ / $< 1.00E-06$ 1/h 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 $1.00E-04$ / $1.00E-08$ 1/h for SIL 3 and better than or equal to $1.00E-03$ / $1.00E-07$ 1/h for SIL 2.

The modules under evaluation can be considered to be Type A subsystems.

For **Type A** subsystems the SFF has to fulfill the requirements as stated in table 2 of IEC 61508-2 which are the following:

	Hardware fault tolerance (HFT)		
	0	1	2
SIL 2	$60\% \leq SFF < 90\%$	$SFF < 60\%$	
SIL 3	$90\% \leq SFF < 99\%$	$60\% \leq SFF < 90\%$	$SFF < 60\%$

The following tables show under which conditions the described modules (considering one input and one output being part of the safety function) fulfill this requirement.

Table 1: KFD2-SL-4 with regard to SIL 2 requirements

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = $1.00E-09$ 1/h	$PFD_{AVG} = 4.39E-06$	$PFD_{AVG} = 8.81E-06$	$PFD_{AVG} = 2.22E-05$

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1.00E-03$ or $1.00E-07$ 1/h, respectively. The PFD_{AVG} values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements for SIL 2 which are set by table 2 of IEC 61508-2 for type A subsystems.

Table 2: KFD0-RSH-1(-Y2) (without test pulse) with regard to SIL 3 requirements

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = $4.00E-10$ 1/h	$PFD_{AVG} = 1.75E-06$	$PFD_{AVG} = 3.50E-06$	$PFD_{AVG} = 8.76E-06$

Table 3: KFD0-RSH-1-Y2 (with test pulse) with regard to SIL 3 requirements

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = $4.00E-09$ 1/h	$PFD_{AVG} = 1.75E-05$	$PFD_{AVG} = 3.52E-05$	$PFD_{AVG} = 8.78E-05$

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1.00E-04$ or $1.00E-08$ 1/h, respectively. The PFD_{AVG} / PFH values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements for SIL 3 which are set by table 2 of IEC 61508-2 for type A subsystems.

The four channels on the KFD2-SL-4 module should not be used for one safety function as they contain common components.

A user of the Pepperl+Fuchs solenoid driver or safety relay can utilize the failure rates given in sections 5.1 to 5.3 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 failure rates are valid for the useful lifetime of the solenoid driver KFD2-SL-4 and the safety relay KFD0-RSH-1(-Y2) (see Appendix 1).

It is important to realize that the “don’t care” failures are included in the “safe” failure category according to IEC 61508:2000. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.



Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved.....	6
2.3 Standards / Literature used.....	6
2.4 Reference documents.....	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida</i>	7
3 Description of the analyzed modules	8
3.1 KFD2-SL-4	8
3.2 KFD0-RSH-1.....	9
3.3 KFD0-RSH-1-Y2	10
4 Failure Modes, Effects, and Diagnostics Analysis	11
4.1 Description of the failure categories.....	11
4.2 Methodology – FMEDA, Failure rates.....	11
4.2.1 FMEDA.....	11
4.2.2 Failure rates	11
4.2.3 Assumptions.....	12
5 Results of the assessment.....	12
5.1 KFD2-SL-4	16
5.2 KFD0-RSH-1.....	18
5.3 KFD0-RSH-1-Y2	20
6 Terms and Definitions.....	22
7 Status of the document.....	23
7.1 Liability.....	23
7.2 Releases	23
7.3 Release Signatures.....	23
Appendix 1: 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* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This report shall describe the results of the FMEDAs carried out on the solenoid driver KFD2-SL-4 and the safety relay KFD0-RSH-1.

It shall be assessed whether these modules meet the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements for SIL 2 / SIL 3 sub-systems according to IEC 61508.

The assessment **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a partnership company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl+Fuchs Manufacturer of the solenoid driver and the safety relay.

exida Did the FMEDAs together with the determination of the Safe Failure Fraction (SFF) and calculated the average Probability of Failure on Demand (PFD_{AVG}) using Markov models.

Pepperl+Fuchs GmbH contracted *exida* in December 2001 and June 2006 with the FMEDA and PFD calculation of the above mentioned modules.

2.3 Standards / Literature used

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

N1	IEC 61508-2:1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N3	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N4	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	10.09.01	Bloc diagram for KFD2-SL-4
[D2]	01-5313A of 03.09.01	Circuit diagram for KFD2-SL-4
[D3]	112730 of 12.11.01	Bill of material for KFD2-SL-4
[D4]	KFD0-RSH-1-106793 of 04.09.00	Circuit diagram for KFD0-RSH-1
[D5]	Schaltbild RSH Tricon 01-8436A (incl load test).pdf	Circuit diagram "01-8436A" of 20.02.09 for KFD0-RSH-1-Y2
[D6]	215438_PDP520.pdf	Bill of material for KFD0-RSH-1-Y2
[D7]	WG invensis RSH Exida-Nachtrag R005.msg of 25.03.09	Description of hardware changes
[D8]	FS_Impact Analysis RSH-Y2.doc	Impact analysis regarding changes in KFD0-RSH-1-Y2 FS-0028PF-25 of 17.04.09

2.4.2 Documentation generated by exida

[R1]	FMEDA KFD2-SL-4 Relays V1 R1.0 – Results of 04.03.02
[R2]	FMEDA KFD2-SL-4 Relays V1 R1.0 – Analysis of 04.03.02
[R3]	FMEDA KFD2-SL-4 V1 R1.0 – Results of 04.03.02
[R4]	FMEDA KFD2-SL-4 V1 R1.0 – Analysis of 04.03.02
[R5]	FMEDA KFD0-RSH-1 Relays V1 R1.0 – Results of 04.03.02
[R6]	FMEDA KFD0-RSH-1 Relays V1 R1.0 – Analysis of 04.03.02
[R7]	FMEDA KFD0-RSH-1 V1 R1.0 – Results of 04.03.02
[R8]	FMEDA KFD0-RSH-1 V1 R1.0 – Analysis of 04.03.02
[R9]	FMEDA V6 KFD0-RSH-1-Y V1 R1.0.xls of 31.05.06
[R10]	FMEDA V6 KFD0-RSH-1-Y2 V2R0.xls of 02.05.09
[R11]	FMEDA KFD0-RSH-1 Relays V2R0.xls of 08.04.09

3 Description of the analyzed modules

3.1 KFD2-SL-4

The KFD2-SL-4 solenoid driver module is equipped with 4 channels with common source.

