Failure Modes, Effects and Diagnostic Analysis

Project:
Repeater / Driver / Interface Boards
D1010, D1014, D1020, D1021, D1032, D1033, D1034

Customer:

G.M. International s.r.l
Villasanta
Italy

Contract No.: GM 03/07-24
Report No.: GM 03/07-24 R001
Version V2, Revision R1, November 2006
Stephan Aschenbrenner

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

Management summary

This report summarizes the results of the hardware assessment carried out on the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034. Table 1 gives an overview of the different types that have been assessed.

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

Table 1: Overview of the assessed boards

Type	Function	Output channels
D1010[1]	Repeater Power Supply	1/2
D1014	Repeater Power Supply (HART compatible)	1/2
D1020	Powered Isolating Driver	1/2
D1021	Powered Isolating Driver with fault detection	1
D1032	Switch/Proximity Detector Repeater (relay output)	2/4
D1033	Switch/Proximity Detector Repeater (transistor output)	2/4
D1034	Contact/Proximity Detector Interface	1/2

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

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

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 and $\geq 10^{-4}$ 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.

For a SIL 2 application the total PFD_{AVG} value of the SIF must be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the assessed boards would then be 1,00E-03.

For a SIL 3 application the total PFD_{AVG} value of the SIF must be smaller than 1,00E-03, hence the maximum allowable PFD_{AVG} value for the assessed boards would then be 1,00E-04.

The Repeater / Driver / Interface Boards are considered to be Type A[2] components with a hardware fault tolerance of 0.

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

For Type A components the SFF has to be between 90% and 99% for SIL 3 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

[1] D1010 also exists in the versions D1010S-054, D1010S-056 and D1010S-057. These devices are mV to mA converters and use the passive input on a standard D1010S.

[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.

Assuming that the application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled (considering one input / one output being part of the safety function).

Summary for D1010 – active input

Table 2: Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**126**
Fail dangerous detected (internal diagnostics or indirectly[3])	1
Fail high (detected by the logic solver)	34
Fail low (detected by the logic solver)	91
Fail Dangerous Undetected	**36**
No Effect	**201**
Not part	**69**
MTBF = MTTF + MTTR	**265 years**

Table 3: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [4]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [5]	**DC_D** [5]
0 FIT	201 FIT	126 FIT	36 FIT	90%	0%	77%

Table 4: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,58E-04	PFD_{AVG} = 7,88E-04	PFD_{AVG} = 1,58E-03

[3] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[4] Note that the SU category includes failures that do not cause a spurious trip

[5] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Summary for D1010 passive input

Table 5: Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**142**
Fail dangerous detected (internal diagnostics or indirectly[6])	1
Fail high (detected by the logic solver)	34
Fail low (detected by the logic solver)	107
Fail Dangerous Undetected	**41**
No Effect	**236**
Not part	**13**
MTBF = MTTF + MTTR	**265 years**

Table 6: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [7]	λ_{DD}	λ_{DU}	**SFF**	DC_S [8]	DC_D [8]
0 FIT	236 FIT	142 FIT	41 FIT	90%	0%	77%

Table 7: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,79E-04	PFD_{AVG} = 8,92E-04	PFD_{AVG} = 1,78E-03

[6] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[7] Note that the SU category includes failures that do not cause a spurious trip

[8] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Summary for D1010S-054, -056, -057

Table 8: Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**119**
Fail dangerous detected (internal diagnostics or indirectly[9])	1
Fail high (detected by the logic solver)	36
Fail low (detected by the logic solver)	82
Fail Dangerous Undetected	**38**
No Effect	**200**
Not part	**6**
MTBF = MTTF + MTTR	**315 years**

Table 9: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [10]	λ_{DD}	λ_{DU}	SFF	DC_S [11]	DC_D [11]
0 FIT	200 FIT	119 FIT	38 FIT	89%	0%	75%

Table 10: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,66E-04	PFD_{AVG} = 8,30E-04	PFD_{AVG} = 1,66E-03

