



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

HART Multiplexer Type 9192 with connection board Type 9196  
or pac-carrier Type 9195

Customer:

R. STAHL Schaltgeräte GmbH  
Waldenburg  
Germany

Contract No.: Stahl 04/04-03

Report No.: Stahl 04/04-03 R002

Version V1, Revision R1.0, June 2004

Stephan Aschenbrenner

## Management summary

This report summarizes the results of the analysis carried out on the HART multiplexer Type 9192 with connection board Type 9196 or pac-carrier Type 9195.

**Table 1: Options of the connection boards 9196 / 9195**

<b>Option 1</b>	With de-coupling diode and sense resistor
<b>Option 2</b>	Without de-coupling diode but with sense resistor
<b>Option 3</b>	With de-coupling diode but without sense resistor
<b>Option 4</b>	Without de-coupling diode and without sense resistor

The assessment does not contain an evaluation of the correct functioning of the HART multiplexer but a statement about being interference free 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).

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  $\geq 10^{-4}$  to  $< 10^{-3}$  for SIL 3 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  $10^{-4}$ .

The modules under evaluation can be considered to be Type B<sup>1</sup> components. However, the components that can contribute to a disturbance of the safety system are considered to be Type A<sup>2</sup> 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 3	90% ≤ SFF < 99%	60% ≤ SFF < 90%	SFF < 60%

The following table shows under which conditions the critical components 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 2: HART multiplexer Type 9192 with connection board Type 9196 or pac-carrier Type 9195**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
<b>Option 1</b>	PFD <sub>AVG</sub> = 2.04E-06	PFD <sub>AVG</sub> = 1.02E-05	PFD <sub>AVG</sub> = 2.04E-05	91,06%
<b>Option 2</b>	PFD <sub>AVG</sub> = 5.04E-07	PFD <sub>AVG</sub> = 2.52E-06	PFD <sub>AVG</sub> = 5.04E-06	97,26%
<b>Option 3</b>	PFD <sub>AVG</sub> = 1.77E-06	PFD <sub>AVG</sub> = 8.87E-06	PFD <sub>AVG</sub> = 1.77E-05	91,90%
<b>Option 4</b>	PFD <sub>AVG</sub> = 2.41E-07	PFD <sub>AVG</sub> = 1.20E-06	PFD <sub>AVG</sub> = 2.41E-06	98,63%

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

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

The boxes marked in green (■) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $10^{-4}$ . The system also fulfills the architectural constraints requirements (HFT/SFF) for SIL 3, which are set by table 2 of IEC 61508-2 for type A components with a hardware fault tolerance of 0.

The calculations are based on the assumption that the HART multiplexer 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 Type 9192 with connection board Type 9196 or Type 9195.....	8
5 Failure Modes, Effects, and Diagnostics Analysis .....	10
5.1 Description of the failure categories.....	10
5.2 Methodology – FMEDA, Failure rates .....	10
5.2.1 FMEDA.....	10
5.2.2 Failure rates .....	10
5.2.3 Assumption .....	11
5.2.4 Critical Points of Failure .....	11
6 Results of the assessment.....	13
6.1 HART multiplexer Type 9192 with connection board Type 9196 or Type 9195.....	14
7 Terms and Definitions .....	17
8 Status of the document.....	18
8.1 Liability .....	18
8.2 Releases .....	18
8.3 Release Signatures.....	18

## 1 Purpose and Scope

This report shall describe the results of the FMEDAs carried out on the HART multiplexer Type 9192 with connection board Type 9196 or pac-carrier Type 9195.

It shall be shown that the HART multiplexer and the connection boards 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 devices meet the average Probability of Failure on Demand (PFD<sub>AVG</sub>) requirements for SIL 3 sub-systems according to IEC 61508 with regard to being interference free 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 multiplexer and the connection boards.

## 2 Project management

### 2.1 Roles of the parties involved

R. Stahl Schaltgeräte GmbH     Manufacturer of the HART multiplexer and the connection boards.

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

R. Stahl Schaltgeräte GmbH contracted *exida.com* in May 2004 with the FMEDA and PFD<sub>AVG</sub> calculation of the above mentioned devices.

### 2.2 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]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	SN 29500	Failure rates of components