The inputs are protected against reverse polarity.

The device has 4 high side switches with a common external supply.

The maximum output current is 600 mA per channel, if all outputs are in use.

The load can be:

- inductive (for example solenoids)
- resistive
- light-bulbs (power = 10 W)

The maximum delay between input and output is 2 ms.

At the time anyone channel is shortcut- and overload protected. In case of a short circuit the output will switch on/off rapidly (switching mode). When the fault is resolved, the device will go on working in normal mode.

The safety function is defined as the outputs being switched off by the emergency shutdown input.

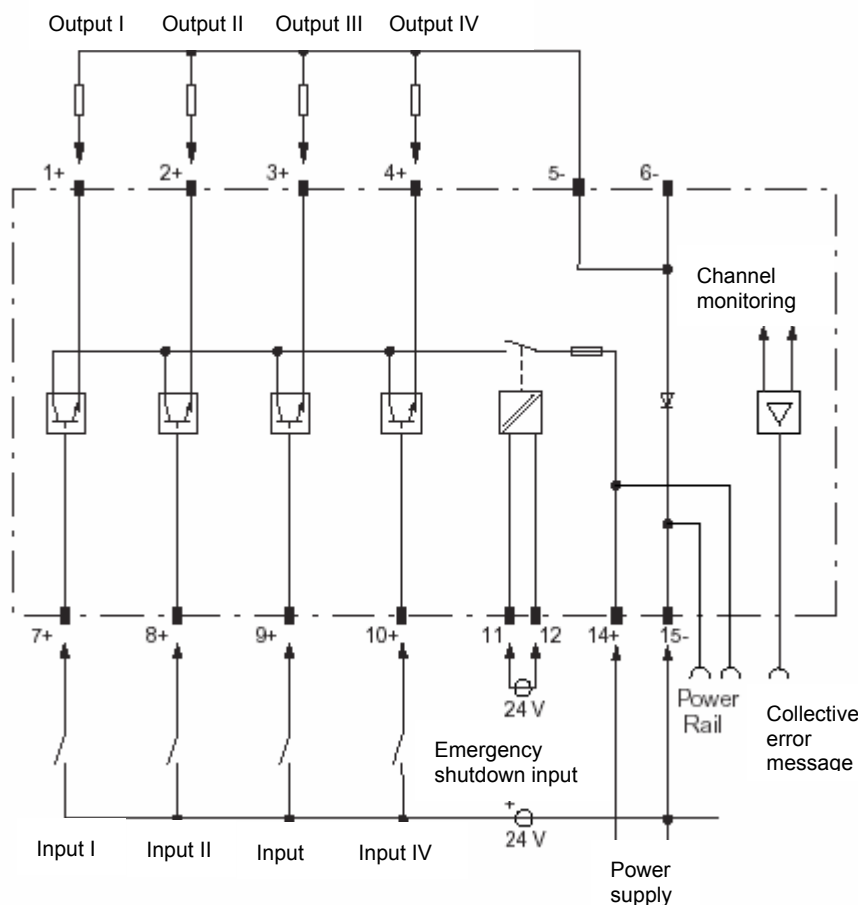


Figure 1: Block diagram of KFD2-SL-4

3.2 KFD0-RSH-1

The KFD0-RSH-1 safety relay module is suitable for safely switching off a control circuit.

The output is safely galvanically isolated from the input up to a nominal voltage of 230 Veff and is protected against contact welding by a fuse.

The three relays are of different design, but have a common effect on the switch output.

The safety function is defined as the output being switched off by de-energizing the logic input.