[9] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[10] Note that the SU category includes failures that do not cause a spurious trip

[11] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Summary for D1014

Table 11: Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**147**
Fail dangerous detected (internal diagnostics or indirectly[12])	0
Fail high (detected by the logic solver)	42
Fail low (detected by the logic solver)	105
Fail Dangerous Undetected	**22**
No Effect	**182**
Not part	**15**
MTBF = MTTF + MTTR	**312 years**

Table 12: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [13]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [14]	**DC_D** [14]
0 FIT	182 FIT	147 FIT	22 FIT	93%	0%	87%

Table 13: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 9,43E-05	PFD_{AVG} = 4,71E-04	PFD_{AVG} = 9,42E-04

Summary for D1020

Table 14: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [13]	λ_{DD}	λ_{DU}	**SFF**
0 FIT	292 FIT	0 FIT	86 FIT	77%

Table 15: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 3,78E-04	PFD_{AVG} = 1,89E-03	PFD_{AVG} = 3,77E-03

[12] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[13] Note that the SU category includes failures that do not cause a spurious trip

[14] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Summary for D1021

Table 16: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [15]	λ_{DD}	λ_{DU}	SFF
0 FIT	285 FIT	0 FIT	118 FIT	70%

Table 17: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 5,18E-04	PFD_{AVG} = 2,59E-03	PFD_{AVG} = 5,16E-03

Summary for D1032

Table 18: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [15]	λ_{DD}	λ_{DU}	SFF
0 FIT	210 FIT	0 FIT	28 FIT	88%

Table 19: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,20E-04	PFD_{AVG} = 6,02E-04	PFD_{AVG} = 1,20E-03

Summary for D1033

Table 20: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [15]	λ_{DD}	λ_{DU}	SFF
0 FIT	212 FIT	0 FIT	35 FIT	85%

Table 21: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,55E-04	PFD_{AVG} = 7,72E-04	PFD_{AVG} = 1,54E-03

[15] Note that the SU category includes failures that do not cause a spurious trip

Summary for D1034

Table 22: Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**102**
Fail dangerous detected (internal diagnostics or indirectly[16])	0
Fail high (detected by the logic solver)	38
Fail low (detected by the logic solver)	64
Fail Dangerous Undetected	**20**
No Effect	**185**
Not part	**6**
MTBF = MTTF + MTTR	**365 years**

Table 23: Failure rates according to IEC 61508

λ_{SD}	λ_{SU} [17]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [18]	**DC_D** [18]
0 FIT	185 FIT	102 FIT	20 FIT	93%	0%	83%

Table 24: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 8,70E-05	PFD_{AVG} = 4,35E-04	PFD_{AVG} = 8,69E-04

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 / SIL 3 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 or 1,00E-04, respectively. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 / SIL 3 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 or 1,00E-04, respectively.

A user of the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates for different operating conditions is presented in section 5.1 to 5.9 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The two channels on the D1010 and D1020 boards and the four channels on the D1032 and D1033 boards 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.

[16] “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[17] Note that the SU category includes failures that do not cause a spurious trip

[18] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the development process

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

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics. In addition, this option includes an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and may help justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices when combined with plant specific proven-in-use records.

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 EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This assessment shall be done according to option 1.

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034. Table 1 gives an overview of the different types which have been assessed.

The information in this report can be used to evaluate whether the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per 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 knowledge companies specializing in automation system safety and availability with over 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida* is a partnership 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

G.M. International s.r.l	Manufacturer of the assessed Repeater / Driver / Interface Boards
exida	Performed the hardware assessment according to option 1 (see section 1).

