



## **FMEDA including SFF determination and PFD calculation**

Project:  
HART Multiplexer HiD Mux2700 and  
HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16

Customer:  
Pepperl+Fuchs GmbH  
Mannheim  
Germany

Contract No.: P+F 02/4-11  
Report No.: P+F 02/4-11 R006  
Version V2, Revision R0, January 2009  
Stephan Aschenbrenner

## Management summary

This report summarizes the results of the analysis carried out on the HART Multiplexer HiD Mux2700 and HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16.

**The assessment does not contain an evaluation of the correct functioning of the HART Multiplexers but a statement about the interference freeness on the safety related 4..20mA loop when used for HART communication with regard to the suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL).**

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

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be  $\geq 10^{-4}$  to  $< 10^{-3}$  for SIL 3 safety functions and  $\geq 10^{-3}$  to  $< 10^{-2}$  for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to  $10^{-4}$  for SIL 3 and better than or equal to  $10^{-3}$  for SIL 2.

The modules under evaluation can be considered to be Type B components. However, the components that can contribute to a disturbance of the safety system are considered to be Type A components.

For **Type A** components 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	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$	
SIL 3	$90\% \leq \text{SFF} < 99\%$	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$

The following tables show under which conditions the critical components of the two modules that can contribute to a disturbance of the safety system fulfill this requirement (considering only one communication line being part of the safety function).

**Table 1: KFD2-HMM-16 together with KFD0-HMS-16 without additional module interface**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 1.23\text{E-}06$	$\text{PFD}_{\text{AVG}} = 6.13\text{E-}06$	$\text{PFD}_{\text{AVG}} = 1.23\text{E-}05$

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-3}$ . The PFD values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 2 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 0.

If the HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16 is used with the module interface as described in section 4.1 then two de-coupling capacitors have to fail to bring the subsystem into a dangerous state. This corresponds to a hardware fault tolerance of 1.

**Table 2: KFD2-HMM-16 together with KFD0-HMS-16 with additional module interface**

<b>T[Proof] = 1 year</b>	<b>T[Proof] = 5 years</b>	<b>T[Proof] = 10 years</b>
<b>PFD<sub>AVG</sub> = 6.13E-08</b>	<b>PFD<sub>AVG</sub> = 3.07E-07</b>	<b>PFD<sub>AVG</sub> = 6.13E-07</b>

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-4}$ . The PFD values even fulfill the requirements of a higher SIL but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

**Table 3: HART Multiplexer HiD Mux2700**

<b>T[Proof] = 1 year</b>	<b>T[Proof] = 5 years</b>	<b>T[Proof] = 10 years</b>
<b>PFD<sub>AVG</sub> = 2.50E-07</b>	<b>PFD<sub>AVG</sub> = 1.25E-06</b>	<b>PFD<sub>AVG</sub> = 2.50E-06</b>

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-4}$ . The PFD values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

The calculations are based on the assumption that the HART Multiplexers are mounted in an environment that is IP 54 compliant (e.g. housing, control cabinet or control room).

## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	5
2 Project management.....	5
2.1 Roles of the parties involved .....	5
2.2 Standards / Literature used .....	5
2.3 Reference documents .....	6
2.3.1 Documentation provided by the customer.....	6
2.3.2 Documentation generated by <i>exida.com</i> .....	6
3 Description of the HART communication .....	7
4 Description of the analyzed modules .....	8
4.1 HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16 .....	8
4.2 HART Multiplexer HiD Mux2700.....	11
5 Failure Modes, Effects, and Diagnostics Analysis .....	12
5.1 Description of the failure categories .....	12
5.2 Methodology – FMEDA, Failure rates.....	12
5.2.1 FMEDA.....	12
5.2.2 Failure rates .....	12
5.2.3 Assumption.....	13
6 Results of the assessment.....	13
6.1 HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16 .....	15
6.2 HART Multiplexer HiD Mux2700.....	17
7 Terms and Definitions.....	19
8 Status of the document.....	20
8.1 Liability.....	20
8.2 Releases .....	20
8.3 Release Signatures.....	20

## 1 Purpose and Scope

This report shall describe the results of the FMEDAs carried out on the HART Multiplexer HiD Mux2700 and HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16.

It shall be shown that the HART Multiplexers do not electrically interfere with the connected safety related system when using the 4..20mA loop for the HART communication.

It shall be assessed whether these modules meet the Probability of Failure on Demand (PFD) requirements for SIL 2 / SIL 3 sub-systems according to IEC 61508 with regard to the interference freeness on the safety related 4..20mA loop.

The assessment **does neither** consider any calculations necessary for proving intrinsic safety **nor** an evaluation of the correct functioning of the HART Multiplexers.

Pepperl+Fuchs GmbH contracted *exida.com* in May 2002 with the FMEDA and PFD calculation of the above mentioned modules.

## 2 Project management

### 2.1 Roles of the parties involved

Pepperl+Fuchs            Manufacturer of the HART Multiplexers.

*exida.com*                Did the FMEDAs together with the determination of the Safe Failure Fraction (SFF) and calculated the Probability of Failure on Demand (PFD) using Markov models.

