



Failure Modes, Effects and Diagnostic Analysis

Project:

Smart Transmitter Power Supplies HiD2025/2026(SK) and
HiD2029/2030(SK)

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 04/05-08

Report No.: P+F 04/05-08 R018

Version V2, Revision R0, July 2011

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK) in the versions listed in the drawings referenced in section 2.4.1.

SK stands for "SINK" mode. In this version of the assessment report also the "SOURCE" mode of the considered modules was assessed. Therefore SK is put in brackets.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Failure rates used in this analysis are basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to $1,00E-03$.

The Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK) are considered to be Type A¹ subsystems with a hardware fault tolerance of 0.

For Type A subsystems the SFF has to be between 60% and 90% for SIL 2 subsystems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures. For these applications the following tables show how the above stated requirements are fulfilled under worst-case assumptions.

It is important to realize that the "no effect" 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.

The two channels on the two channel modules should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain safety function, as they contain common components.

¹ Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

Table 1: Summary for HiD2025/2026 – Failure rates

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S ²	DC _D ²
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	60 FIT	112 FIT	44 FIT	92 FIT	70,0%	32,4%	34,9%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	44 FIT	112 FIT	60 FIT	92 FIT	70,0%	28,2%	39,4%

Table 2: Summary for HiD2025/2026 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4,04E-04	PFD_{AVG} = 8,07E-04	PFD_{AVG} = 2,02E-03

Table 3: Summary for HiD2025/2026SK – Failure rates

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	63 FIT	117 FIT	48 FIT	93 FIT	70,8%	35,0%	34,0%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	48 FIT	117 FIT	63 FIT	93 FIT	70,8%	29,0%	40,3%

Table 4: Summary for HiD2025/2026 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4,09E-04	PFD_{AVG} = 8,18E-04	PFD_{AVG} = 2,04E-03



Table 5: Summary for HiD2029/2030(SK) – Failure rates

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	183 FIT	167 FIT	84 FIT	95 FIT	82,0%	52,2%	46,9%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	84 FIT	167 FIT	183 FIT	95 FIT	82,0%	33,4%	65,8%

Table 6: Summary for HiD2029/2030(SK) – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4,16E-04	PFD_{AVG} = 8,31E-04	PFD_{AVG} = 2,08E-03

² DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for the Smart Transmitter Power Supplies.

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$.

A user of the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK) can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 to 5.3 along with all assumptions.

The failure rates are valid for the useful life of the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK), which is estimated to be between 8 and 12 years (see Appendix 3).



Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards / Literature used.....	7
2.4 Reference documents.....	8
2.4.1 Documentation provided by the customer.....	8
2.4.2 Documentation generated by <i>exida</i>	8
3 Description of the analyzed modules	9
3.1 HiD2025/2026(SK).....	9
3.1.1 HiD2025/2026	9
3.1.2 HiD2025/2026SK	10
3.2 HiD2029/2030(SK).....	11
3.2.1 HiD2029/2030	11
3.2.2 HiD2029/2030SK	12
4 Failure Modes, Effects, and Diagnostics Analysis	13
4.1 Description of the failure categories.....	13
4.2 Methodology – FMEDA, Failure rates.....	14
4.2.1 FMEDA.....	14
4.2.2 Failure rates	14
4.2.3 Assumptions.....	14
4.2.4 Example explaining the behavior of the safety logic solver.....	15
5 Results of the assessment.....	16
5.1 HiD2025/2026	17
5.2 HiD2025/2026SK	19
5.3 HiD2029/2030(SK).....	21
6 Terms and Definitions	23
7 Status of the document	24
7.1 Liability	24
7.2 Releases	24
7.3 Release Signatures.....	24
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	25
Appendix 2: Impact of lifetime of critical components on the failure rate	26

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 document shall describe the results of the FMEDAs carried out on the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK).

It shall be assessed whether these devices meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 2 subsystems according to IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world's leading product certification and 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 global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed 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 Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK).

exida Performed the hardware assessment according to option 1 (see section 1).

Pepperl+Fuchs GmbH contracted *exida* in June 2004 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* 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

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	Failure Mode Effect Analysis – Elcon Isolator, Type HiD2030SK – Report; 30.03.00
[D2]	Circuit Diagram ES-984225-A1 – Electrical schematic Series 2000 Barrier Model HiD 2030SK; 11.02.00
[D3]	Component List CL-984225-A2 – HiD2030SK; 11.02.00
[D4]	Circuit Diagram 351-0052 – HiD 2029SK; 21.06.02
[D5]	E-mails dated March 7, 2001, May 2, 2001 and May 5, 2001 from Elcon Instruments to <i>exida</i> with description about the differences in “source” mode and in “sink” mode
[D6]	data-sheet-HiD2026.pdf
[D7]	data-sheet-HiD2026SK.pdf
[D8]	FS0067PF-25.doc of 04.07.11 - Impact Analysis about re-design of HiD2025, HiD2026, HiD2025SK, HiD2026SK
[D9]	3521062a.pdf - 352-1062A Part list HiD2026 of 20.12.10
[D10]	3521063a.pdf - 352-1063A Part list HiD2026SK of 20.12.10
[D11]	3510472a.pdf - Circuit Diagram 351-0472A of 26.02.08 for HiD2026 and HiD2026SK
[D12]	FMEDA FS0067PF-26.xls of 12.05.11
[D13]	FMEDA FS0067PF-26_2.xls of 12.05.11
[D14]	RE Redesign HiD2025-2026 HiD2025-2026SK.msg of 25.07.11