G.M. International s.r.l contracted *exida* in September 2006 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	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]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components
[N7]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	TRP025_r1.doc of 02.02.04	FMEDA report for D1021
[D2]	TRP026_r1.doc of 02.02.04	FMEDA report for D1032
[D3]	TRP027_r1.doc of 02.02.04	FMEDA report for D1033
[D4]	Data sheet DTS0016-7	Repeater Power Supply - Smart Compatible DIN-Rail - Models D1010 S - D1010 D
[D5]	Data sheet DTS0181-1	High Integrity - SIL 2 - Repeater Power Supply - Hart Compatible for Safety-Related Systems DIN-Rail Models D1014 S - D1014 D
[D6]	Data sheet DTS0017-5	Powered Isolating Driver - Smart Compatible DIN-Rail - Models D1020 S - D1020 D
[D7]	Data sheet DTS0133-4	Powered Isolating Driver with fault detection - Smart Compatible - DIN-Rail Model D1021 S
[D8]	Data sheet DTS0148-2	Switch/Proximity Detector Repeater - Relay Output DIN-Rail - Models D1032 D - D1032 Q
[D9]	Data sheet DTS0151-2	Switch/Proximity Detector Repeater - Transistor Output DIN-Rail - Models D1033 D - D1033 Q
[D10]	Data sheet DTS0182-1	High Integrity - SIL 2 - Contact/Proximity Detector Interface for Safety-Related Systems - DIN-Rail Models D1034 S - D1034 D
[D11]	SCD009.PDF	Circuit diagram “D1010 Repeater Power Supply DIN Rail” Rev. 5
[D12]	SCD048.PDF	Circuit diagram “D1011-D1014-D1034 Repeater Power Supply DIN Rail” Rev. 2
[D13]	SCD012.PDF	Circuit diagram “D1020 Isolating Driver DIN Rail” Rev. 6
[D14]	SCD020 Rev. 1	Circuit diagram D1021
[D15]	SCD022 Rev. 2	Circuit diagram D1032 and D1033
[D16]	PRL038.PDF	Parts list D1010D
[D17]	PRL039.PDF	Parts list D1010S
[D18]	PRL175.pdf	Parts list D1010S-054
[D19]	PRL120.PDF	Parts list D1014S
[D20]	PRL122.PDF	Parts list D1014D
[D21]	PRL042.PDF	Parts list D1020D
[D22]	PRL043.PDF	Parts list D1020S
[D23]	PRL068 Rev. 1	Parts list D1021
[D24]	PRL083 Rev. 2	Parts list D1033
[D25]	PRL124.PDF	Parts list D1034S
[D26]	PRL125.PDF	Parts list D1034D
[D27]	FMEDA D1010S-054.xls of 19.09.06	

[D28]	FMEDA D1010S_Active_Input.xls of 06.09.06
[D29]	FMEDA D1010S_Passive_Input.xls of 06.09.06
[D30]	FMEDA D1014S.xls of 25.09.06
[D31]	FMEDA D1020S.xls of 14.09.06
[D32]	FMEDA D1034.xls of 25.09.06

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V5 R0.3 D1021 V1 R1.0.xls of 15.03.04
[R2]	FMEDA V5 R0.3 D1032 V1 R1.0.xls of 15.03.04
[R3]	FMEDA V5 R0.3 D1033 V1 R1.0.xls of 15.03.04
[R4]	FMEDA D1010S_Active_Input_SA2.xls of 03.11.06
[R5]	FMEDA D1010S_Passive_Input_SA2.xls of 03.11.06
[R6]	FMEDA D1010S-054_SA.xls of 02.11.06
[R7]	FMEDA D1014S_SA.xls of 30.10.06
[R8]	FMEDA D1020S_SA2.xls of 03.11.06
[R9]	FMEDA D1034_SA.xls of 31.10.06

3 Description of the analyzed module

3.1 Repeater Power Supply D1010

The single and dual channel DIN Rail Repeater Power Supply, D1010 S and D1010 D, provides a fully floating DC supply for energizing conventional 2-wire 4..20 mA Transmitter, or separately powered 3, 4 wire 4..20 mA Transmitter located in Hazardous Area, and repeats the current in floating circuit to drive a Safe Area load.