### 2.2 Standards / Literature used

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

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

## 2.3 Reference documents

### 2.3.1 Documentation provided by the customer

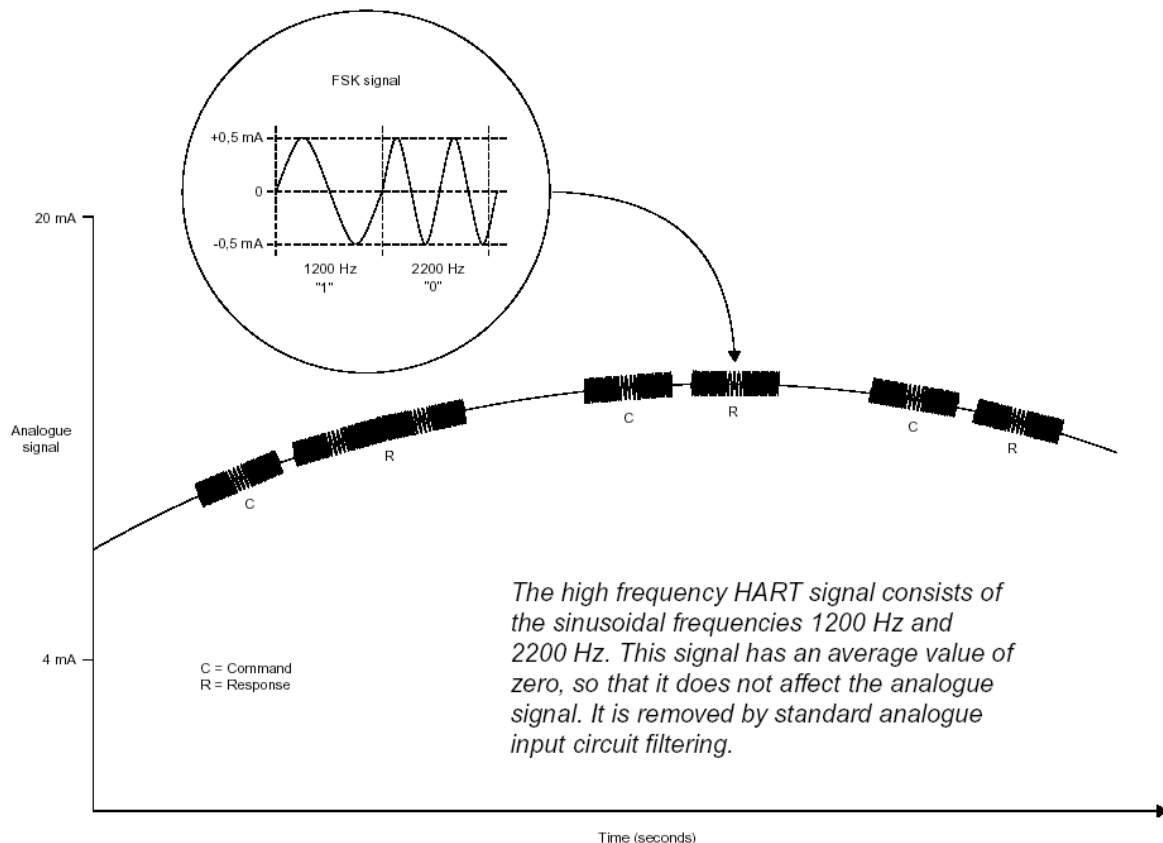
[D1]	3510330b.pdf	Circuit diagram 351-0330B for mother board KFD2-HMM-16 and KFD0-HMS-16
[D2]	3510374b.pdf	Circuit diagram 351-0374B for processor board KFD2-HMM-16
[D3]	3520647d.pdf	Bill of material 352-0647D for mother board KFD2-HMM-16
[D4]	3520684c.pdf	Bill of material 352-0684C for processor board KFD2-HMM-16
[D5]	3520683b.pdf	Bill of material 352-0683B for KFD0-HMS-16
[D6]	3510300.pdf	Circuit diagram 351-0300 for mother board HiD Mux2700
[D7]	3520220b.pdf	Bill of material 352-0220B for mother board HiD Mux2700
[D8]	3510174.pdf	Circuit diagram 351-0174 for processor board HiD Mux2700
[D9]	3520213b.pdf	Bill of material 352-0213B for processor board HiD Mux2700
[D10]		Datasheet metallized polyester capacitor WIMA MKS 2
[D11]	RE Report 06 Umbenennung HiD Mux2700.msg	Request for modification

### 2.3.2 Documentation generated by *exida.com*

[R1]	FMEDA KFD2-HMM-16 V1 R1.0 – Analysis of 24.06.02
[R2]	FMEDA KFD2-HMM-16 V1 R1.0 – Results of 24.06.02
[R3]	FMEDA MUX 2700 V1 R1.0 – Analysis of 24.06.02
[R4]	FMEDA MUX 2700 V1 R1.0 – Results of 24.06.02

### 3 Description of the HART communication

The HART<sup>1</sup> protocol is supported by many conventional 4..20 mA field devices, which thus enable digital communication for configuration and servicing purposes. Many device parameters and also the measured values themselves can thus be digitally transferred to and from the device. This digital communication runs in parallel with the 4..20 mA signal on the same cable. This is possible through a current modulation, which is superimposed on the user signal.



**Figure 1: Modulated HART signal**

HART is a master-slave protocol: A field device does only respond when requested (except in "Burst mode").

The message duration is several hundred milliseconds, so that between two and three messages can be transferred per second.

On HART, there are three groups of commands:

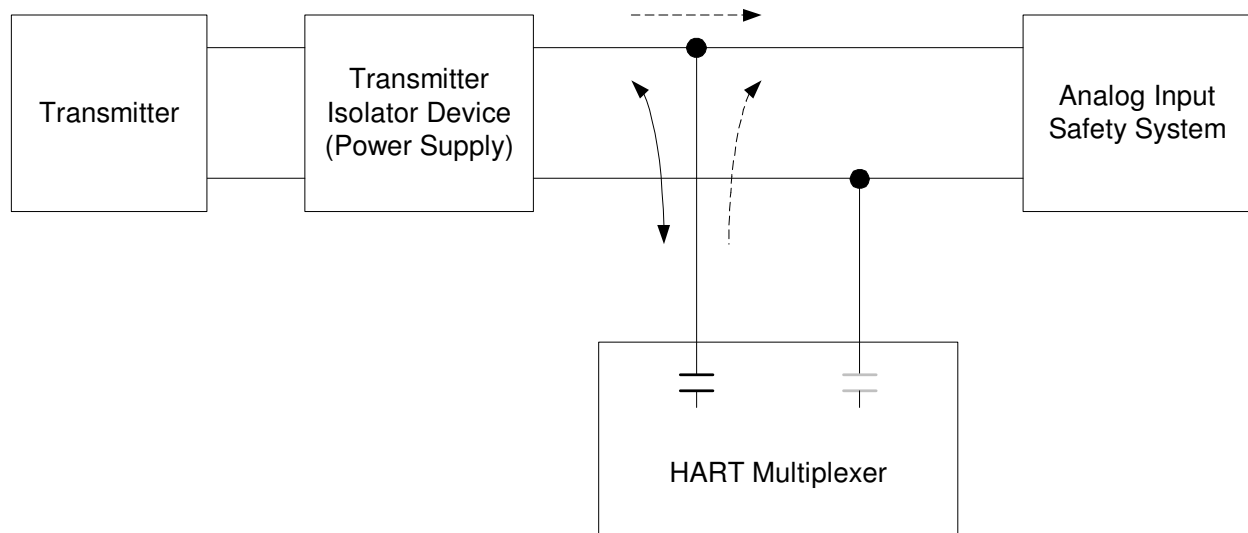
- The "Universal" commands; these must be supported by all field devices;
- The "Common practice" commands; these are pre-defined commands, suitable for many field devices, which, if they are supported by the device, must be implemented in the pre-defined form;
- Device-specific commands; these are commands, which are particularly suitable for this field device.

<sup>1</sup> HART = Highway Addressable Remote Transducer

## 4 Description of the analyzed modules

In safety-related applications the HART communication is used to provide additional (non safety-related) information about statuses and reading, allow for better preventive maintenance and thus improve the integrity of the field instrumentation.

For this purpose the HART Multiplexers have to be directly connected to the field wiring of the respective safety-related system (see Figure 2).



**Figure 2: Connection of the HART Multiplexers with the safety-related system**

### 4.1 HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16

The HART Multiplexer KFD2-HMM-16 can operate up to 256 analog transmitters. The built-in slave unit operates the first 16 loops, and a maximum of further 15 KFD0-HMS-16 slaves can be connected.

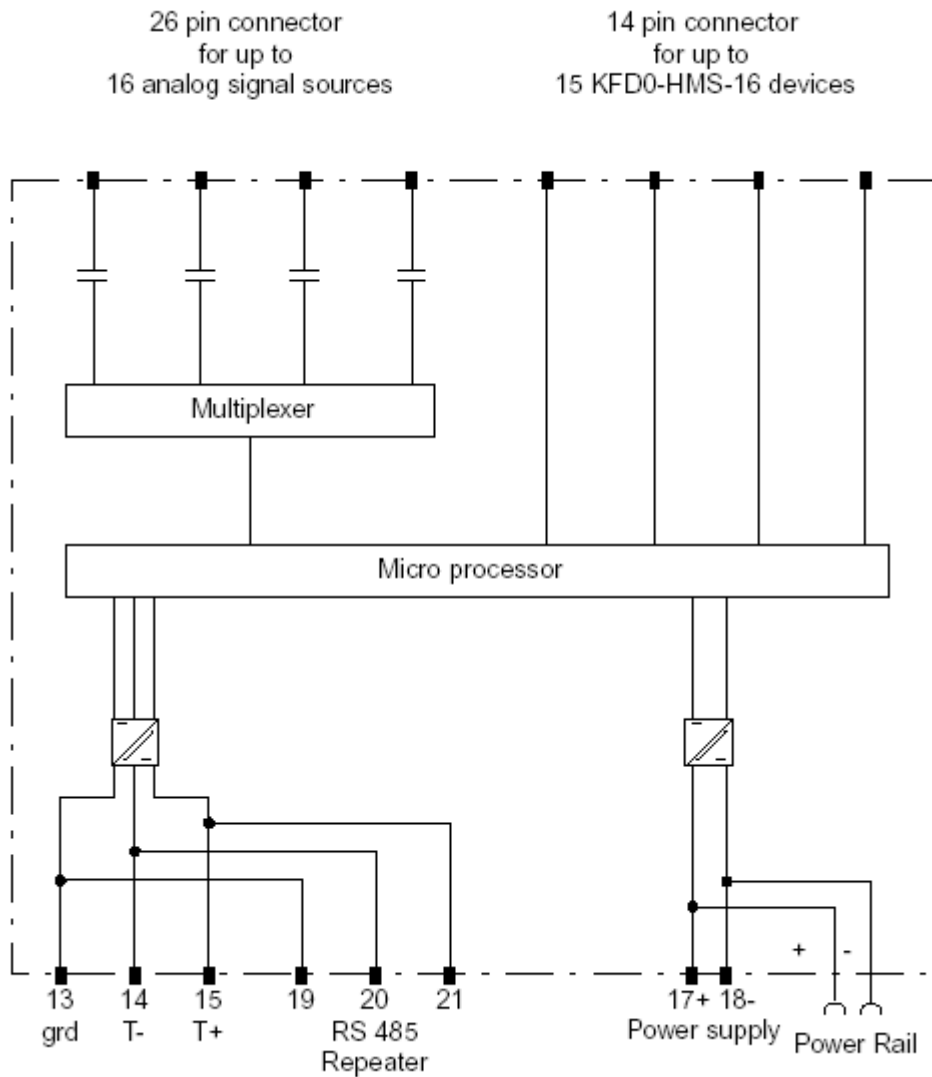
The power supply (24 VDC nominal voltage) is provided via the power rail or terminals 17 and 18. The optional slave units or the RPI control module are connected with the master via a 14-core flat cable. Its connector is placed on the same housing side as the terminals for the RS 485 interface and the voltage supply.

The analog signals for each unit are connected separately via a 26-core cable. 16 leads are provided for the HART signals of the analog instrument circuits, the other 10 are connected to ground.