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V5 HiD2026 V0 R1.1.xls of 23.08.04
[R2]	FMEDA V5 HiD2026SK V0 R1.1.xls of 23.08.04
[R3]	FMEDA V5 HiD2030SK V0 R1.1.xls of 08.09.04

3 Description of the analyzed modules

3.1 HiD2025/2026(SK)

Outputs are isolated from the inputs and are referenced to the power supply common.

The Smart Transmitter Power Supplies HiD2025/2026(SK) are considered to be Type A subsystems with a hardware fault tolerance of 0.

The Smart Transmitter Power Supply HiD2025(SK) is a single channel module. The Smart Transmitter Power Supply HiD2026(SK) consists of two channels as shown in Figure 1.

3.1.1 HiD2025/2026

The HiD2025/2026 modules provide a fully floating supply to power a two wire transmitter in a Hazardous Area, repeating the current to drive a Safe Area load. Bi-directional communication is provided for smart transmitters which use current modulation to transmit data and voltage modulation to receive data.

The specified operating range is 4-20 mA or 1-5V.

The voltage output is obtained by shunting the 4-20mA current output.

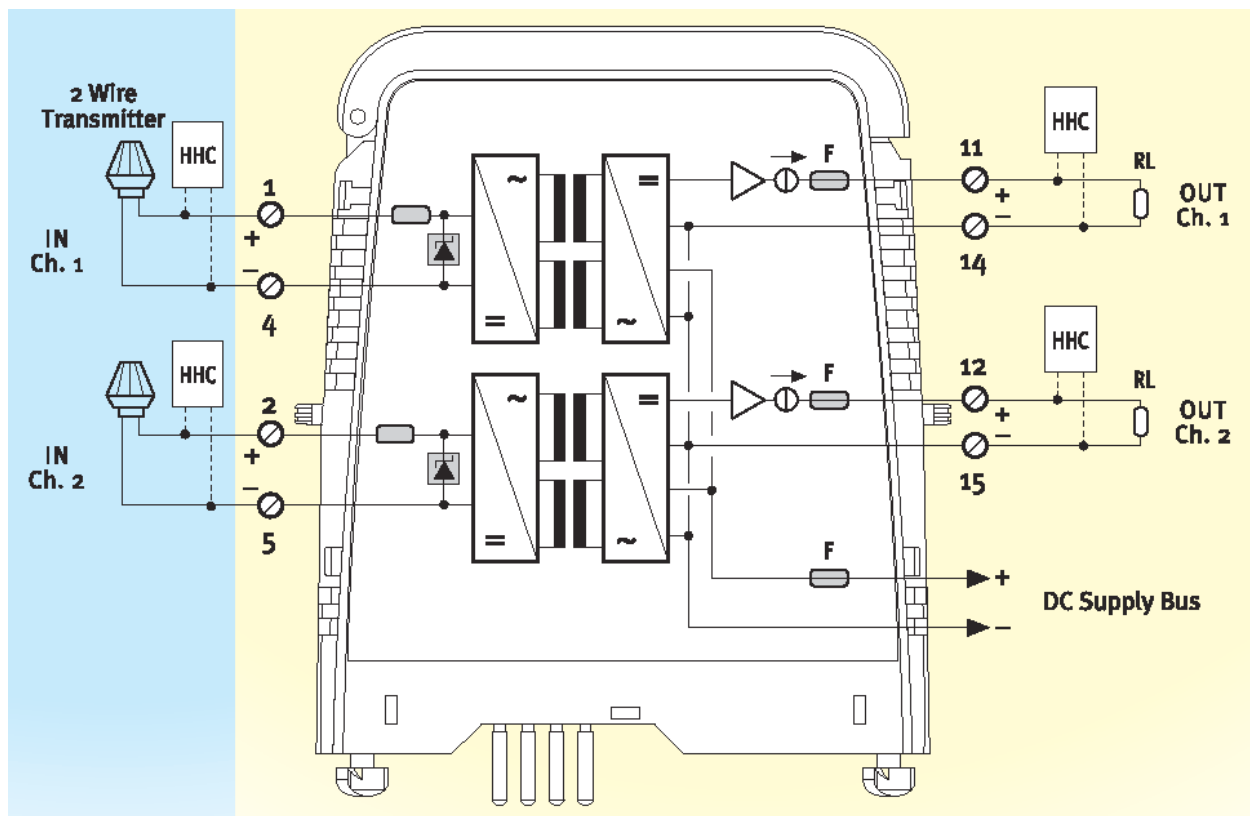


Figure 1: Block diagram of HiD2026

3.1.2 HiD2025/2026SK

The HiD2025/2026SK modules provide a fully floating supply to power a two wire transmitter in a Hazardous Area, repeating the current in sink mode to simulate a two wire transmitter load in Safe Area. Bi-directional communication is provided for smart transmitters which use current modulation to transmit data and voltage modulation to receive data.