The circuit allows bi-directional communication signals, for Smart Transmitters.

1 or 2 channels intrinsically safe analog input for 2 wire loop powered or separately powered smart transmitters, provides 3 port isolation (input/output/supply) and current (source or sink) or voltage output signal.

The Repeater Power Supply D1010 is considered to be a Type A component with a hardware fault tolerance of 0.

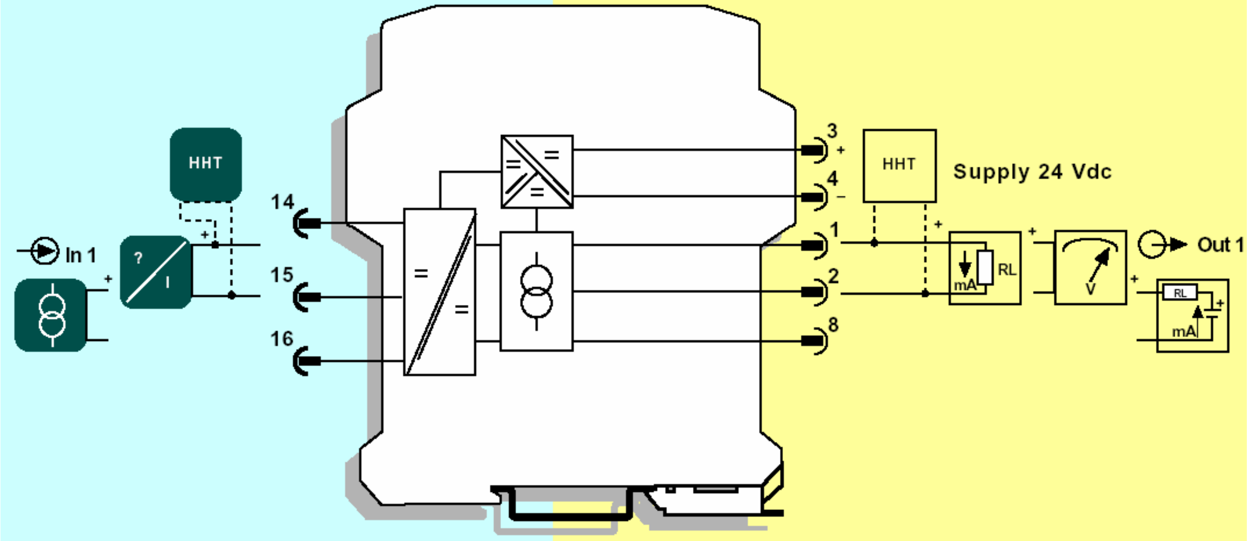


Figure 1: Repeater Power Supply D1010 S

3.2 mV / mA Converter D1010-054, -056, -057

The single channel DIN Rail mV / mA Converters D1010S-054, D1010S-056 and D1010S-057 convert a mV signal from sensors located in Hazardous Area, and repeat the current in floating circuit to drive a Safe Area load.

1 channel intrinsically safe analog input provides 3 port isolation (input/output/supply) and current (source) output signal.

The DIN Rail mV / mA Converters D1010S-054, D1010S-056 and D1010S-057 are considered to be Type A components with a hardware fault tolerance of 0.