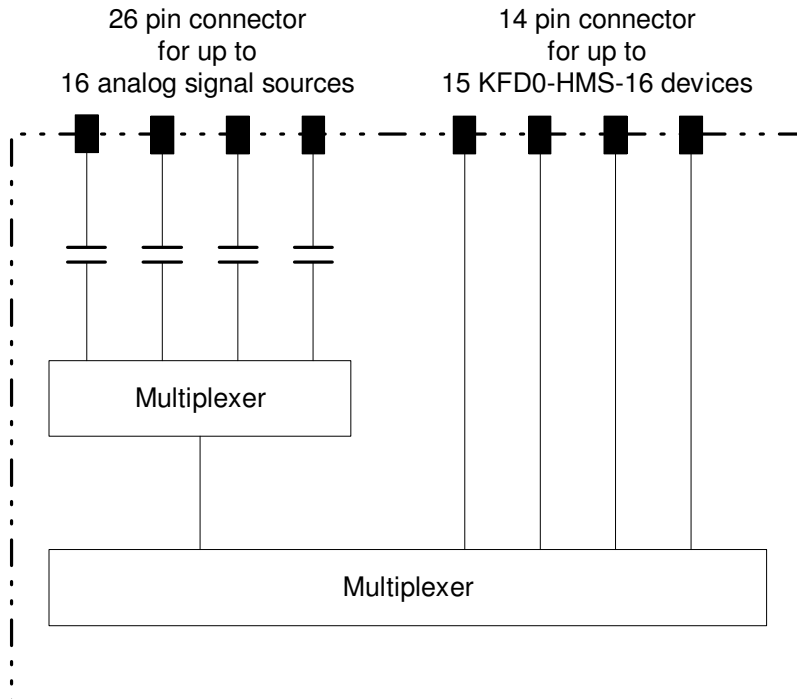
The minimum load resistance of the analog instrument circuits is 230  $\Omega$  (min. load resistance in accordance with the HART specification), the max. load resistance is 500  $\Omega$ . Load resistances of up to 1000  $\Omega$  are possible, however, resistance values greater than 500  $\Omega$  can interfere with the HART communication.

A process control system or a PC can be connected via a RS 485 interface (terminals 13, 14 and 15). Up to 31 KFD2-HMM-16 can be operated on one RS 485 interface. Terminals 19, 20 and 21 can be used to connect additional stations to the RS 485 interface. The DIP-switch on the housing front is for the setting of the RS 485 address and the baud rate.



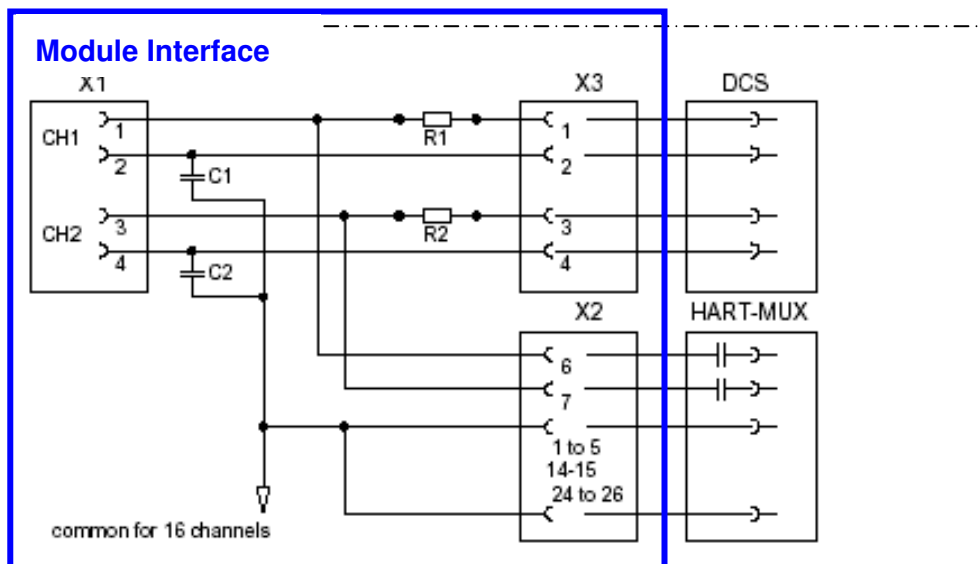


**Figure 3: Block diagram of HART Multiplexer KFD2-HMM-16**



**Figure 4: Block diagram of KFD2-HMS-16**

The HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16 has only one de-coupling capacitor for each analog signal as can be seen in Figure 3 and Figure 4, but can be connected to a module interface as shown in Figure 5 to also have the ground de-coupled by a second capacitor.



**Figure 5: Block diagram HART Multiplexer with module interface for loop 1 and 2**

## 4.2 HART Multiplexer HiD Mux2700

The HART Multiplexer HiD Mux2700 provides 32 signal channels for connection to “smart” transmitters or control devices supporting digital communication according to the HART standard.

Two Decoupling Capacitors are provided, one for each signal connection.

Both + Ve (positive) & - Ve (negative) signal wires are therefore decoupled from DC signal. Only the high frequency digital HART protocol signal passes through to the internal Multiplexer circuitry.

It acts as a gateway between a workstation - typically a PC - and the field instrumentation.

Each HART Multiplexer HiD Mux2700 is networked simply by connecting the high-speed RS485 output in multidrop configuration. The HART Multiplexer HiD Mux2700 interrogates each field device, under the supervision of the workstation, retrieving information for storage in its internal database, which can then be accessed at ease.