The outputs are sink mode. Thus an external power supply must be connected to the output terminal.

The specified operating range is 4-20 mA.

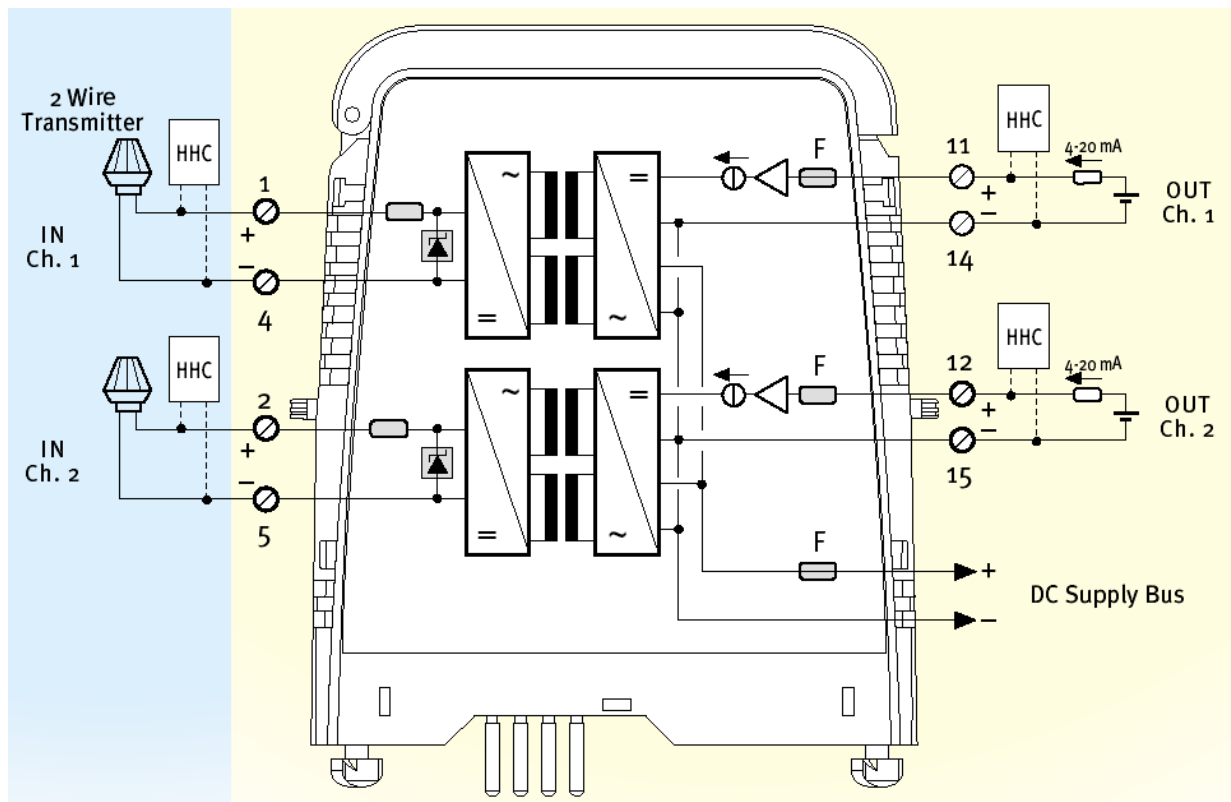


Figure 2: Block diagram of HiD2026SK

3.2 HiD2029/2030(SK)

Outputs are isolated from the inputs, the power supply and each other.

The specified operating range is 4-20 mA.

The Smart Transmitter Power Supplies HiD2029/2030(SK) are considered to be Type A subsystems with a hardware fault tolerance of 0.

The Smart Transmitter Power Supply HiD2029(SK) is a single channel module. The Smart Transmitter Power Supply HiD2030(SK) consists of two channels as shown in Figure 1.

3.2.1 HiD2029/2030

The HiD2029/2030 modules provide a fully floating supply to power a two or three wire transmitter in a Hazardous Area, repeating the current to drive a Safe Area load. Bi-directional communication is provided for smart transmitters which use current modulation to transmit data and voltage modulation to receive data.