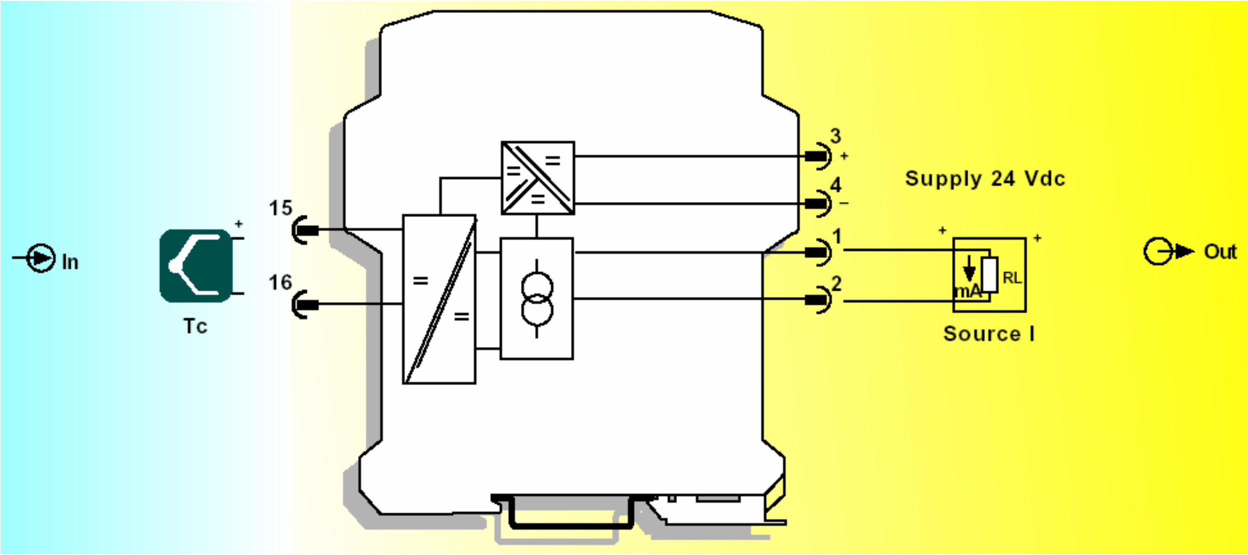


Figure 2: mV / mA Converters D1010S-054, D1010S-056 and D1010S-057

3.3 Repeater Power Supply (HART compatible) D1014

The single and dual channel DIN Rail Repeater Power Supply, D1014 S and D1014 D, provides a fully floating DC supply for energizing conventional 2-wire 4..20 mA transmitter located in hazardous area, and repeats the current in floating circuit to drive a safe area load.

The circuit allows bi-directional communication signals, for HART Transmitters.

1 or 2 channels intrinsically safe analog input for 2 wire loop powered HART transmitters, provides 3 port isolation (input/output/supply) and current (source or sink) or voltage output signal.

The Repeater Power Supply D1014 is considered to be a Type A component with a hardware fault tolerance of 0.