## 2.3 Reference documents

### 2.3.1 Documentation provided by the customer

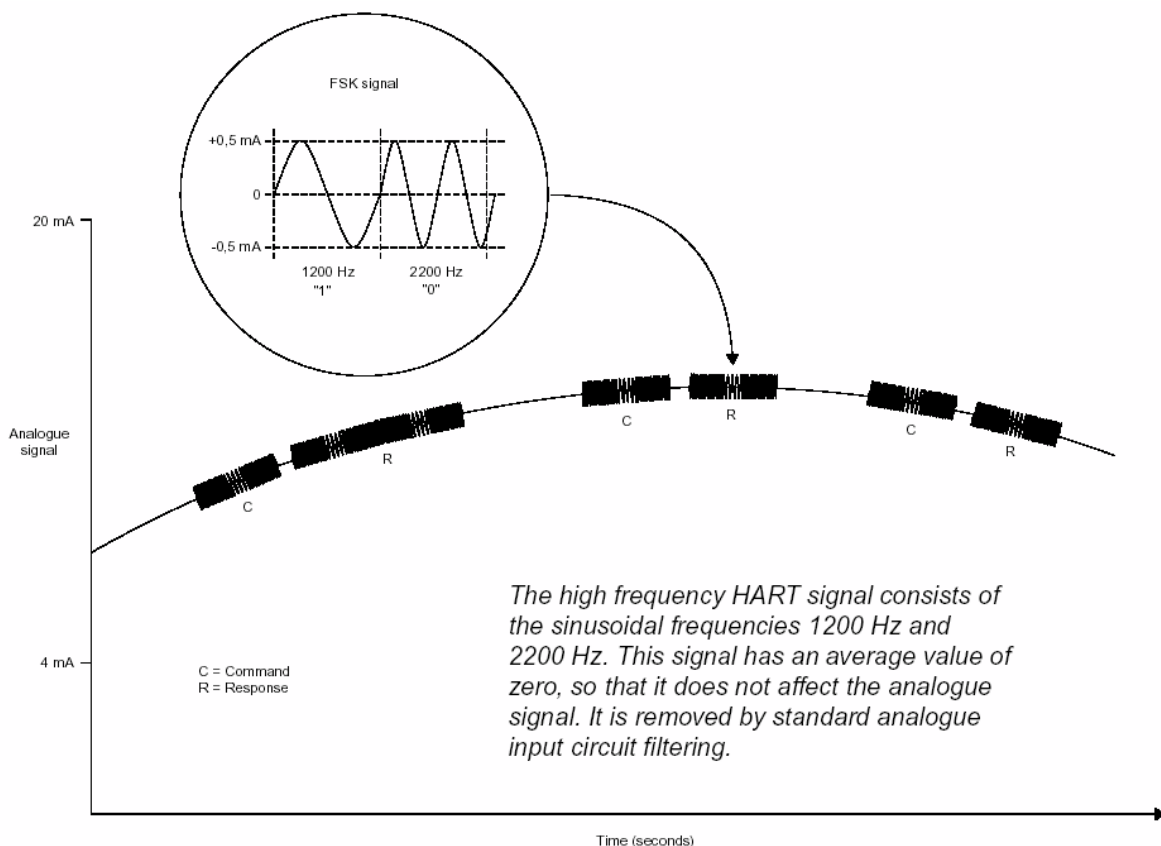
[D1]	Auszug_Beschr_9192.doc	Description of the HART multiplexer 9192 on block level
[D2]	FMEDA_9195_9196.doc and FMEA_9196_01c_02c.doc	Description of the different options of the connection boards 9196 and 9195
[D3]		Data sheet HART multiplexer Type 9192
[D4]	91 926 01 20 0 Ind. 02	Circuit diagram "HART-Multiplexer 32 Kanäle – Typ 9192/32-10-10 HART-Modem und Steuerung"
[D6]	91 926 02 20 0 Ind. 01	Circuit diagram "HART-Multiplexer 32 Kanäle – Typ 9192/32-10-10 Stecker-Leiterplatte"
[D5]	91 966 01 20 0 Ind. 01	Circuit diagram "Anschlussboard – 9196/16H-XX0-01c, 9196/16H-XX0-02c "

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

[R1]	FMEDA V5 HART 9192 V1 R1.0 D-R-C.xls of 19.05.04
[R2]	FMEDA V5 HART 9192 V1 R1.0 R-C.xls of 19.05.04
[R3]	FMEDA V5 HART 9192 V1 R1.0 D-C.xls of 19.05.04
[R4]	FMEDA V5 HART 9192 V1 R1.0 C.xls of 19.05.04

### 3 Description of the HART communication

The HART<sup>3</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 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 a particular field device.

<sup>3</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, allowing for better preventive maintenance and thus improving the integrity of the field instrumentation.

For this purpose the HART multiplexer has to be directly connected to the field wiring of the respective safety-related system (see Figure 4).

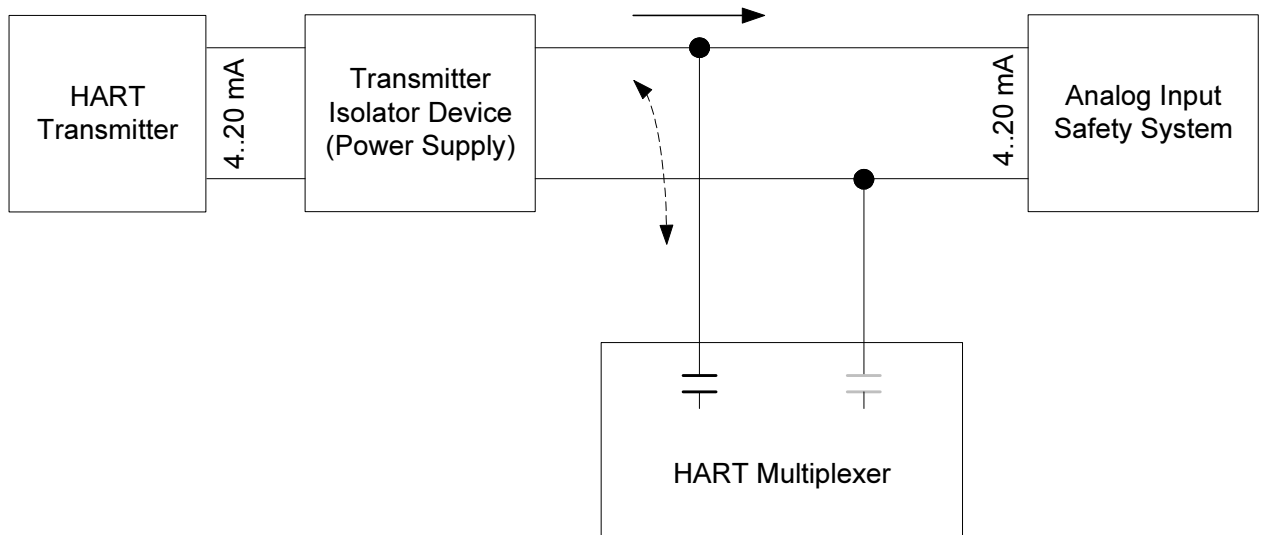


Figure 2: Connection of the HART multiplexer with the safety-related system

### 4.1 HART multiplexer Type 9192 with connection board Type 9196 or Type 9195

The HART multiplexer Type 9192 is used for digital connection of up to 32 HART capable field devices, such as transmitters and regulating valves, to a programmable controller.