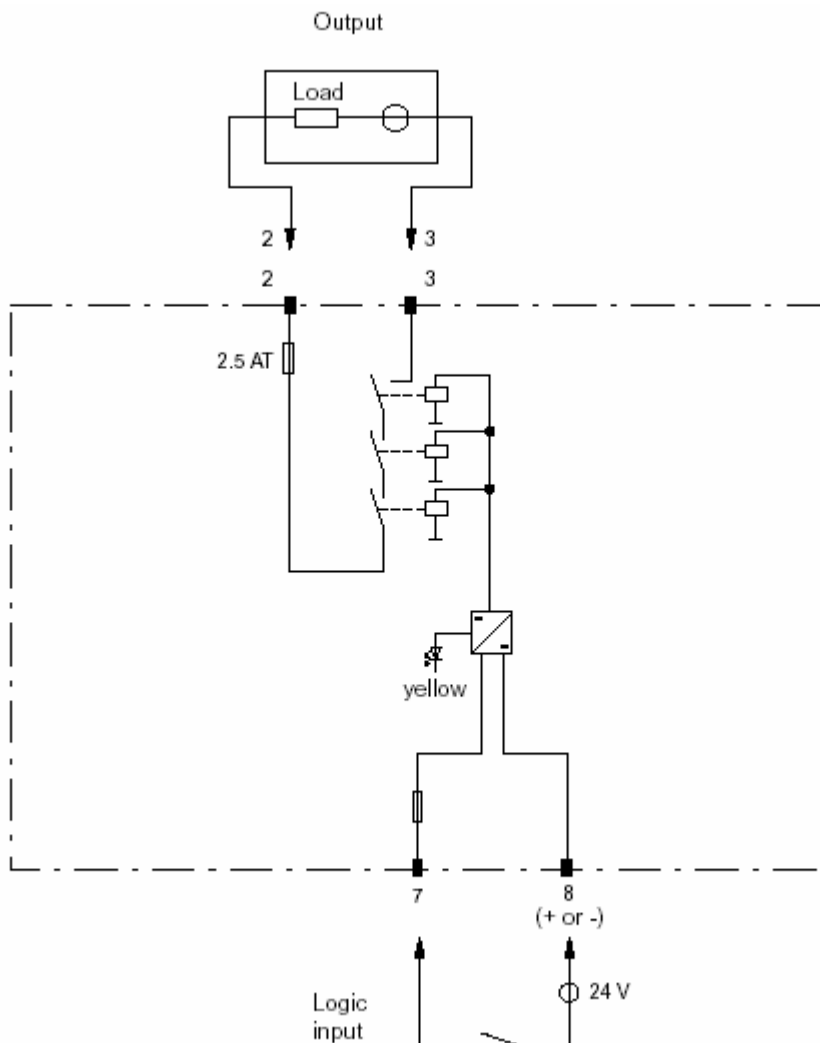


Figure 2: Block diagram of KFD0-RSH-1

3.3 KFD0-RSH-1-Y2

The KFD0-RSH-1-Y2 safety relay module is suitable for safely switching off a control circuit.

The safety relay KFD0-RSH-1-Y2 is a variant which can be connected to a control signal with periodically repeating High pulses during the OFF-state, Low pulses during the ON-state and a load impedance check.

The output is safely galvanically isolated from the input up to a nominal voltage of 230 Veff and is protected against contact welding by a fuse.

The three relays are of different design, but have a common effect on the switch output.

The safety function is defined as the output being switched off by de-energizing the logic input.

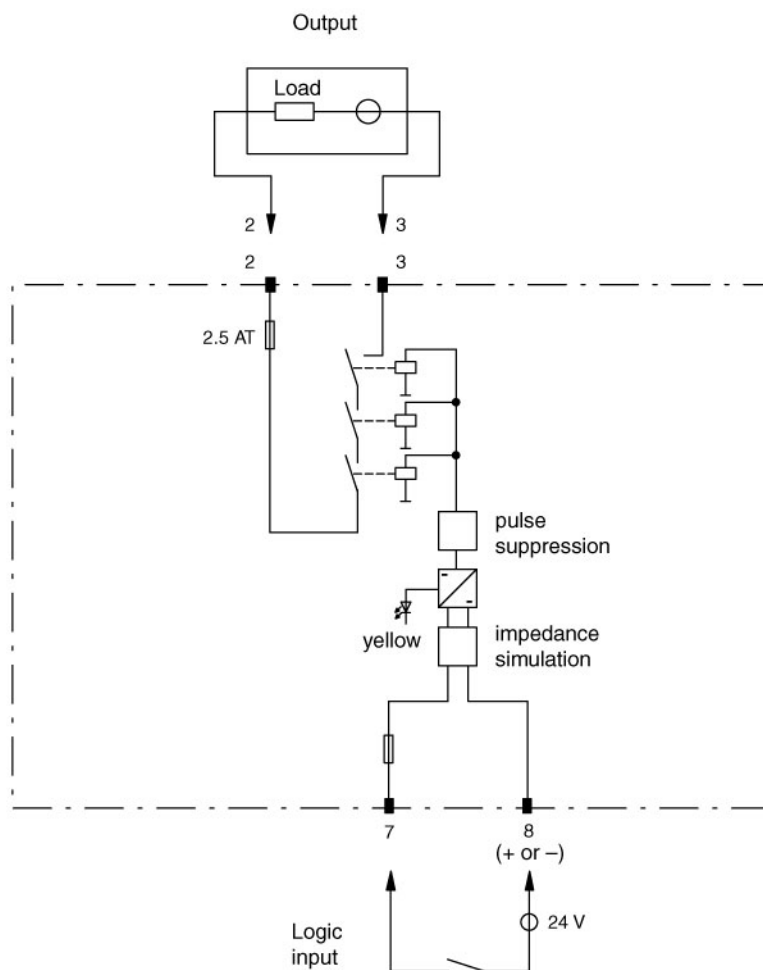


Figure 3: Block diagram of KFD0-RSH-1-Y2

4 Failure Modes, Effects, and Diagnostics Analysis

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.

A **dangerous** failure (D) 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 “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 of the module / (sub)system.

“Not considered” (!) means that this failure mode was not considered. When calculating the SFF and the PFD this failure mode is divided into 50% safe failures and 50% dangerous undetected failures.

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* 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 60654-1, 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 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the solenoid driver and the safety relay.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All component failure modes are known.
- The repair time after a safe failure is 8 hours.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment.
- External power supply failure rates are not included.
- The relay outputs are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.

5 Results of the assessment

exida did the FMEDAs together with Pepperl+Fuchs.

The four channels on the KFD2-SL-4 module 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:

$$\lambda_{\text{total}} = \lambda_{\text{safe}} + \lambda_{\text{dangerous}} + \lambda_{\text{don't care}}^1 + \lambda_{\text{not considered}}^2.$$

$$\text{SFF} = 1 - \lambda_{\text{du}}^3 / \lambda_{\text{total}}$$

The reason for considering also the “not considered” failure rate for the calculation of the SFF is that the SFF is a measure for the effectiveness of the implemented diagnostic and the percentage of known “safe” failures against all possible component failures.

exida estimated for the PFD_{AVG} calculation the effect of the “not considered” failures as 50% “safe” failures and 50% “dangerous” failures.

¹ These are all failures that have no impact on the safety function. The behavior of the system is neither dangerous nor safe.

² This is the failure rate of failure modes that were not considered.

³ This is the failure rate of all dangerous undetected failures plus 50% of the “non considered” failures.

For the KFD2-SL-4 module and the KFD0-RSH-1 module the shut-down path is carried out redundant. Therefore each module was split into two separate subsystems. One representing the power supply and additional electronic having a hardware fault tolerance of 0 and one representing the shut-down path having a hardware fault tolerance of 1 or 2. This separation is illustrated in Figure 4 and Figure 5.