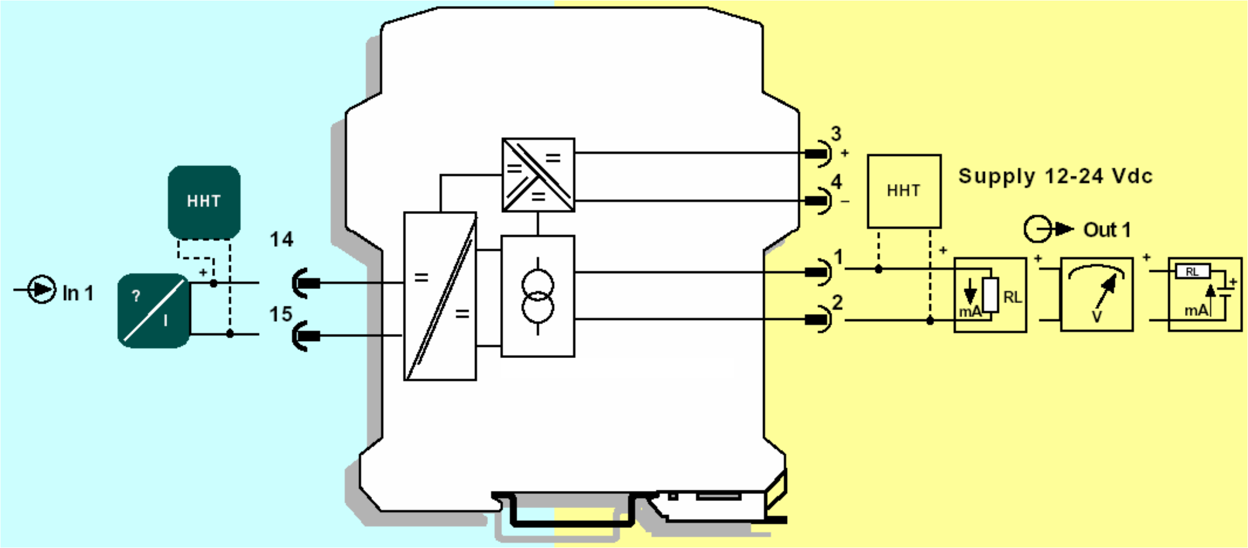


Figure 3: Repeater Power Supply D1014 S

3.4 Powered Isolating Driver D1020

The single and dual Isolating Driver, D1020 S and D1020 D, isolates and transfers a 4..20 mA signal from a controller located in safe area to a load of up to 750 Ohm in hazardous area.

The circuit allows bi-directional communication signals, for Smart I/P.

1 or 2 channels intrinsically safe analog output for 2 wire I/P Smart converters or valve positioners, provides 3 port isolation (input/output/supply).

The Powered Isolating Driver D1020 is considered to be a Type A component with a hardware fault tolerance of 0.

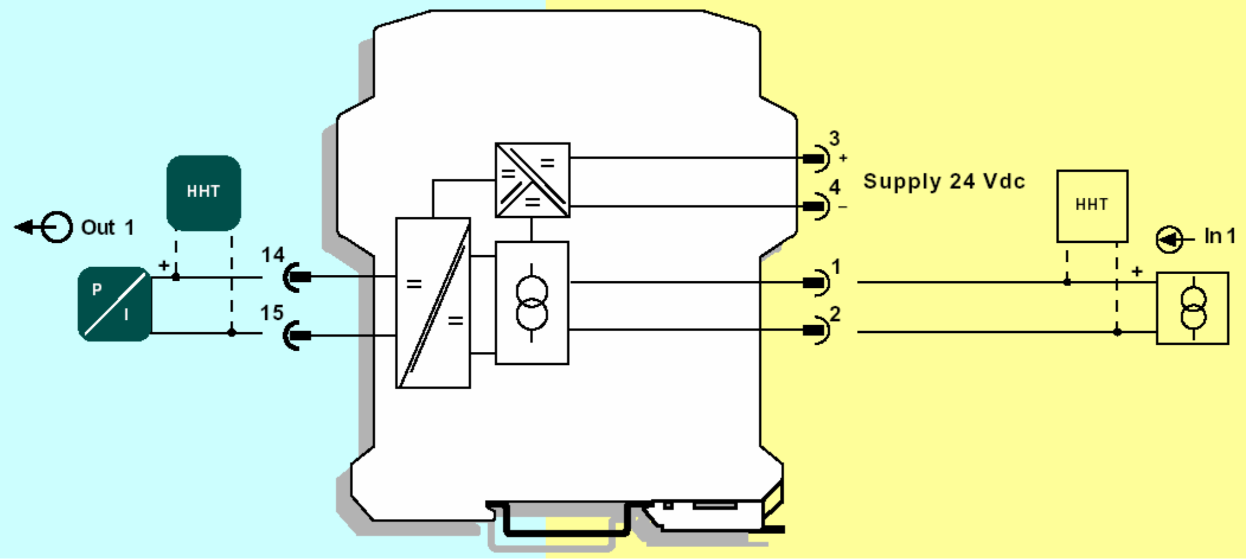


Figure 4: Powered Isolating Driver D1020 S

3.5 Powered Isolating Driver with fault detection D1021

The single Isolating Driver D1021 S isolates and transfers a 4..20 mA signal from a controller located in safe area to a load of up to 750 Ohm in hazardous area.

The circuit allows bi-directional communication signals, for Smart I/P.