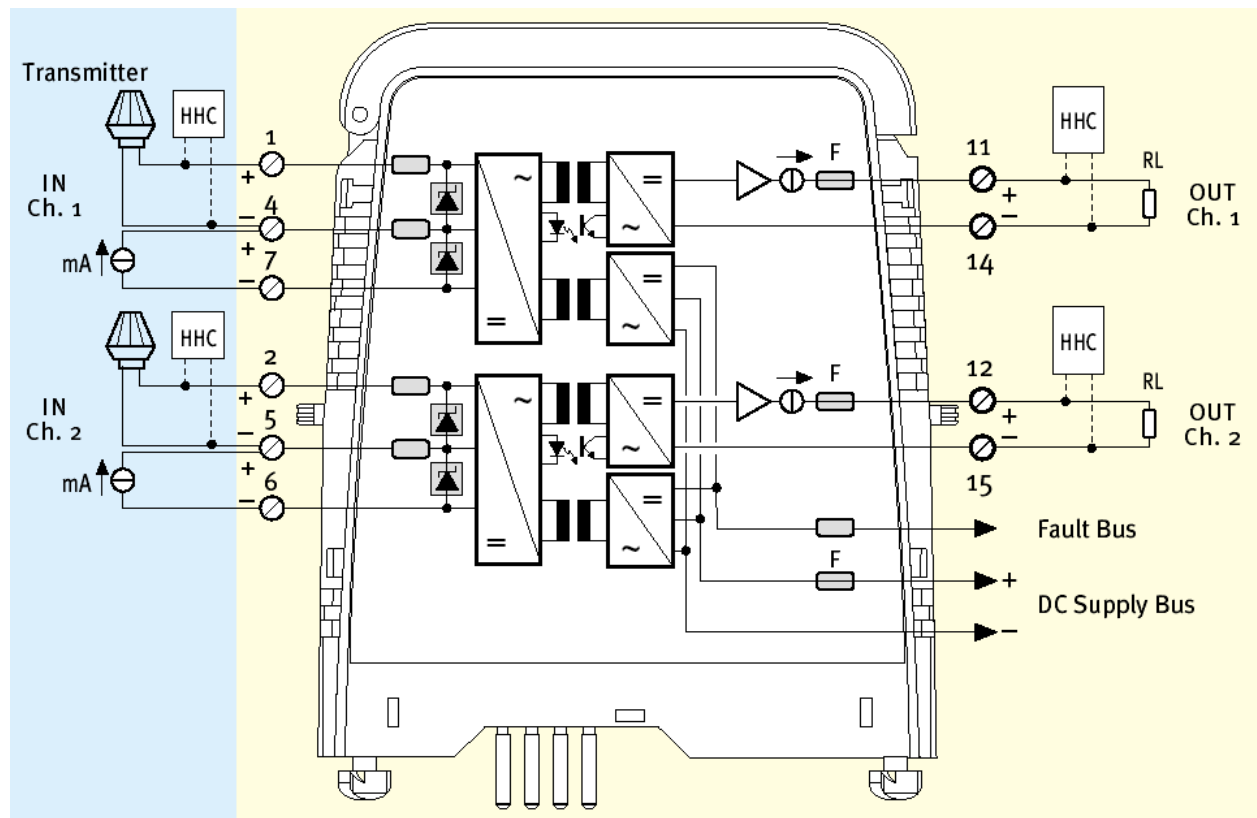


Figure 3: Block diagram of HiD2030

3.2.2 HiD2029/2030SK

The HiD2029/2030SK modules provide a fully floating supply to power a two or three wire transmitter in a Hazardous Area, repeating the current in sink mode to simulate a two wire transmitter load in Safe Area. Bi-directional communication is provided for smart transmitters which use current modulation to transmit data and voltage modulation to receive data.

The outputs are sink mode. Thus an external power supply must be connected to the output terminal.