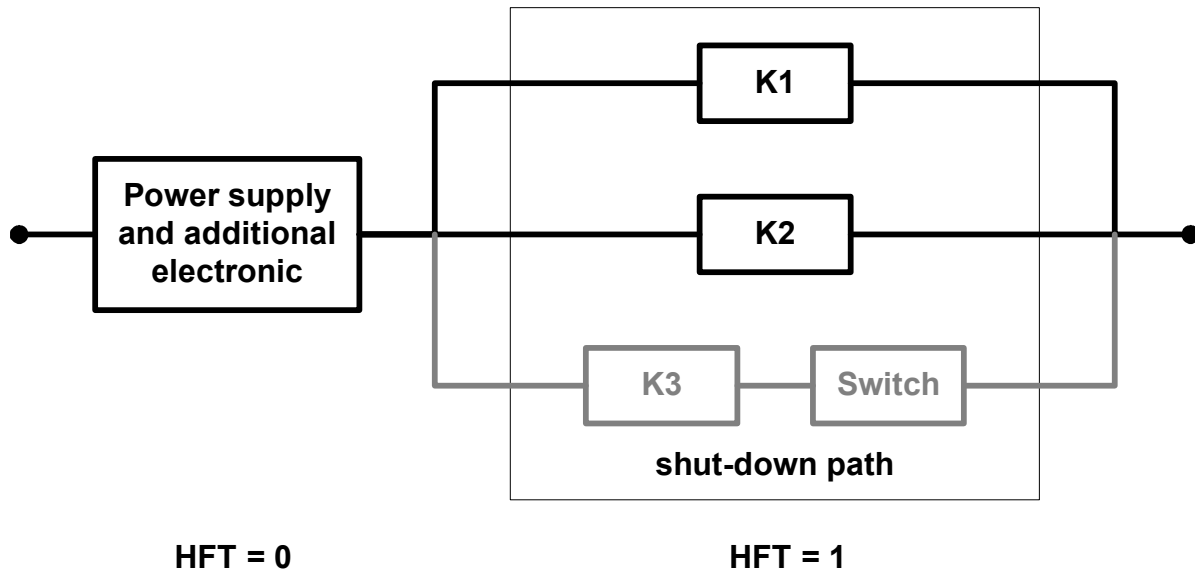


Figure 4: Separation of KFD2-SL-4 into two subsystems

The shutdown path of the KFD2-SL-4 module actually has a hardware fault tolerance of 2, as the output cannot only be disabled by K1 or K2 but also by K3 and the high side switch. However the high side switch is considered to be a Type B subsystem according to IEC 61508 which requires a HFT of 2 to achieve SIL 2 with SFF < 60%. The same can be achieved for Type A subsystems with a HFT of 1. Therefore the analysis was done by putting the third shutdown path (K3 and switch) together with “Power supply and additional electronic” and only considering the shutdown path consisting of K1 and K2 with a HFT of 1.

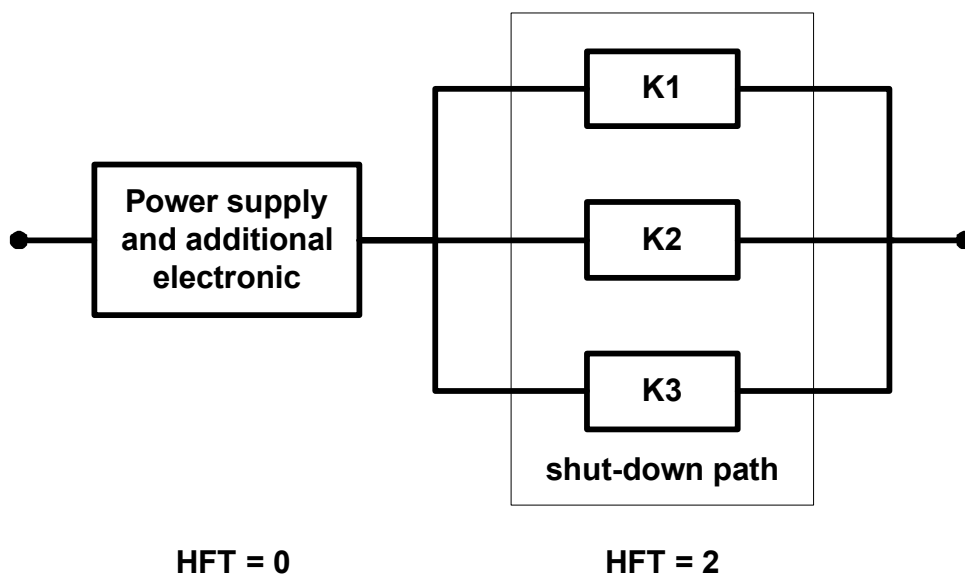


Figure 5: Separation of KFD0-RSH-1 into two subsystems

For the calculation of the PFD_{AVG} the following Markov models for a 1oo1, 1oo2 and 1oo3 architecture were used. As there are no explicit on-line diagnostics, no state “dd” – dangerous detected is required. As after a complete proof all states are going back to the OK state no proof rate is shown in the Markov models but included in the calculation.