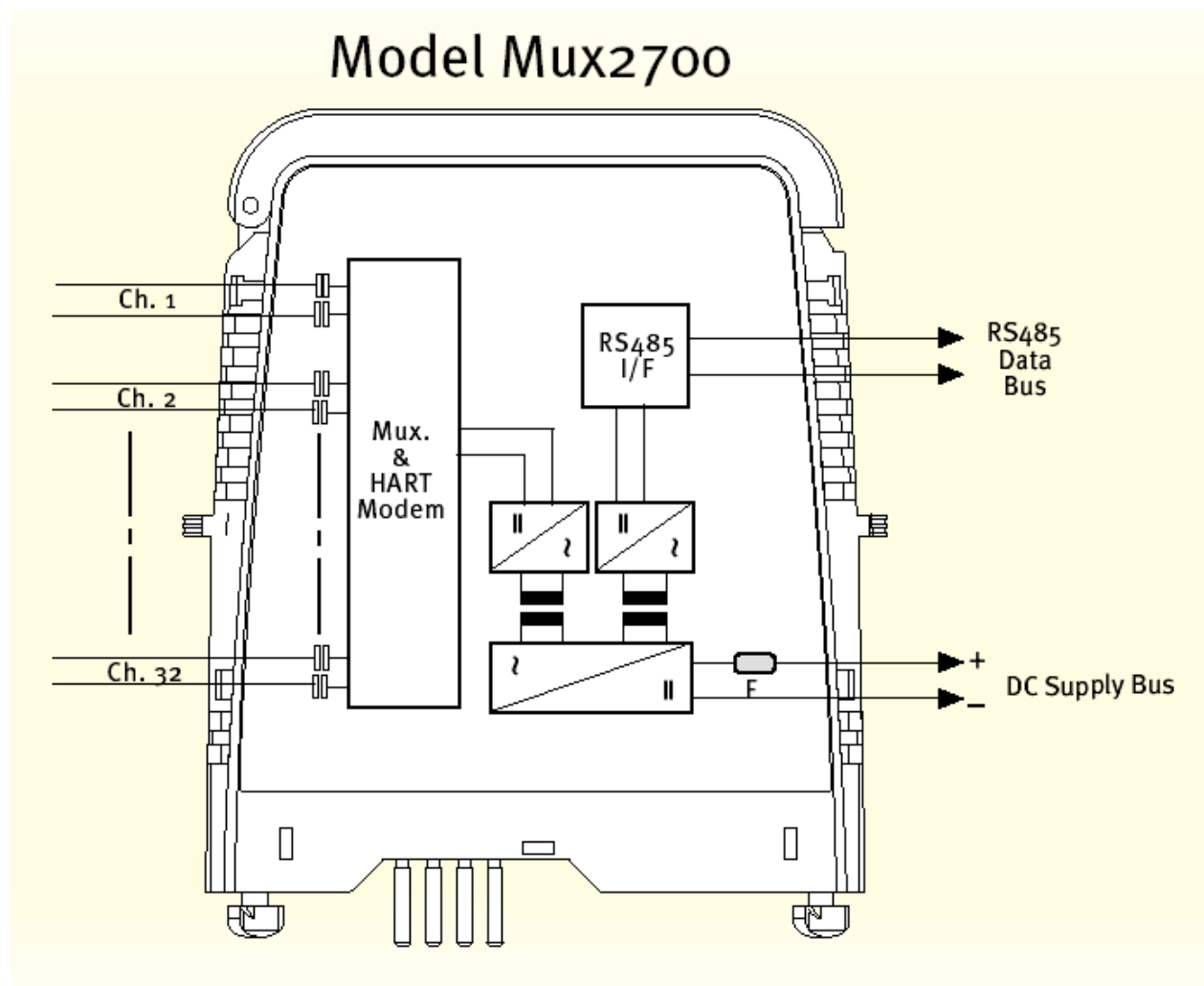


Figure 6: Block diagram of HART Multiplexer HiD Mux2700

## 5 Failure Modes, Effects, and Diagnostics Analysis

### 5.1 Description of the failure categories

The **fail-safe state** is defined as the HART Multiplexer is not communicating.

Failures are categorized and defined as follows:

A **safe** failure (S) is defined as a single failure that causes the HART Multiplexer not to communicate.

A **dangerous** failure (D) is defined as a single failure that disturbs the safety system connected to the HART Multiplexer.

A “don't care” failure (#) is defined as a single failure of a component that is part of the safety function but has no effect on the safety function of the module / (sub)system.

### 5.2 Methodology – FMEDA, Failure rates

#### 5.2.1 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 change 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 from MIL STD 1629A, Failure Modes and Effects Analysis.

#### 5.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA are from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. It is expected that actual field failure results with average environmental stress will be superior to the results predicted by these numbers.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data is preferable to general industry average data. Industrial plant sites with high levels of stress must use failure rate data that is adjusted to a higher value to account for the specific conditions of the plant.

### 5.2.3 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the HART Multiplexers.

- 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.
- All modules are operated in the low demand mode of operation.
- Only one communication line is considered to be part of the safety function.

## 6 Results of the assessment

*exida.com* did the FMEDAs supported by Pepperl+Fuchs.

The analysis has shown that only a couple of components of the HART Multiplexers can be found where potentially dangerous failures exist. All other component failures can only lead to the defined safe state but can never disturb the connected safety-related system. The following critical points were identified:

1. Short circuits (to ground, to power or between each other) of the signal lines from the interconnection terminal to the field side of the de-coupling capacitors;
2. Short circuit of the de-coupling capacitor.

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

$\lambda_{total}$  consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care}^2$$

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

For the FMEDAs the following failure modes and below mentioned distributions were used.

#### Capacitor fixed plastic (in accordance with [N3])

Failure Mode	Distribution (in %)
Short	40
Open	42
Change in value	18

<sup>2</sup> These are all failures that have no impact on the safety function. The behavior of the system is neither dangerous nor safe.

### Capacitor AI-ELKO (in accordance with [N3])

Failure Mode	Distribution (in %)
Short	38
Open	31
Seal failure	31

For the calculation of the PFD the following Markov models for a 1oo1 and 1oo2 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.com* as a simulation tool. The results are documented in the following sections.