The PC communicates with the HART multiplexer via an RS 485 bus.

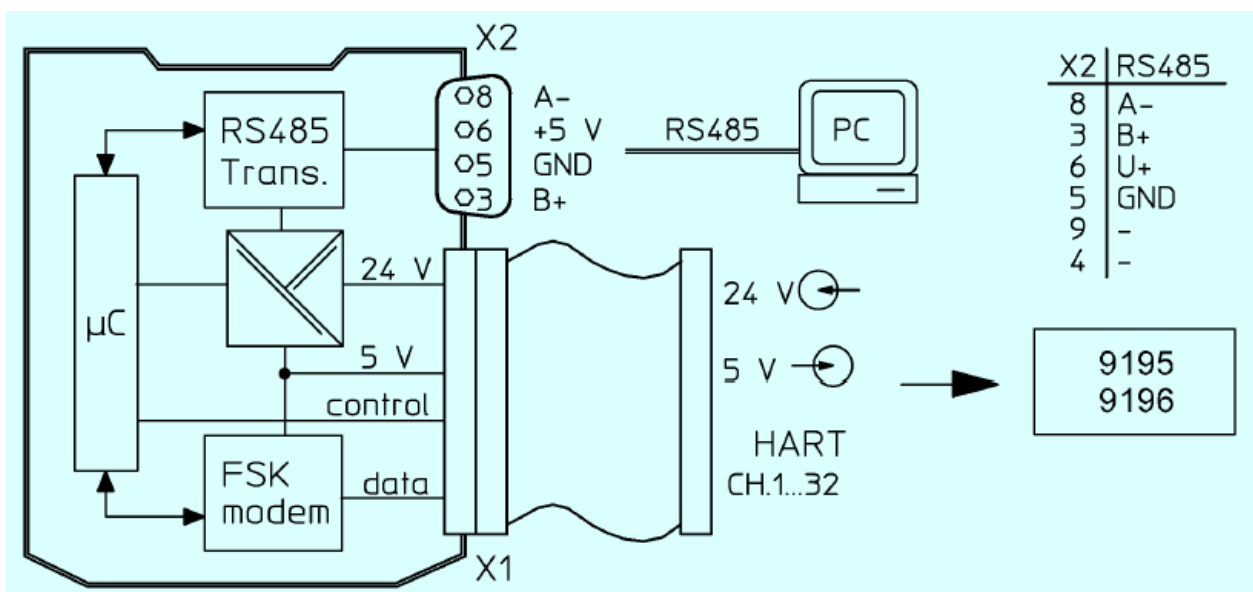
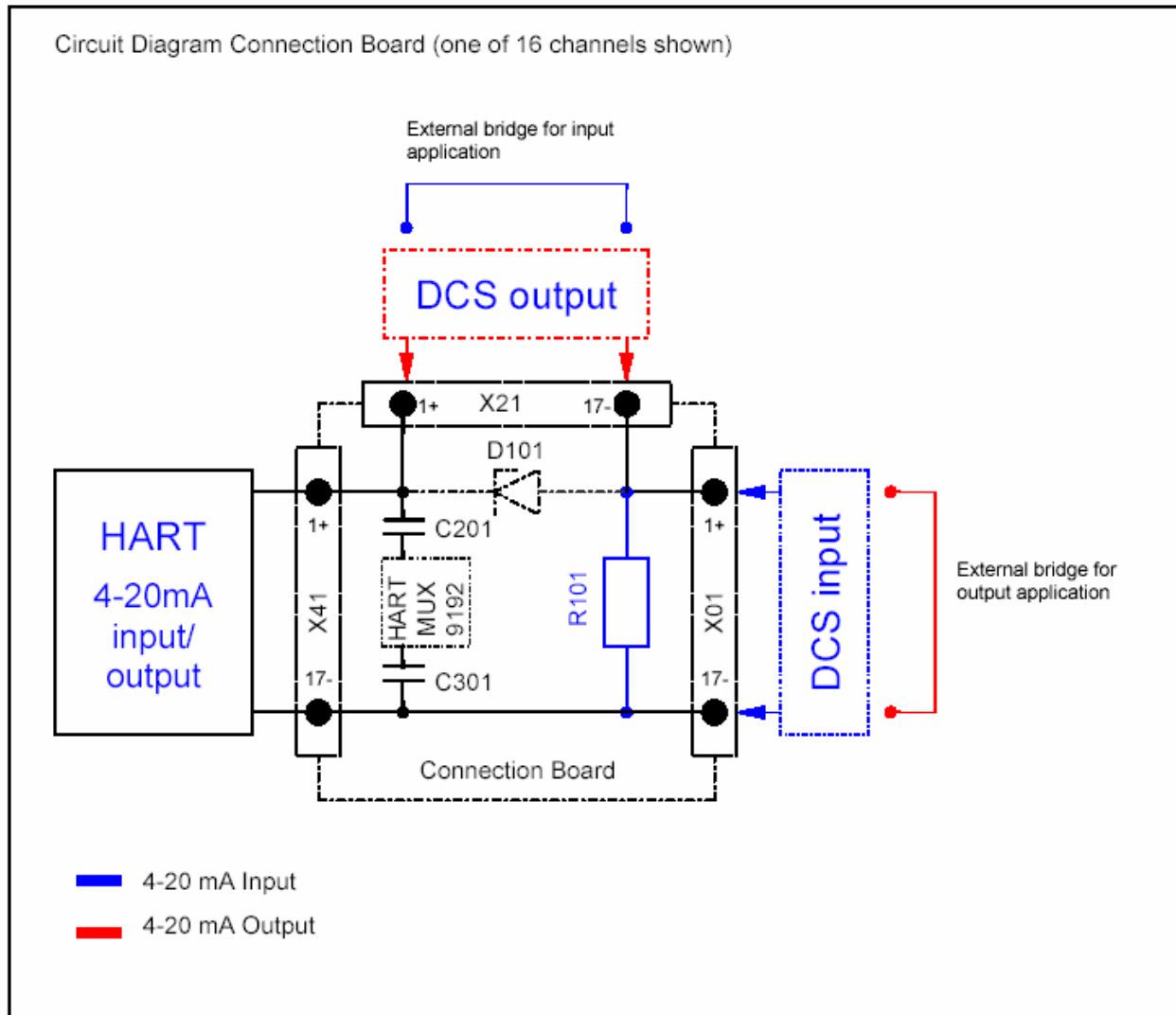