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

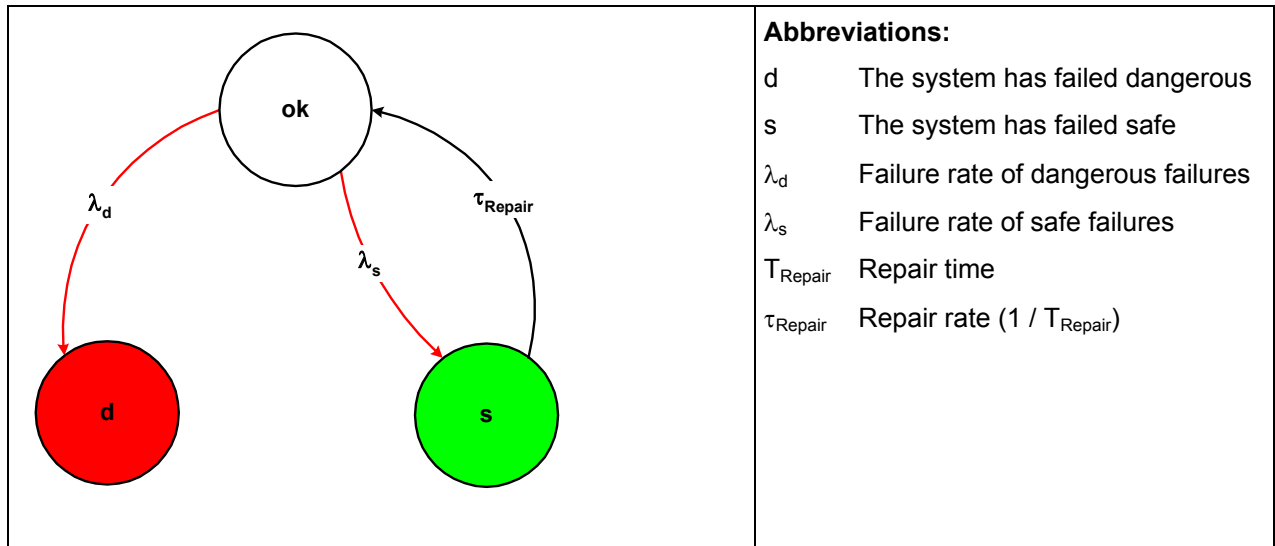


Figure 6: Markov model for a 1oo1 architecture

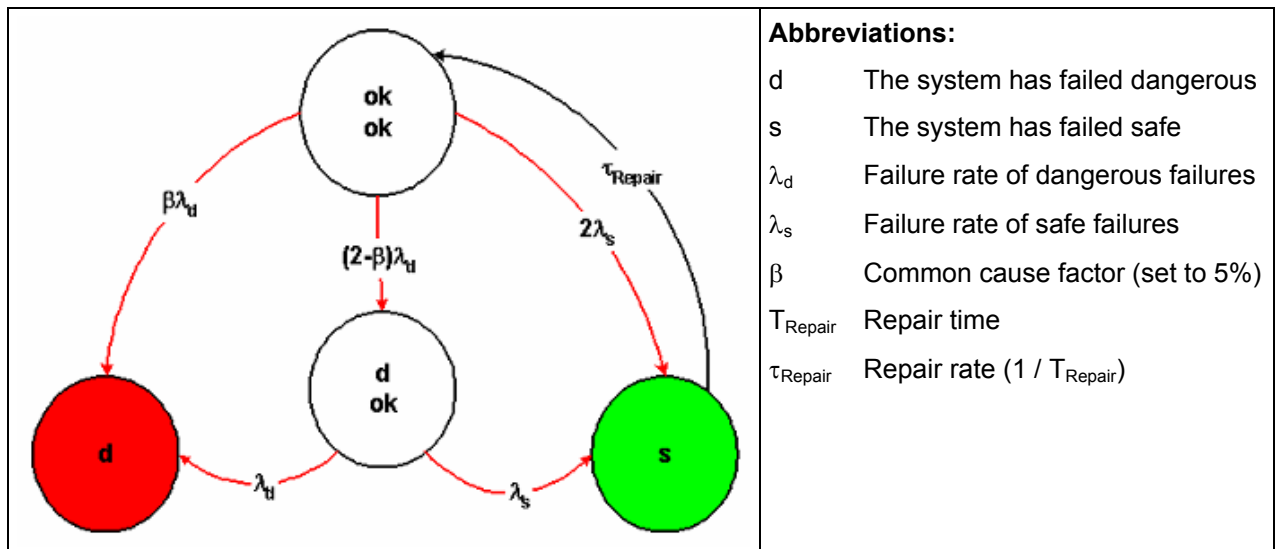
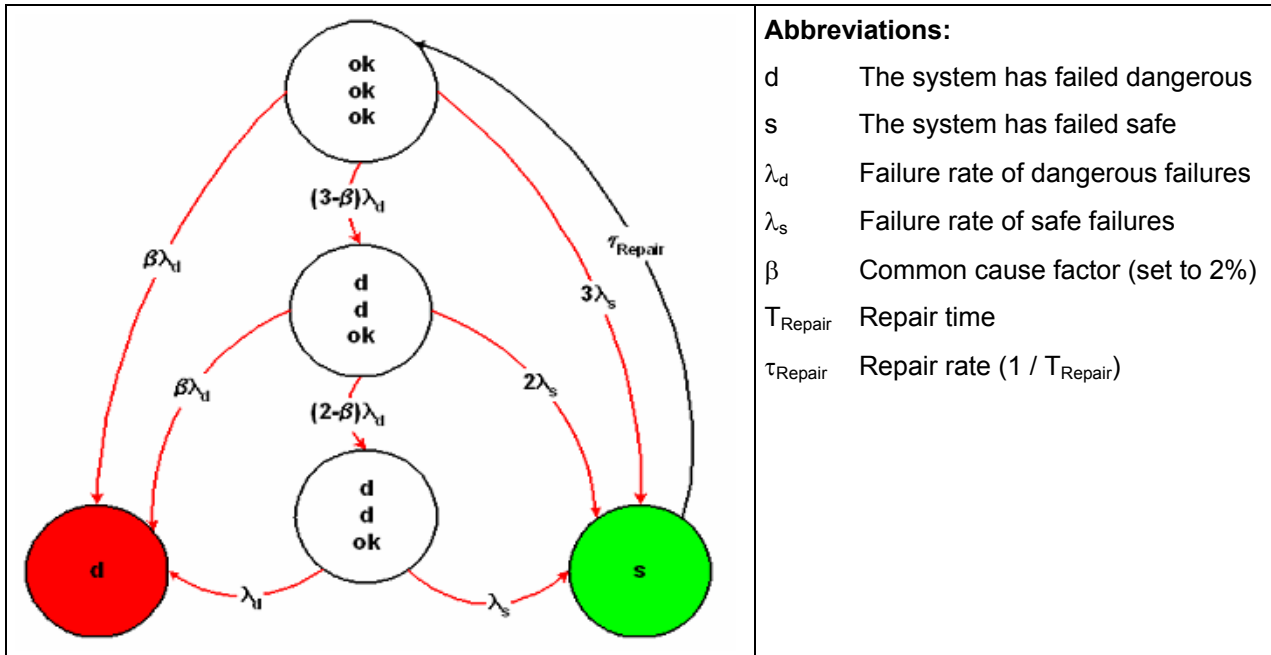