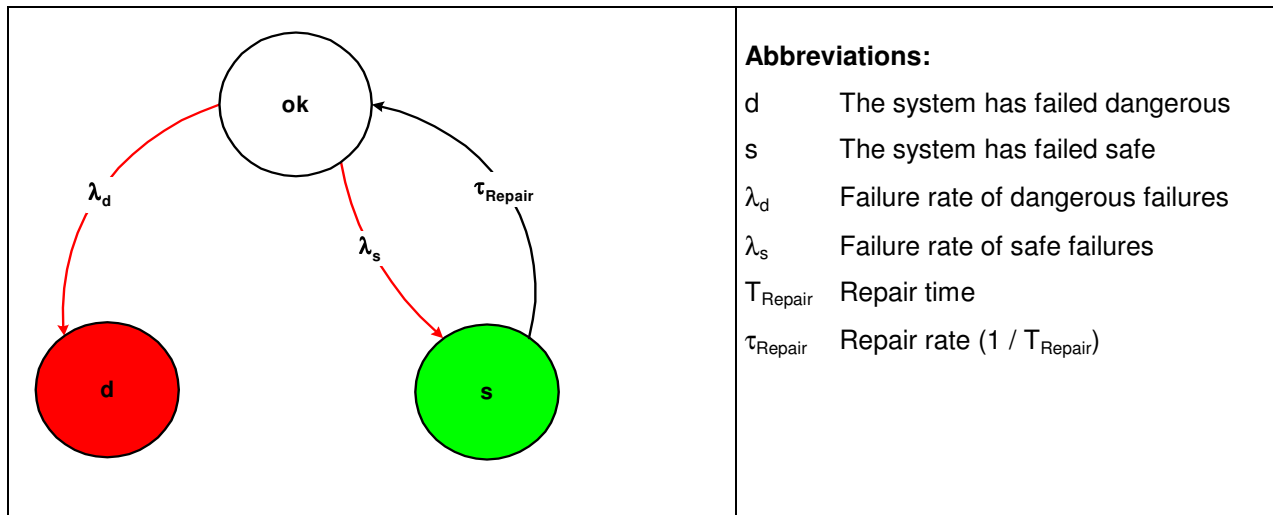


Figure 7: Markov model for a 1oo1 architecture

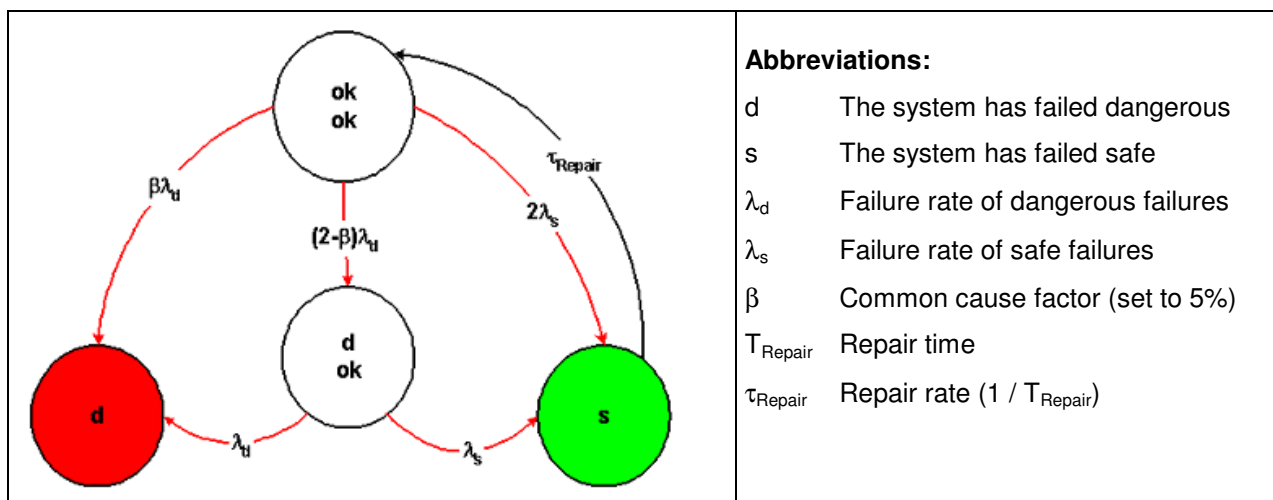


Figure 8: Markov model for a 1oo2 architecture

## 6.1 HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16

Item 1. of the critical points identified in section 6 can be excluded according to draft IEC 60947-5-3 A.1.2 if:

- The HART Multiplexers are mounted in a housing of minimum IP 54
- The base material used is according to IEC 60249, the design and use of the printed board is according to IEC 60326 T3 and the creepage distances and clearances are designed according to IEC 60664-1 (1992) with pollution degree 2 / installation category III, **or**
- The printed side(s) are coated with an insulation material in accordance to IEC 60664-3 (1992)

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category II for a nominal voltage of 24 VDC are given in Table 4.

**Table 4: Clearances and creepage distances according to IEC 60661-1**

	Clearances (table 2)	Creepage distances (table 4)
Printed wiring material	0,1 mm	0,04 mm

According to Pepperl+Fuchs the base material used is according to IEC 60249 and the minimum creepage distances and clearances are 0,15 mm. This is considered to be sufficient as the interesting distances are part of an energy-consuming equipment supplied from fixed installation, i.e. installation category II. In addition the HART Multiplexer is not a safety critical system itself but is connected to one. Thus there are no to special requirements with regard to reliability and availability (see section 2.2.2.1.1 of IEC 60664-1) and installation category III does not apply.

Item 2. of the critical points identified in section 6 was analyzed in form of a FMEDA under the assumptions described in section 5.2.3 and 6.