Figure 3: Block diagram



The principle structure of the connection boards 9196 and 9195 is shown in Figure 4



**Figure 4: Overview of the principle structure of the connection boards 9195 / 9196**

Instead of considering a HFT=1 for the two de-coupling capacitors, a HFT=0 is considered with one capacitor being the "protection" of the second one. A "diagnostic coverage" of 95% is considered for one capacitor which also considers a common cause factor of 5%. Faults of the second capacitor are treated as safe failures.

## 5 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with R. Stahl Schaltgeräte GmbH and is documented in [R1] to [R4].

### 5.1 Description of the failure categories

The **fail-safe state** is defined as the HART multiplexer is not disturbing the 4..20 mA loop.

Failures are categorized and defined as follows:

A **safe** failure (S) is defined as a single failure of the HART multiplexer which is not disturbing the 4..20 mA loop.

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

### 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 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.

#### 5.2.2 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. These 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.

### 5.2.3 Assumption

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

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- 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 40°C. Humidity levels are assumed within manufacturer's rating.
- All modules are operated in the low demand mode of operation.
- Only one communication line is considered to be part of the safety function.
- External power supply failure rates are not included.
- Instead of considering a HFT=1 for the two de-coupling capacitors, a HFT=0 is considered with one capacitor being the "protection" of the second one. A "diagnostic coverage" of 95% is considered for one capacitor which also considers a common cause factor of 5%. Faults of the second capacitor are treated as safe failures.

### 5.2.4 Critical Points of Failure

The analysis has shown that only a couple of components of the HART multiplexer 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 capacitors.
3. Certain failure modes of the de-coupling diode.
4. Certain failure modes of the sense resistor.

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

- The HART multiplexer is 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 with IEC 60664-3 (1992)

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category III for a nominal voltage of 24 VDC are given in Table 3.

**Table 3: Clearances and creepage distances according to IEC 60661-1**

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

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	0,04 mm	0,04 mm

According to R. Stahl Schaltgeräte GmbH the base material used is FR4 according to NEMA- LI 1-1989 which is identical to IEC 60249, maximum temperature > 130°C (according to UL 796A), comparative tracking index CTI > 175 according to IEC112 with UL approval. The minimum clearance and creepage distances are > 0,04 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. The printed sides are not additionally coated with an insulation material.

## 6 Results of the assessment

*exida.com* did the FMEDAs supported by R. Stahl Schaltgeräte GmbH.

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

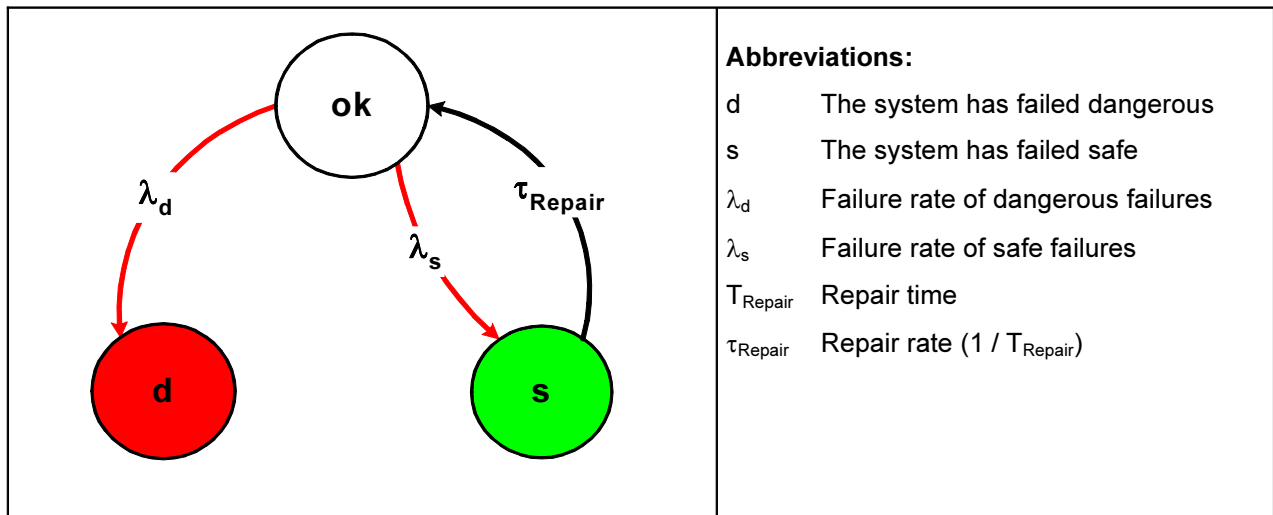
$\lambda_{total}$  consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous}$$

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

For the calculation of  $PFD_{AVG}$  the following Markov model for a 1oo1 architecture was 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 5: Markov model for a 1oo1 architecture**