Figure 7: Markov model for a 1oo2 architecture



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
- β Common cause factor (set to 2%)
- T_{Repair} Repair time
- τ_{Repair} Repair rate ($1 / T_{\text{Repair}}$)

Figure 8: Markov model for a 1oo3 architecture

5.1 KFD2-SL-4

The FMEDA carried out on the KFD2-SL-4 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

Power supply and additional electronic:

$$\lambda_{\text{total}} = 2,25\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 6,38\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 1,61\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 100,00\% \text{ (HFT} = 0)$$

NOTE: As all faults of the power supply and the additional electronic will either contribute to λ_{safe} or $\lambda_{\text{don't care}}$ the failure modes of the different components were not explicitly analyzed. Thus “don't care” failures could also be “safe” failures and vice versa. According to the definition in the beginning of this section this does not have any impact on the SFF.

Because no dangerous failures are possible the $\text{PFD}_{\text{AVG}} = 0$ for this sub-system.

Shutdown path (consisting of K1 and K2):

$$\lambda_{\text{total}} = 5,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 3,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 60,00\% \text{ (HFT} = 1)$$

NOTE: The failure rates are the ones of one channel (here one relay).

The PFD was calculated for three different proof times using the Markov model as described in Figure 7.

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1.00E-09 1/h	PFD_{AVG} = 4.39E-06	PFD_{AVG} = 8.81E-06	PFD_{AVG} = 2.22E-05

The boxes marked in green () mean that the calculated $\text{PFD}_{\text{AVG}} / \text{PFH}$ values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1.00\text{E-}03$ or $1.00\text{E-}07 \text{ 1/h}$, respectively. The PFD_{AVG} values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements for SIL 2 which are set by table 2 of IEC 61508-2 for type A subsystems.

The following figure shows the result of the PFD_{AVG} calculation for $\beta = 5\%$ (maximum common cause factor for a logic sub-system according to IEC 61508-6).

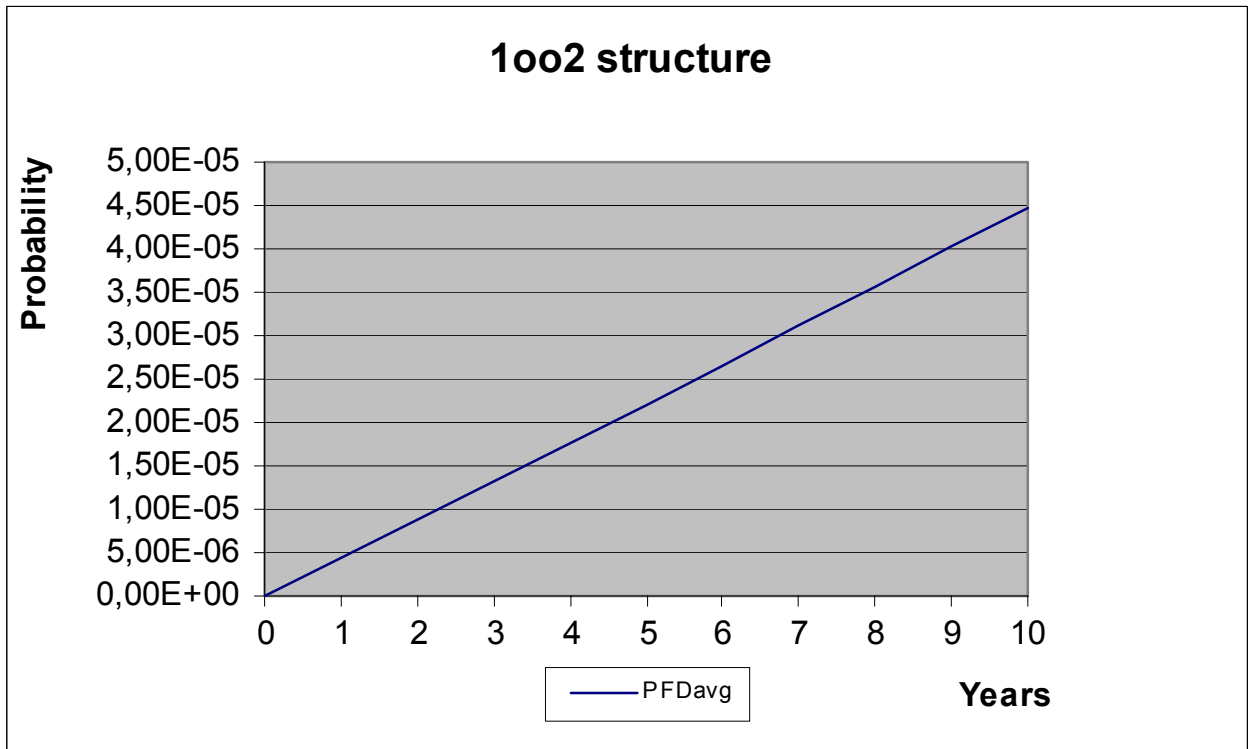


Figure 9: PFD_{AVG}(t)

The PFD_{AVG} / PFH value for the KFD2-SL-4 solenoid driver module is the sum of the two PFD_{AVG} / PFH values for the two sub-systems. As the PFD_{AVG} / PFH value for the first sub-system is zero the PFD_{AVG} / PFH value for the KFD2-SL-4 solenoid driver module is given by the second sub-system which is shown above.