The following failure rates and SFF were calculated for the de-coupling capacitor:

$$\lambda_{\text{total}} = 7,00\text{E-}10 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 2,94\text{E-}10 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,80\text{E-}10 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 1,26\text{E-}10 \text{ 1/h}$$

$$\text{SFF} = 60,00\% \text{ (HFT} = 0)$$

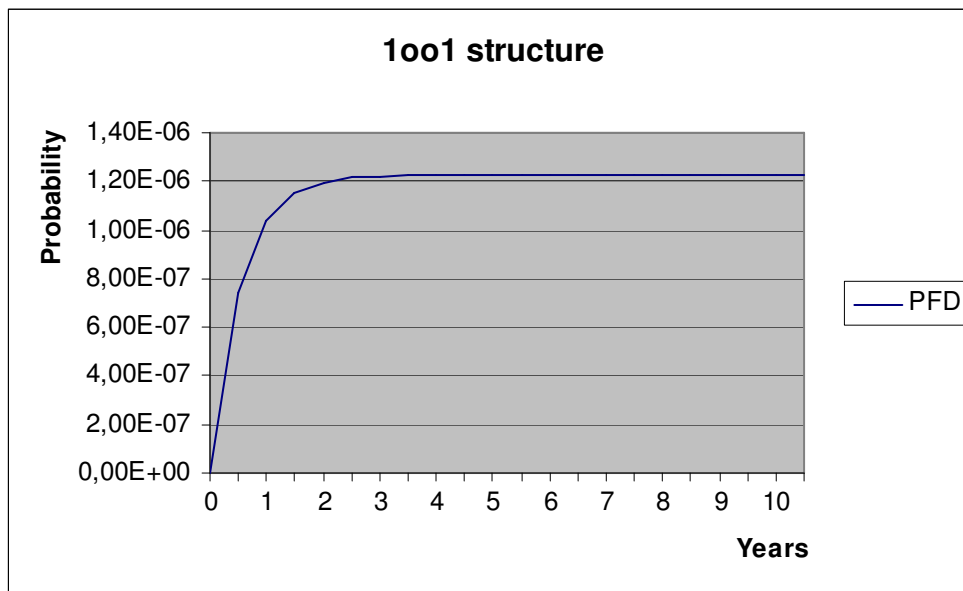
**NOTE:** As all faults of the additional electronic will either contribute to  $\lambda_{\text{safe}}$  or  $\lambda_{\text{don't care}}$  with regard to the interference freeness on the 4..20mA signal the failure modes of the different components were not explicitly analyzed and are not part of the above mentioned failure rates.

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

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b>PFD<sub>AVG</sub> = 1.23E-06</b>	<b>PFD<sub>AVG</sub> = 6.13E-06</b>	<b>PFD<sub>AVG</sub> = 1.23E-05</b>

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-3}$ . The PFD values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 2 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 0.

The following figure shows the result of the PFD calculation for T[Proof] = 1 year.



**Figure 9: PFD for T[Proof] = 1 year**

If the HART Multiplexer KFD2-HMM-16 together with KFD0-HMS-16 is used with the module interface as described in section 4.1 then two de-coupling capacitors have to fail to bring the subsystem into a dangerous state. This corresponds to a hardware fault tolerance of 1.

The PFD was calculated for three different proof times using the Markov model as described in Figure 8.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b>PFD<sub>AVG</sub> = 6.13E-08</b>	<b>PFD<sub>AVG</sub> = 3.07E-07</b>	<b>PFD<sub>AVG</sub> = 6.13E-07</b>

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-4}$ . The PFD values even fulfill the requirements of a higher SIL but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

The following figure shows the result of the PFD calculation for T[Proof] = 1 year and  $\beta = 5\%$  (maximum common cause factor for a logic sub-system according to IEC 61508-6).



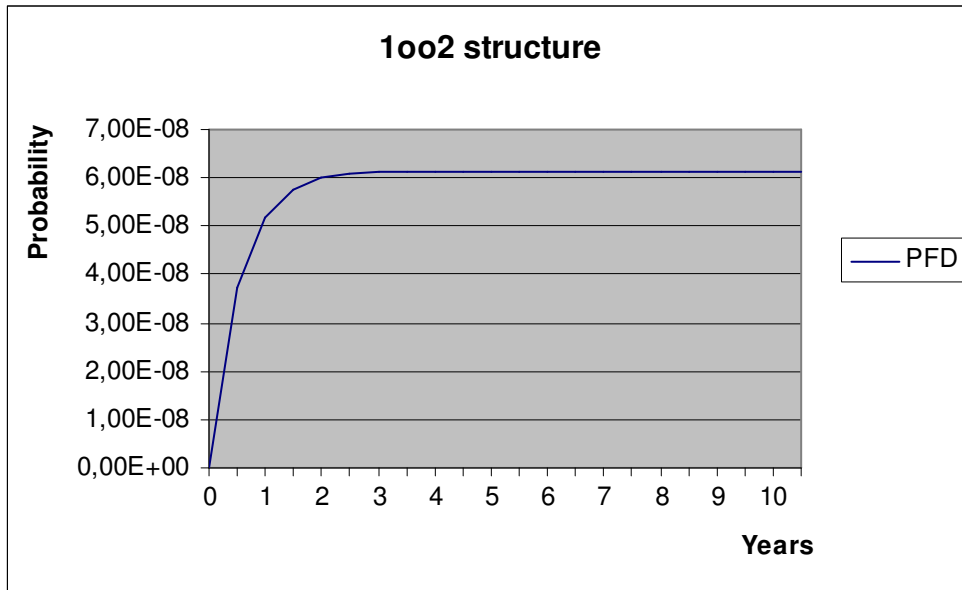


Figure 10: PFD for T[Proof] = 1 year and β = 5%

## 6.2 HART Multiplexer HiD Mux2700

Item 1. of the critical points identified in section 6 can be excluded according to draft IEC 60947-5-3 A.1.2 if:

- The HART Multiplexers are mounted in a housing of minimum IP 54
- The base material used is according to IEC 60249, the design and use of the printed board is according to IEC 60326 T3 and the creepage distances and clearances are designed according to IEC 60664-1 (1992) with pollution degree 2 / installation category III, **or**
- The printed side(s) are coated with an insulation material in accordance to IEC 60664-3 (1992)

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category II for a nominal voltage of 24 VDC are given in Table 5.