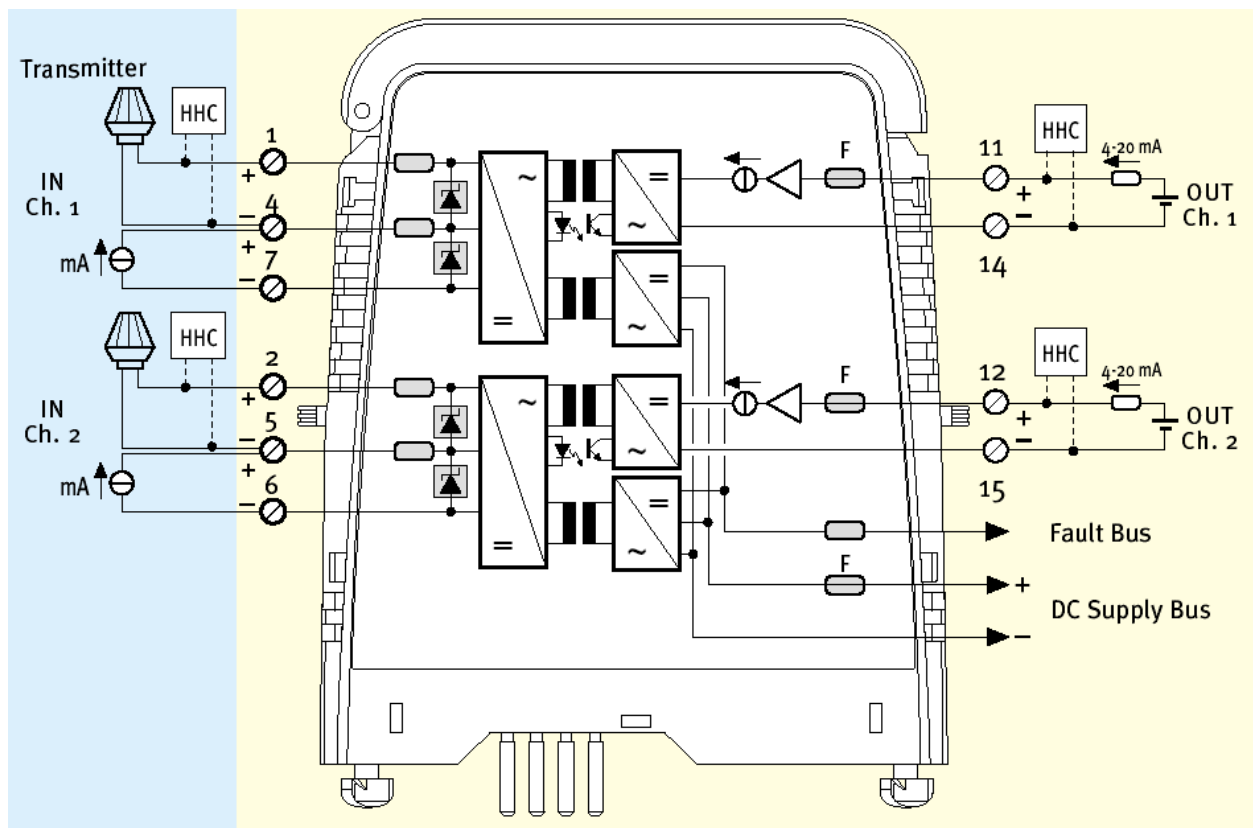


Figure 4: Block diagram of HiD2030SK

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs GmbH and is documented in [R1] to [R3].

4.1 Description of the failure categories

In order to judge the failure behavior of the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK), the following definitions for the failure of the product were considered.

Fail-Safe State	Depending on the application the fail-safe state is defined as the output leading to "fail high" or "fail low".
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 2% of full span.
Fail High	Failure that causes the output signal to go to the maximum output current ($> 20 \text{ mA}$)
Fail Low	Failure that causes the output signal to go to the minimum output current ($< 4 \text{ mA}$)
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output current by not more than 2% of full span. For the calculation of the SFF it is treated like a safe undetected failure.
Not considered	Not considered (!) means that this failure mode was not considered. When calculating the SFF this failure mode is divided into 25% fail high failures, 25% fail low failures and 50% dangerous failures.
Not part	Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application programming of the safety logic solver a fail low or fail high can either be dangerous detected or safe detected. Consequently during a Safety Integrity Level (SIL) verification assessment the fail high and fail low categories need to be classified as either safe detected (S) or dangerous detected (DD).

The "no effect" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508:2000. In IEC 61508:2000 the "no effect" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 645-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- The 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.
- External power supply failure rates are not included.
- The separate fault output of the HiD2029/2030(SK) modules which signals if the input signal is outside the range 0.2-24 mA, is not considered in the FMEDA and the calculations.

4.2.4 Example explaining the behavior of the safety logic solver

The following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value is below a predefined low set value. A current < 4mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 20mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The SPLC Detection Behavior in Table 7 represents the under-range and over-range detection capability of the connected safety logic solver.

Table 7 Application example

Application	SPLC Detection Behavior	λ_{low}	λ_{high}
Low trip	< 4mA	= λ_{sd}	= λ_{du}
Low trip	> 20mA	= λ_{su}	= λ_{dd}
Low trip	< 4mA and > 20mA	= λ_{sd}	= λ_{dd}
High trip	< 4mA	= λ_{dd}	= λ_{su}
High trip	> 20mA	= λ_{du}	= λ_{sd}
High trip	< 4mA and > 20mA	= λ_{dd}	= λ_{sd}

In this analysis it is assumed that the safety logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

5 Results of the assessment

exida did the FMEDAs together with Pepperl+Fuchs.