5.2 KFD0-RSH-1

The FMEDA carried out on the KFD0-RSH-1 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

Power supply and additional electronic:

$$\lambda_{\text{total}} = 1,02\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 3,23\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 6,96\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 100,00\% \text{ (HFT} = 0)$$

Because no dangerous failures are possible the $\text{PFD}_{\text{AVG}} = 0$ for this sub-system.

Shutdown path (consisting of REL1, REL2 and REL3):

$$\lambda_{\text{total}} = 5,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 3,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 60,00\% \text{ (HFT} = 2)$$

NOTE: The failure rates are the ones of one channel (here one relay).

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 8.

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 4.00E-10 1/h	PFD_{AVG} = 1.75E-06	PFD_{AVG} = 3.50E-06	PFD_{AVG} = 8.76E-06

The boxes marked in green () mean that the calculated $\text{PFD}_{\text{AVG}} / \text{PFH}$ values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1.00\text{E-}04$ or $1.00\text{E-}08 \text{ 1/h}$, respectively. The $\text{PFD}_{\text{AVG}} / \text{PFH}$ values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements for SIL 3 which are set by table 2 of IEC 61508-2 for type A subsystems.

The following figure shows the result of the PFD_{AVG} calculation for $\beta = 2\%$ (by one step reduced maximum common cause factor for a logic sub-system according to IEC 61508-6 because of diversity of two of the three relays).

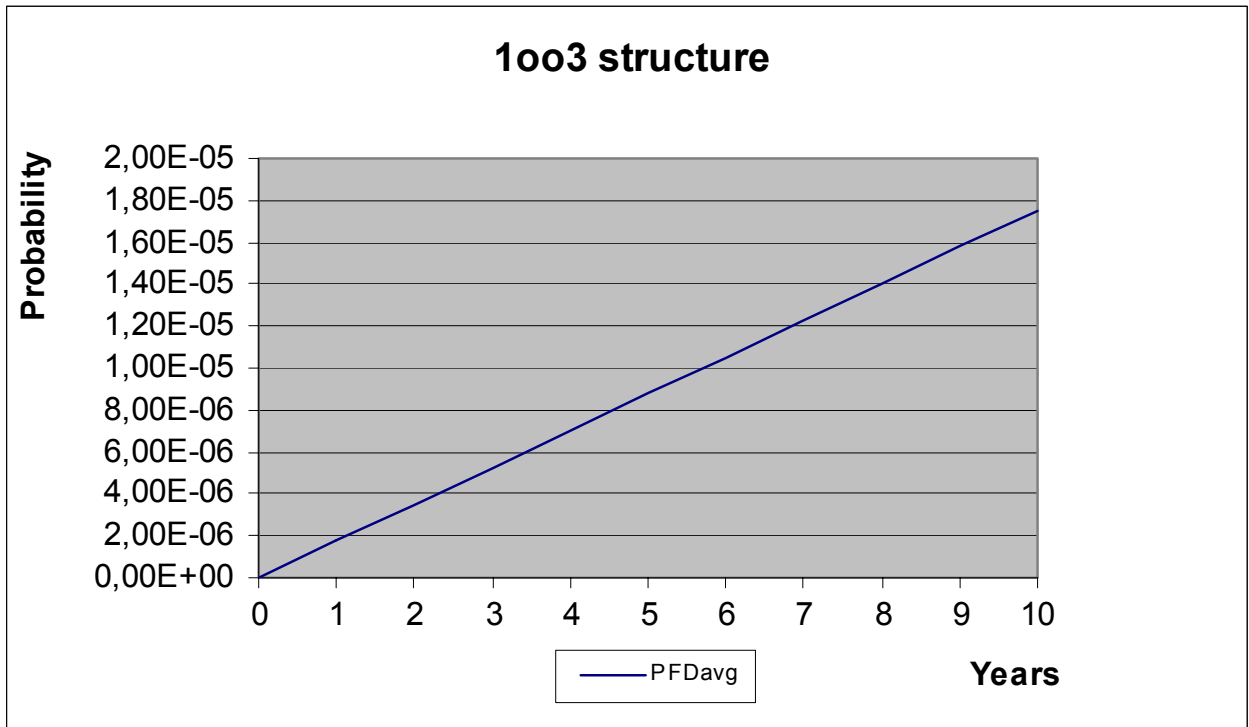


Figure 10: PFD_{AVG}(t)

The PFD_{AVG} / PFH value for the KFD0-RSH-1 safety relay module is the sum of the two PFD_{AVG} / PFH values for the two sub-systems. As the PFD_{AVG} / PFH value for the first sub-system is zero the PFD_{AVG} / PFH value for the KFD0-RSH-1 safety relay module is given by the second sub-system which is shown above.

5.3 KFD0-RSH-1-Y2

The safety relay KFD0-RSH-1-Y2 is a variant which can be connected to a control signal with periodically repeating High pulses during the OFF-state, Low pulses during the ON-state and a load impedance check.

The FMEDA carried out on the KFD0-RSH-1-Y2 module (with test pulse) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

Power supply and additional electronic:

$$\lambda_{\text{total}} = 1,09\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 3,20\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 3,98\text{E-}09 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 7,28\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 96,34\% \text{ (HFT} = 0)$$

Shutdown path (consisting of REL1, REL2 and REL3):

$$\lambda_{\text{total}} = 5,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 3,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,00\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 0,00\text{E+}00 \text{ 1/h}$$

$$\text{SFF} = 60,00\% \text{ (HFT} = 2)$$

NOTE: The failure rates are the ones of one channel (here one relay).