## 6.1 HART multiplexer Type 9192 with connection board Type 9196 or Type 9195

Items 2., 3. and 4. of the critical points identified in section 5.2.4 were 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 4 described options:

	$\lambda_{\text{safe}}$	$\lambda_{\text{dangerous}}$	$\lambda_{\text{total}}$	SFF
<b>Option 1</b>	4,74E-09	4,65E-10	5,20E-09	91,06%
<b>Option 2</b>	4,09E-09	1,15E-10	4,20E-09	97,26%
<b>Option 3</b>	4,60E-09	4,05E-10	5,00E-09	91,90%
<b>Option 4</b>	3,95E-09	5,50E-11	4,00E-09	98,63%

**NOTE:** As all faults of the additional electronic do not have any impact on the interference freeness of 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  $\text{PFD}_{\text{AVG}}$  was calculated for three different proof times using the Markov model as described in Figure 5.

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b>Option 1</b>	<b><math>\text{PFD}_{\text{AVG}} = 2.04\text{E-}06</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 1.02\text{E-}05</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 2.04\text{E-}05</math></b>
<b>Option 2</b>	<b><math>\text{PFD}_{\text{AVG}} = 5.04\text{E-}07</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 2.52\text{E-}06</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 5.04\text{E-}06</math></b>
<b>Option 3</b>	<b><math>\text{PFD}_{\text{AVG}} = 1.77\text{E-}06</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 8.87\text{E-}06</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 1.77\text{E-}05</math></b>
<b>Option 4</b>	<b><math>\text{PFD}_{\text{AVG}} = 2.41\text{E-}07</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 1.20\text{E-}06</math></b>	<b><math>\text{PFD}_{\text{AVG}} = 2.41\text{E-}06</math></b>

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  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 system also fulfills the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components with a hardware fault tolerance of 0.

The following figures show the time dependent curve of the  $\text{PFD}_{\text{AVG}}$  calculation.