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

λ_{total} consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect}$$

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

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

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

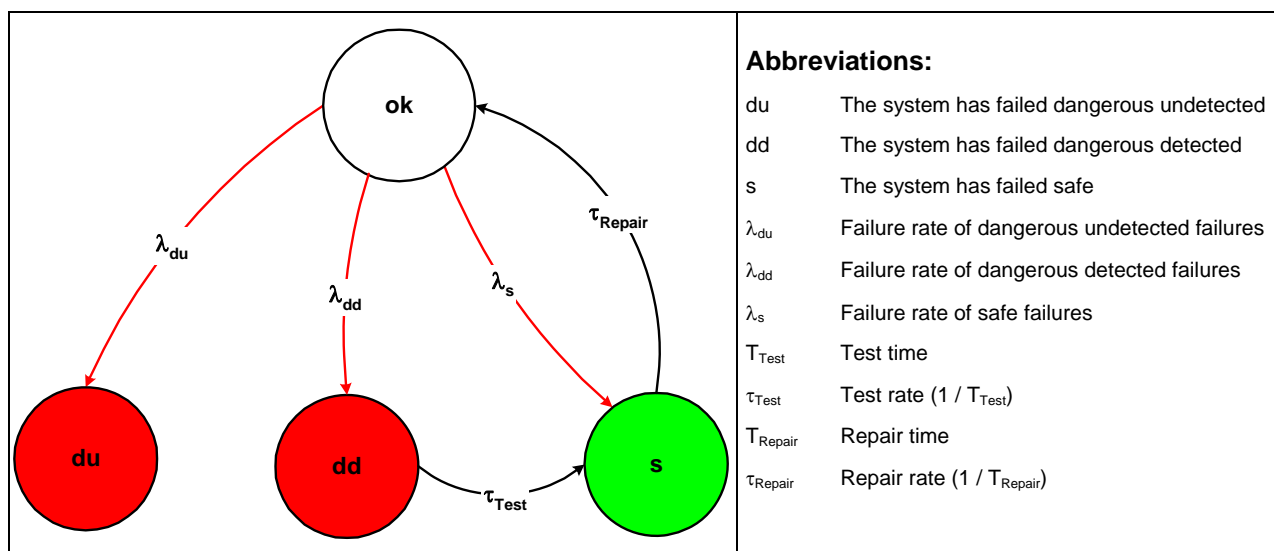


Figure 5: Markov model for a 1oo1D structure

5.1 HiD2025/2026

The FMEDA carried out on HiD2025/2026 leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

$$\lambda_{du} = 6,00E-08 \text{ 1/h}$$

$$\lambda_{high} = 2,79E-08 \text{ 1/h}$$

$$\lambda_{low} = 4,41E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,12E-07 \text{ 1/h}$$

$$\lambda_{not \text{ considered}} = 6,43E-08 \text{ 1/h}$$

$$\lambda_{total} = 3,08E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 7,10E-09 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 362 \text{ years}$$

Under the assumptions described in section 4.2.4 and 5 the following tables show the failure rates according to IEC 61508:2000 depending on whether fail low / fail high was considered to be dangerous detected or safe detected to:

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	60 FIT	112 FIT	44 FIT	92 FIT	70,08%	32,40%	34,90%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	44 FIT	112 FIT	60 FIT	92 FIT	70,08%	28,20%	39,47%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
$PFD_{AVG} = 4,04E-04$	$PFD_{AVG} = 8,07E-04$	$PFD_{AVG} = 2,02E-03$

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$. Figure 6 shows the time dependent curve of PFD_{AVG} .

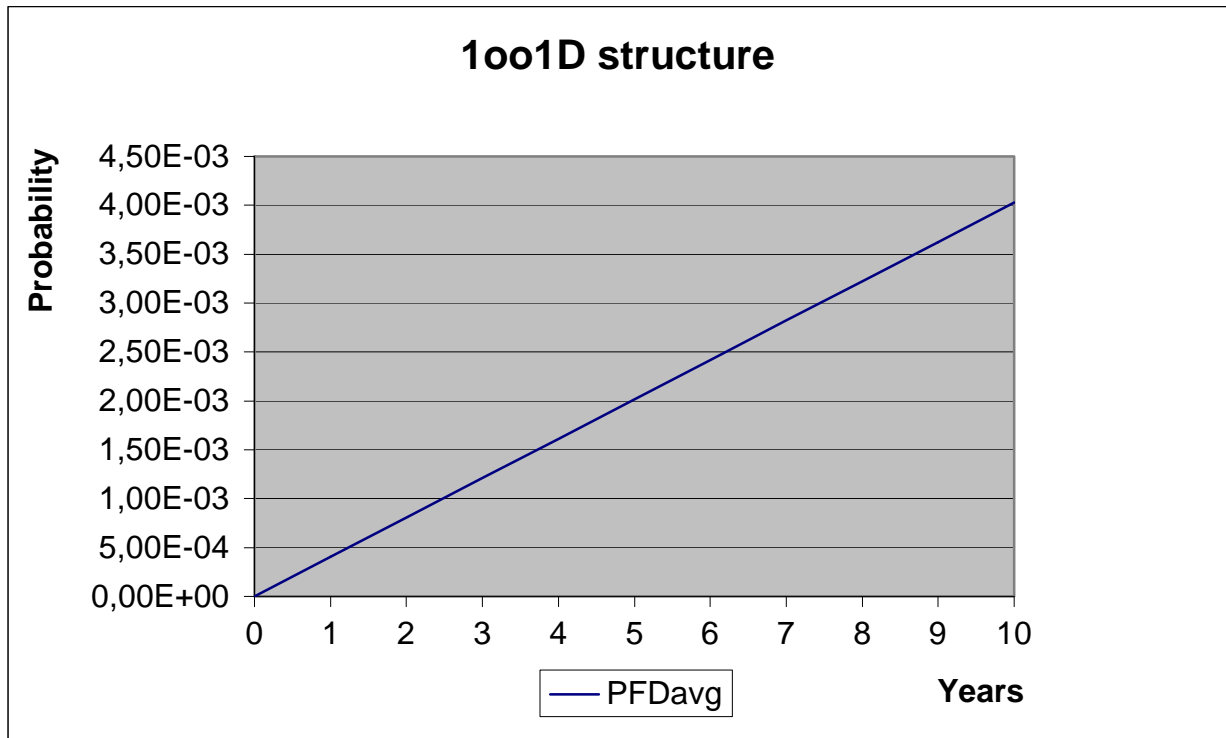


Figure 6: PFD_{AVG}(t) of HiD2025/2026

5.2 HiD2025/2026SK

The FMEDA carried out on HiD2025/2026SK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