The PFD_{AVG} / PFH value for the KFD0-RSH-1-Y2 safety relay module is the sum of the two PFD_{AVG} / PFH values for the two sub-systems.

The PFD_{AVG} was calculated for three different proof times using the Markov models as described in Figure 6 and Figure 8.

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 4.00E-09 1/h	$\text{PFD}_{\text{AVG}} = 1.75\text{E-}05$	$\text{PFD}_{\text{AVG}} = 3.52\text{E-}05$	$\text{PFD}_{\text{AVG}} = 8.78\text{E-}05$

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1.00E-04 or 1.00E-08 1/h, respectively. The PFD_{AVG} / PFH values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements for SIL 3 which are set by table 2 of IEC 61508-2 for type A subsystems. Figure 11 shows the PFD_{AVG} for the first sub-system which is much higher than the one for the second sub-system.

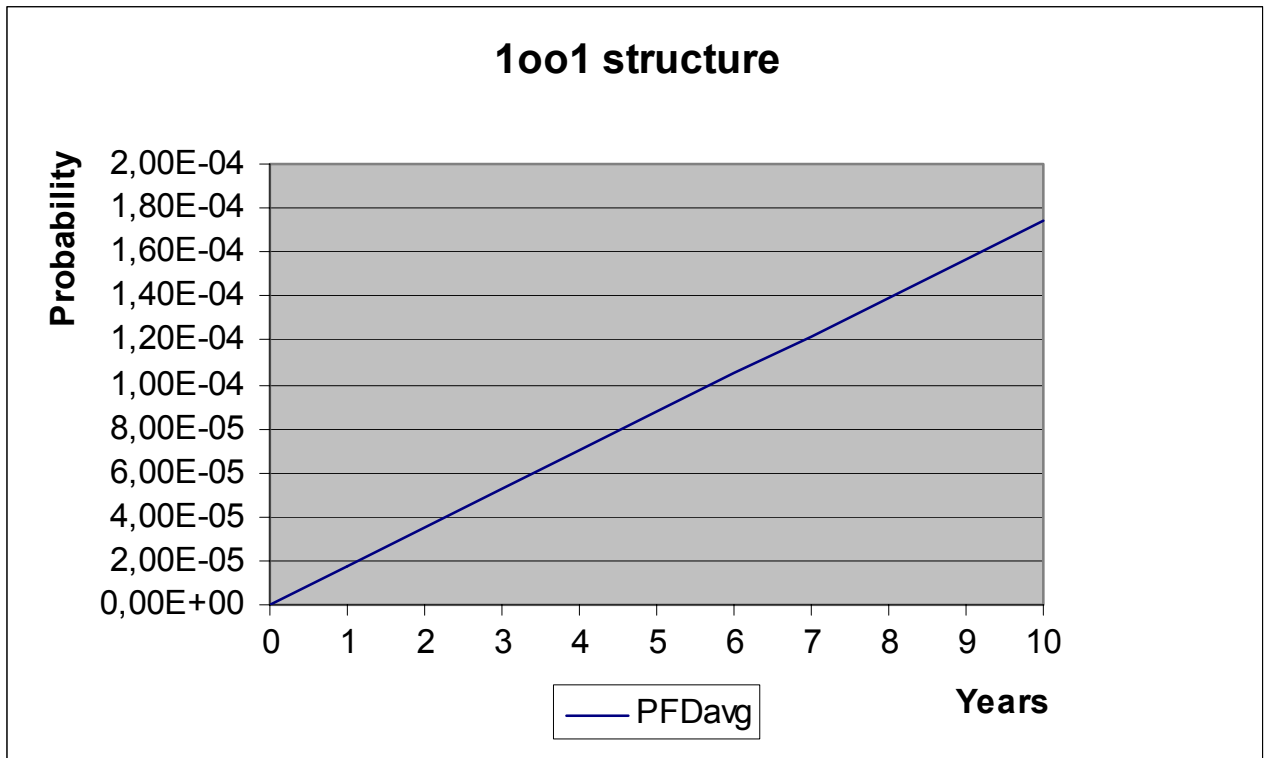


Figure 11: PFD_{AVG}(t)

6 Terms and Definitions

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.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
λ_{total}	Total failure rate λ (overall failure rate of all components)
λ_{safe}	Failure rate λ of all safe failures
$\lambda_{dangerous}$	Failure rate λ of all dangerous failures
λ_{du}	Failure rate λ of dangerous undetected failures
PFD	Probability of Failure on Demand
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

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

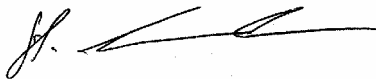
Version History: V3R1: Editorial changes; May 25, 2009
V3R0: Variant KFD0-RSH-1-Y replaced by KFD0-RSH-1-Y2; May 2, 2009
V2, R1.0: Variant KFD0-RSH-1-Y added; June 17, 2006
V1, R1.0: Figure 4 corrected: HFT=1 changed to HFT=2; April 22, 2002
V0, R1.1: Review comments added; March 25, 2002
V0, R1.0: Initial version; March 14, 2002

Authors: Stephan Aschenbrenner

Review: V0, R1.0 by Rainer Faller on March 22, 2002
V0, R1.1 by Harald Eschelbach on April 15, 2002
V3R0 by Harald Eschelbach on May 5, 2009

Release status: Released to Pepperl+Fuchs

7.3 Release Signatures

A handwritten signature in black ink, appearing to be "S. Aschenbrenner", written over a horizontal line.

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

A handwritten signature in black ink, appearing to be "R. Faller", written over a horizontal line.

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

Appendix 1: Impact of lifetime of critical components on the failure rate

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime⁴ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

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

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

Table 4 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 4: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life
Relay	K1, K2 REL1, REL2, REL3	100.000 switching cycles

The relays are the only limiting factor with regard to the useful lifetime of the system.

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime for low demand mode applications but can be the limiting factor for high demand mode applications.

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

⁴ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.