Table 5: Clearances and creepage distances according to IEC 60661-1

	Clearances (table 2)	Creepage distances (table 4)
Printed wiring material	0,1 mm	0,04 mm

According to Pepperl+Fuchs the base material used is according to IEC 60249 and the minimum creepage distances and clearances are 0,25 mm. This is considered to be sufficient as the interesting distances are part of an energy-consuming equipment supplied from fixed installation, i.e. installation category II. In addition the HART Multiplexer is not a safety critical system itself but is connected to one. Thus there are no to special requirements with regard to reliability and availability (see section 2.2.2.1.1 of IEC 60664-1) and installation category III does not apply.

Item 2. of the critical points identified in section 6 was analyzed in form of a FMEDA under the assumptions described in section 5.2.3 and 6.

The following failure rates and SFF were calculated for the two de-coupling capacitors:

$$\lambda_{\text{total}} = 3,70\text{E-}09 \text{ 1/h}$$

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

$$\lambda_{\text{dangerous}} = 1,42\text{E-}09 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 1,06\text{E-}09 \text{ 1/h}$$

$$\text{SFF} = 61,62\% \text{ (HFT} = 1)$$

**NOTE:** As all faults of the additional electronic will either contribute to  $\lambda_{\text{safe}}$  or  $\lambda_{\text{don't care}}$  with regard to the interference freeness on the 4..20mA signal the failure modes of the different components were not explicitly analyzed and are not part of the above mentioned failure rates.

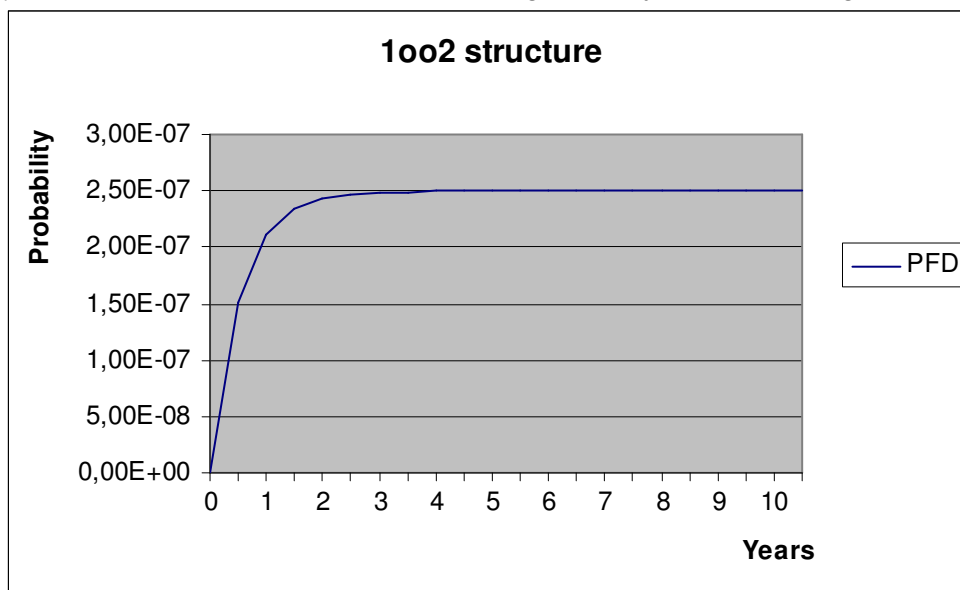
As two de-coupling capacitors have to fail to bring the (sub)system into a dangerous state a hardware fault tolerance of 1 is considered.

The PFD was calculated based on the failure rate of the AI-ELKO as a worst case assumption for three different proof times using the Markov model as described in Figure 8.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD <sub>AVG</sub> = 2.50E-07	PFD <sub>AVG</sub> = 1.25E-06	PFD <sub>AVG</sub> = 2.50E-06

The boxes marked in green (  ) mean that the calculated PFD 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  $10^{-4}$ . The PFD values even fulfill the requirements of a higher SIL but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

The following figure shows the result of the PFD calculation for T[Proof] = 1 year and  $\beta = 5\%$  (maximum common cause factor for a logic sub-system according to IEC 61508-6).



**Figure 11: PFD for T[Proof] = 1 year and  $\beta = 5\%$**

## 7 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.
$\lambda_{total}$	Total failure rate $\lambda$ (overall failure rate of all components)
$\lambda_{safe}$	Failure rate $\lambda$ of all safe failures
$\lambda_{dangerous}$	Failure rate $\lambda$ of all dangerous failures
$\lambda_{du}$	Failure rate $\lambda$ of dangerous undetected failures
PFD	Probability of Failure on Demand
PFD <sub>AVG</sub>	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

## 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

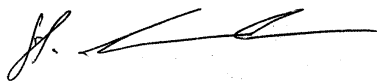
Version History: V0, R1.0: Initial version, June 19, 2002  
V0, R1.1: Failure rates for the de-coupling capacitors of the MUX 2700 corrected; section 2.3.2 completed; failure modes of AI-ELKO in section 6 added; June 24, 2002  
V1, R1.0: Comments after review integrated, June 27, 2002  
V1, R1.1: Management summary corrected; section "Purpose and Scope" modified, June 28, 2002  
V1, R1.2: Management summary changed; section "Purpose and Scope" modified, July 3, 2002  
V2R0: Device name changed, documents updated; January 21, 2009

Authors: Stephan Aschenbrenner

Review: V0, R1.0: Werner Bansemir (P+F), June 24, 2002  
V0, R1.1: Peter Müller (*exida.com*), June 26, 2002

Release status: released to Pepperl+Fuchs

### 8.3 Release Signatures



---

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Senior Project Manager



---

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