$$\lambda_{du} = 6,05E-08 \text{ 1/h}$$

$$\lambda_{high} = 3,12E-08 \text{ 1/h}$$

$$\lambda_{low} = 4,67E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,17E-07 \text{ 1/h}$$

$$\lambda_{not \text{ considered}} = 6,58E-08 \text{ 1/h}$$

$$\lambda_{total} = 3,21E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 7,10E-09 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 348 \text{ years}$$

Under the assumptions described in section 4.2.4 and 5 the following tables show the failure rates according to IEC 61508:2000 depending on whether fail low / fail high was considered to be dangerous detected or safe detected to:

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	63 FIT	117 FIT	48 FIT	93 FIT	70,89%	35,00%	34,04%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	48 FIT	117 FIT	63 FIT	93 FIT	70,89%	29,09%	40,38%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 4,09E-04	PFD _{AVG} = 8,18E-04	PFD _{AVG} = 2,04E-03

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 6 shows the time dependent curve of PFD_{AVG}.

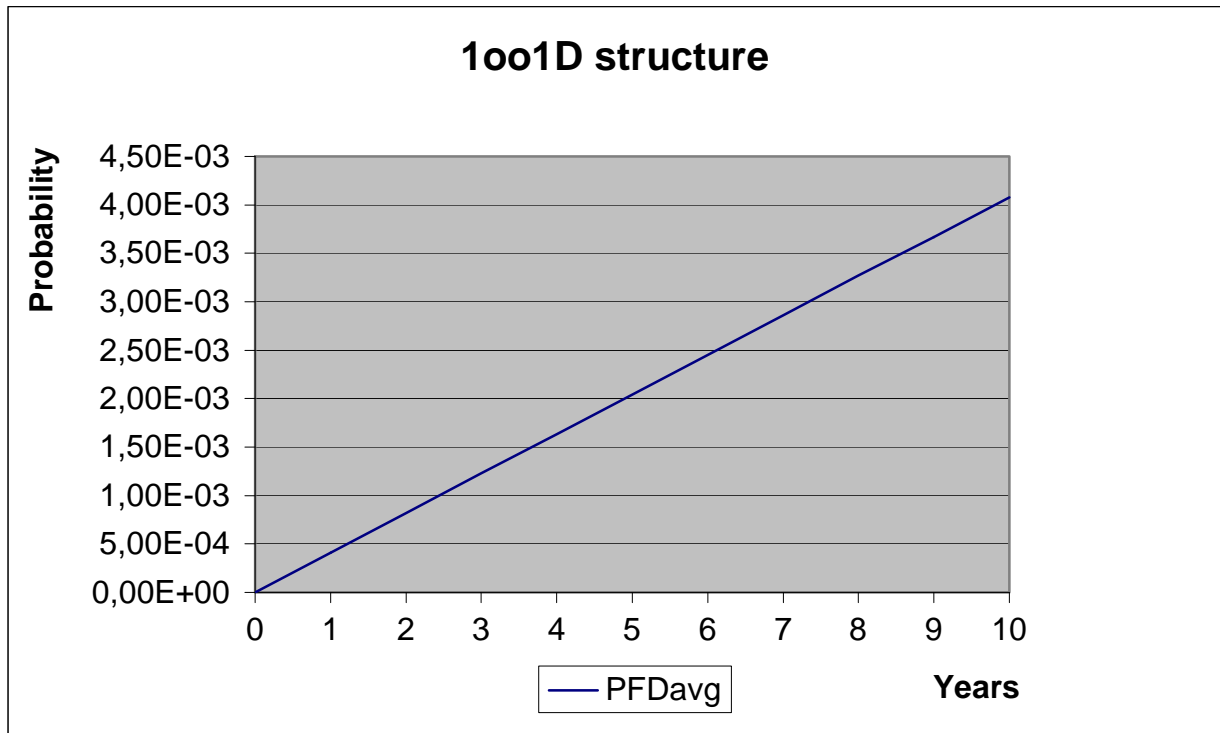


Figure 7: PFD_{AVG}(t) of HiD2025/2026SK

5.3 HiD2029/2030(SK)

The FMEDA carried out on HiD2029/2030(SK) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

$$\lambda_{du} = 3,61E-08 \text{ 1/h}$$

$$\lambda_{high} = 5,47E-08 \text{ 1/h}$$

$$\lambda_{low} = 1,53E-07 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,67E-07 \text{ 1/h}$$

$$\lambda_{not \text{ considered}} = 1,18E-07 \text{ 1/h}$$

$$\lambda_{total} = 5,28E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,84E-08 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 205 \text{ years}$$

Under the assumptions described in section 4.2.4 and 5 the following tables show the failure rates according to IEC 61508:2000 depending on whether fail low / fail high was considered to be dangerous detected or safe detected to:

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	183 FIT	167 FIT	84 FIT	95 FIT	82,03%	52,29%	46,93%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	84 FIT	167 FIT	183 FIT	95 FIT	82,03%	33,47%	65,83%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 4,16E-04	PFD _{AVG} = 8,31E-04	PFD _{AVG} = 2,08E-03

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 6 shows the time dependent curve of PFD_{AVG}.