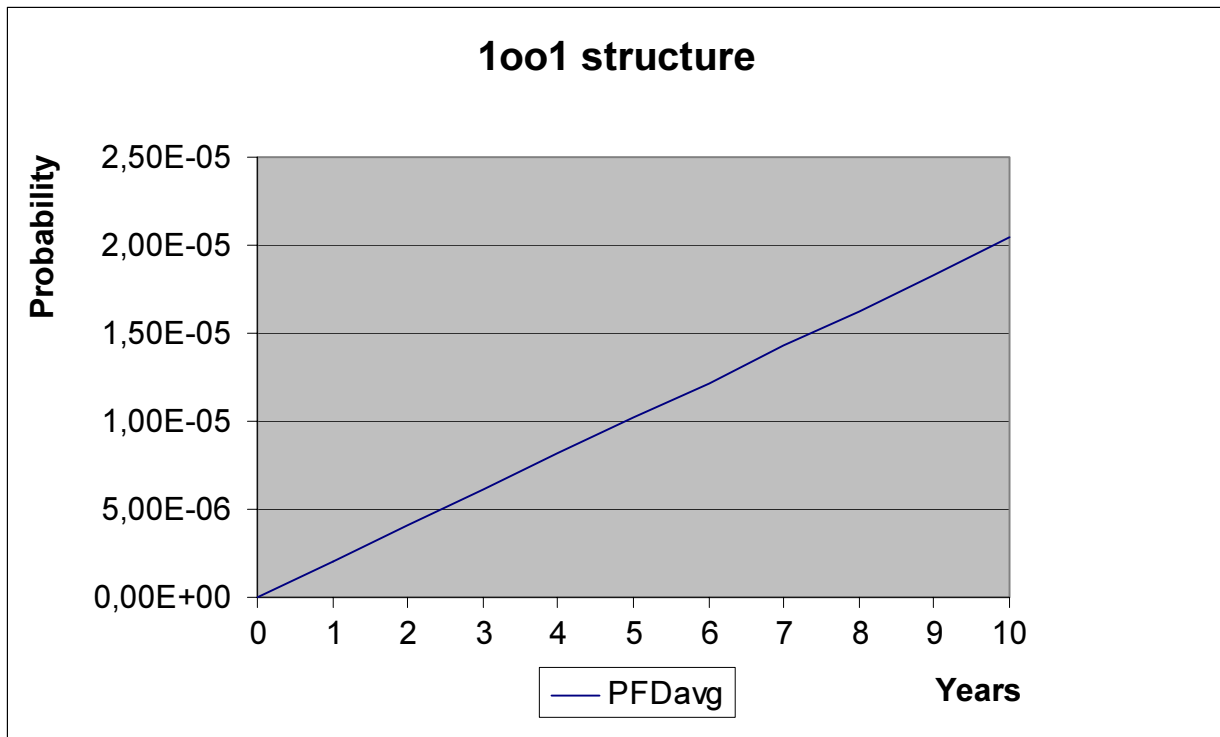


Figure 6: PFD<sub>AVG</sub>(t) for option 1

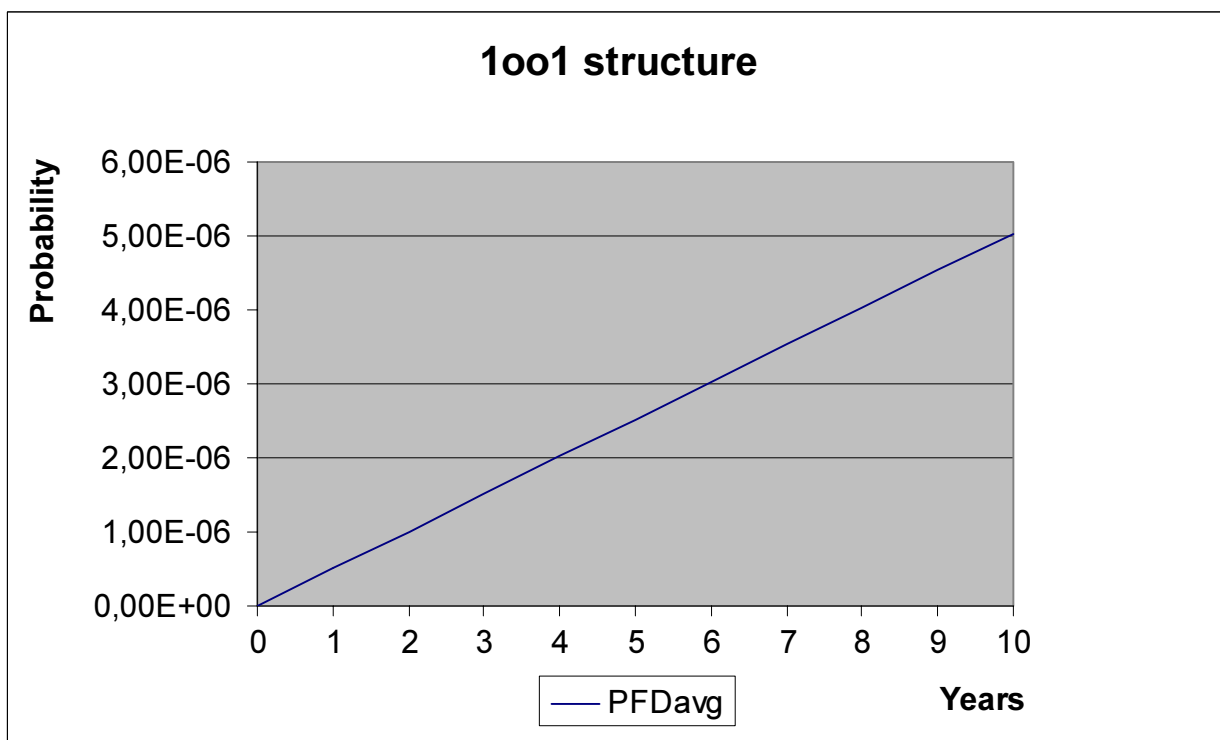


Figure 7: PFD<sub>AVG</sub>(t) for option 2

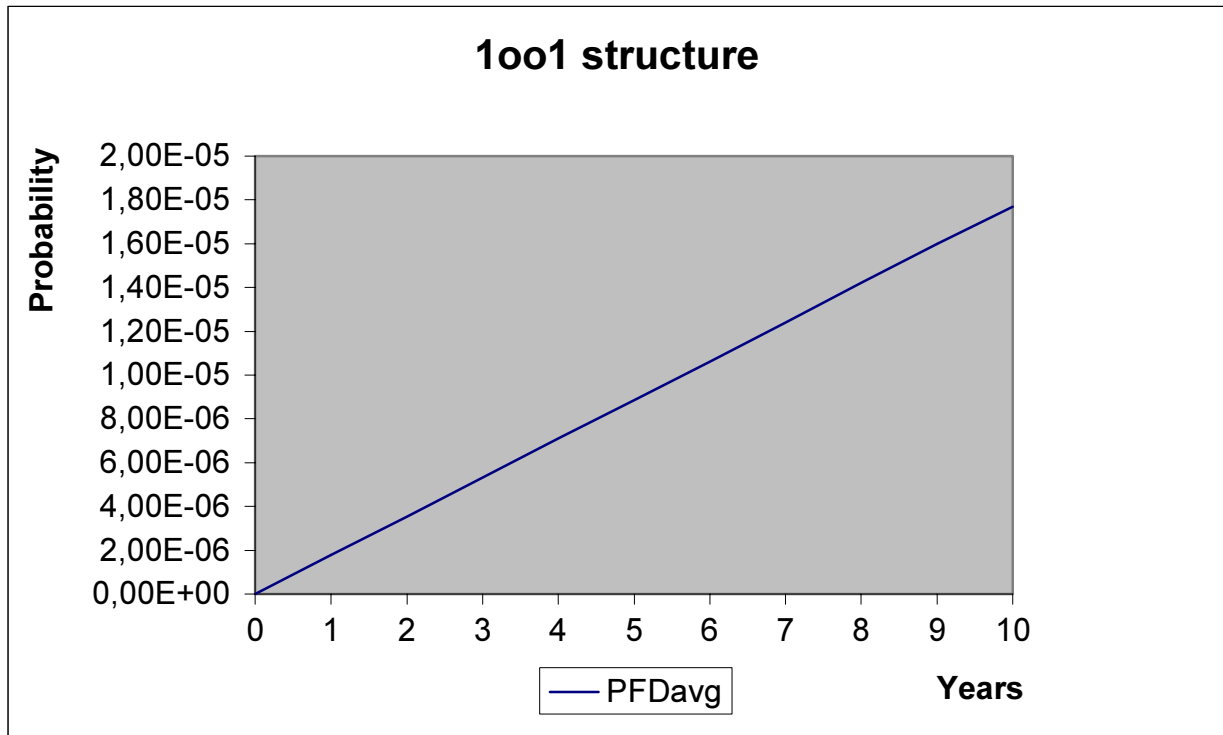


Figure 8: PFD<sub>AVG</sub>(t) for option 3

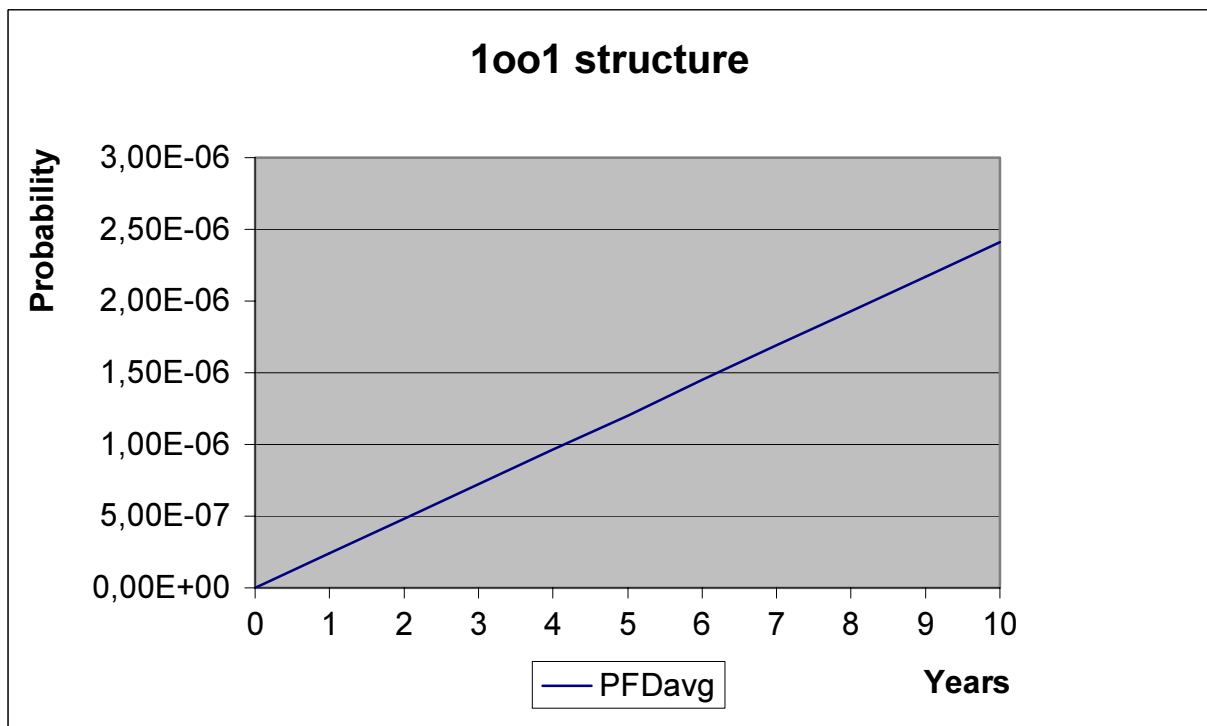


Figure 9: PFD<sub>AVG</sub>(t) for option 4



## 7 Terms and Definitions

FIT	Failure In Time (1x10 <sup>-9</sup> 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.
$\lambda_{total}$	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
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
Type A component	“Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 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: R1.0

Version History: V0, R1.0: Initial version, May 26, 2004

V1, R1.0: Review comments integrated, June 7, 2004

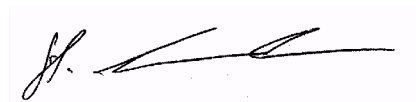
Authors: Stephan Aschenbrenner

Review: V0, R1.0: Franz Danko (Stahl); June 1, 2004

Rachel Amkreutz (exida.com), June 2, 2004

Release status: Released to R. Stahl Schaltgeräte GmbH

### 8.3 Release Signatures



---

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



---

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



**Appendix 1 to  
Report No.: Stahl 04/04-03 R002  
Version V1, Revision R1.0, June 2004**

Project:

HART Multiplexer Type 9192 with connection board Type 9196  
or pac-carrier Type 9195

Customer:

R. STAHL Schaltgeräte GmbH  
Waldenburg  
Germany

Jan Hettenbach

## Appendix 1 Failure rates according to IEC 61508:2010

Table 1: Failure rates for Option 1

Failure category	Failure rates (in FIT)
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0.000</b>
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>0.000</b>