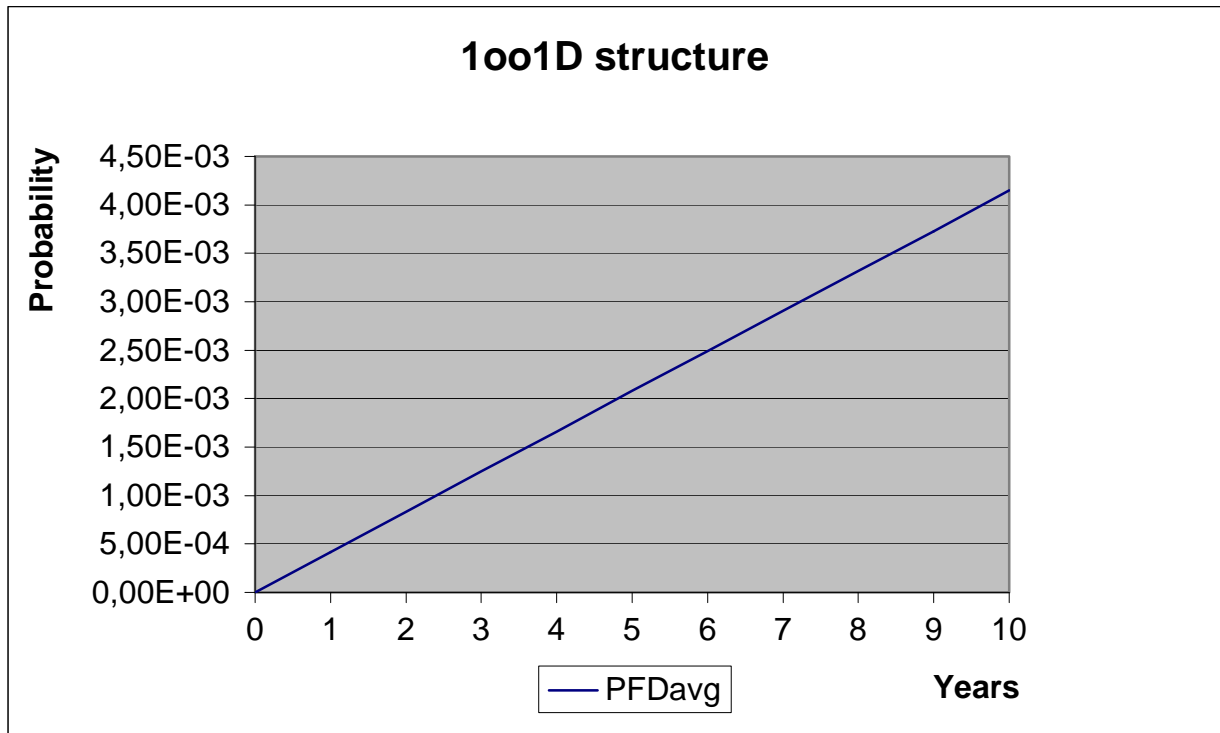


Figure 8: PFD_{AVG}(t) of HiD2029/2030(SK)

6 Terms and Definitions

DC _S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC _D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A subsystem	"Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida 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.

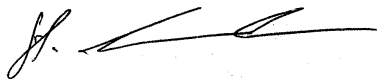
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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: V2R0: PIU statements removed, HiD2025/2026(SK) updated;
July 25, 2011
V1, R1.1: Single channel versions added; January 20, 2005
V1, R1.0: Review comments integrated; October 13, 2004
V0, R1.1: Proven-in-use section completed; September 22, 2004
V0, R1.0: Initial version, September 8, 2004
Authors: Stephan Aschenbrenner
Review: V0, R1.0: Rachel Amkreutz (*exida*), October 11, 2004
Release status: Released to Pepperl+Fuchs

7.3 Release Signatures

A handwritten signature in black ink, appearing to be "S. Aschenbrenner".

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

A handwritten signature in black ink, appearing to be "R. Faller".

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

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Appendix 1 and 2 should be considered when writing the safety manual as they contain important safety related information.

Appendix 2: Impact of lifetime of critical components on the failure rate

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

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

The circuits of the Smart Transmitter Power Supplies HiD2025/2026(SK) and HiD2029/2030(SK) do not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

However, according to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.7.4 note 3 of IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.