<b>Fail Dangerous Detected (<math>\lambda_{DD}</math>)</b>	<b>1.335</b>
Fail Dangerous Detected ( $\lambda_{DD}$ )	1.045
Fail High (H)	0.140
Fail Low (L)	0.150
Fail Annunciation Detected ( $\lambda_{AD}$ )	0.000
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>0.465</b>
Fail Annunciation Undetected ( $\lambda_{AU}$ )	1.100
No effect	2.300
No part	0.000
<b>Total failure rate (safety function)</b>	<b>1.800</b>
<b>SFF<sup>1</sup></b>	<b>(74%)</b>
<b>SIL AC<sup>2</sup></b>	<b>(SIL2)</b>

<sup>1</sup> A HART multiplexer is no element in terms of IEC 61508. Only a negative influence on  $\lambda_{DU}$  can occur. The calculated SFF is thereby not applicable for the given product.

<sup>2</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled. This HART multiplexer is no element in terms of IEC 61508. Thereby, it may be used also in SIL3 applications.

**Table 2: Failure rates for Option 2**

Failure category	Failure rates (in FIT)
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0.000</b>
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>0.000</b>
<b>Fail Dangerous Detected (<math>\lambda_{DD}</math>)</b>	<b>1.185</b>
Fail Dangerous Detected ( $\lambda_{DD}$ )	1.045
Fail High (H)	0.140
Fail Low (L)	0.000
Fail Annunciation Detected ( $\lambda_{AD}$ )	0.000
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>0.115</b>
Fail Annunciation Undetected ( $\lambda_{AU}$ )	1.100
No effect	1.800
No part	0.000
<b>Total failure rate (safety function)</b>	<b>1.300</b>
<b>SFF<sup>3</sup></b>	<b>(91%)</b>
<b>SIL AC<sup>4</sup></b>	<b>(SIL3)</b>

<sup>3</sup> A HART multiplexer is no element in terms of IEC 61508. Only a negative influence on  $\lambda_{DU}$  can occur. The calculated SFF is thereby not applicable for the given product.

<sup>4</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled. This HART multiplexer is no element in terms of IEC 61508.

**Table 3: Failure rates for Option 3**

Failure category	Failure rates (in FIT)
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0.000</b>
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>0.000</b>
<b>Fail Dangerous Detected (<math>\lambda_{DD}</math>)</b>	<b>1.195</b>
Fail Dangerous Detected ( $\lambda_{DD}$ )	1.045
Fail High (H)	0.000
Fail Low (L)	0.150
Fail Annunciation Detected ( $\lambda_{AD}$ )	0.000
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>0.405</b>
Fail Annunciation Undetected ( $\lambda_{AU}$ )	1.100
No effect	2.300
No part	0.000
<b>Total failure rate (safety function)</b>	<b>1.600</b>
<b>SFF<sup>5</sup></b>	<b>(75%)</b>
<b>SIL AC<sup>6</sup></b>	<b>(SIL2)</b>

<sup>5</sup> A HART multiplexer is no element in terms of IEC 61508. Only a negative influence on  $\lambda_{DU}$  can occur. The calculated SFF is thereby not applicable for the given product.

<sup>6</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled. This HART multiplexer is no element in terms of IEC 61508. Thereby, it may be used also in SIL3 applications.

**Table 4: Failure rates for Option 4**

Failure category	Failure rates (in FIT)
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0.000</b>
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>0.000</b>
<b>Fail Dangerous Detected (<math>\lambda_{DD}</math>)</b>	<b>1.045</b>
Fail Dangerous Detected ( $\lambda_{DD}$ )	1.045
Fail High (H)	0.000
Fail Low (L)	0.000
Fail Annunciation Detected ( $\lambda_{AD}$ )	0.000
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>0.055</b>
Fail Annunciation Undetected ( $\lambda_{AU}$ )	1.100
No effect	1.800
No part	0.000
<b>Total failure rate (safety function)</b>	<b>1.100</b>
<b>SFF<sup>7</sup></b>	<b>(95%)</b>
<b>SIL AC<sup>8</sup></b>	<b>(SIL3)</b>

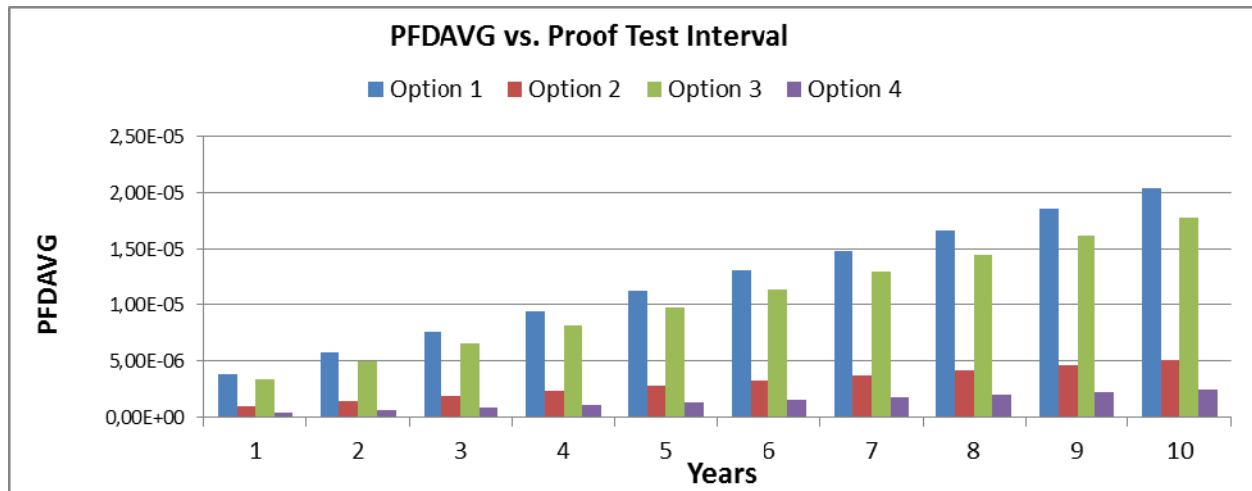
<sup>7</sup> A HART multiplexer is no element in terms of IEC 61508. Only a negative influence on  $\lambda_{DU}$  can occur. The calculated SFF is thereby not applicable for the given product.

<sup>8</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled. This HART multiplexer is no element in terms of IEC 61508.

**Table 5: PFD<sub>AVG</sub> Values**

Configuration	T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 5 years	T[Proof] = 10 years
Option 1	PFD <sub>AVG</sub> = 3,89E-06	PFD <sub>AVG</sub> = 7,56E-06	PFD <sub>AVG</sub> = 1,12E-05	PFD <sub>AVG</sub> = 2,04E-05
Option 2	PFD <sub>AVG</sub> = 9,82E-07	PFD <sub>AVG</sub> = 1,89E-06	PFD <sub>AVG</sub> = 2,80E-06	PFD <sub>AVG</sub> = 5,06E-06
Option 3	PFD <sub>AVG</sub> = 3,40E-06	PFD <sub>AVG</sub> = 6,59E-06	PFD <sub>AVG</sub> = 9,78E-06	PFD <sub>AVG</sub> = 1,78E-05
Option 4	PFD <sub>AVG</sub> = 4,83E-07	PFD <sub>AVG</sub> = 9,16E-07	PFD <sub>AVG</sub> = 1,35E-06	PFD <sub>AVG</sub> = 2,43E-06

The listed PFD<sub>AVG</sub> values are calculated for a proof test coverage of 90%.



**Figure 1: PFD<sub>AVG</sub> (t)**