In the 4..20 mA input range, a field open/short circuit (load or wire fault) reflects a high impedance to the control device output circuit and actuates (de-energizes) the fault indication relay/transistor.

An output under range or over range (< 1 mA or > 25 mA) also de-energizes the fault indication relay/transistor.

1 channel intrinsically safe analog output for 2 wire I/P Smart converters or valve positioners, provides 3 port isolation (input/output/supply).

The Powered Isolating Driver with fault detection D1021 is considered to be a Type A component with a hardware fault tolerance of 0.

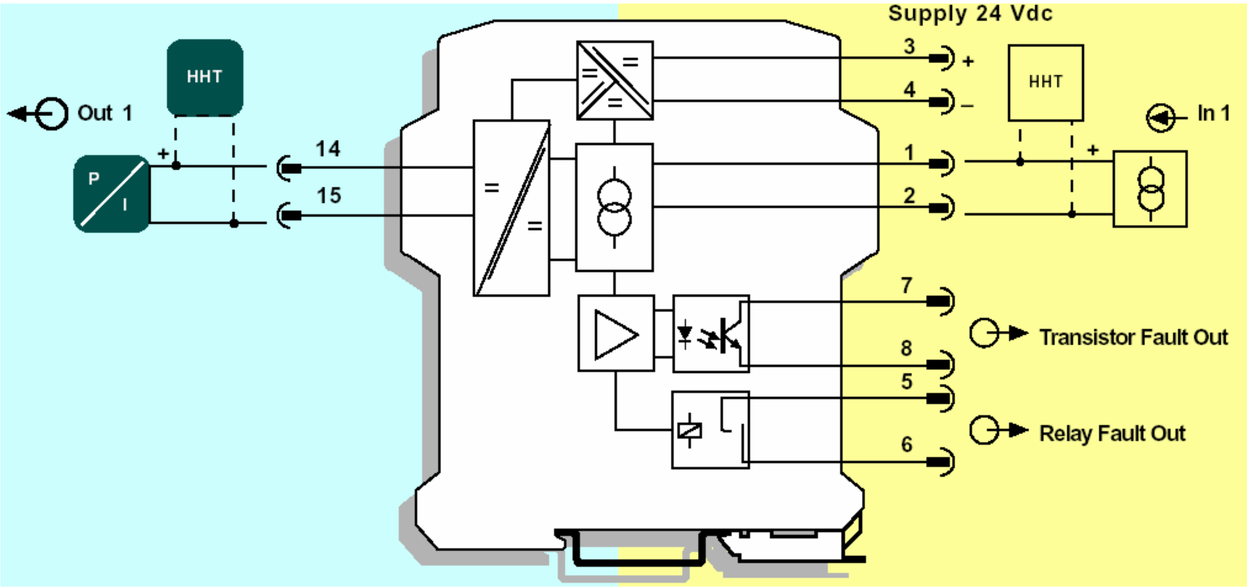


Figure 5: Powered Isolating Driver with fault detection D1021 S

3.6 Switch/Proximity Detector Repeater with relay output D1032

The Switch/Proximity Detector Repeater type D1032 is a DIN Rail unit configurable with two or four channels.

The unit can be configured for contact or proximity detector, NO or NC and for NE or ND relay output.

Each channel enables a safe area load to be controlled by a switch, or a proximity detector, located in hazardous area.

D1032 Q quad channel type has four input channels and actuates the corresponding output relay. Two actuation modes can be independently DIP switch configured on each input channel.

Contact or proximity sensor and its connection line short or open circuit fault detection is also DIP switch configurable.

D1032 D dual channel type has two input channels and four output relays; the unit has two DIP switch configurable operating modes.

2 or 4 channels intrinsically safe switch repeater for contact or proximity sensor provides 3 port isolation (input/output/supply).

The Switch/Proximity Detector Repeater with relay output D1032 is considered to be a Type A component with a hardware fault tolerance of 0.

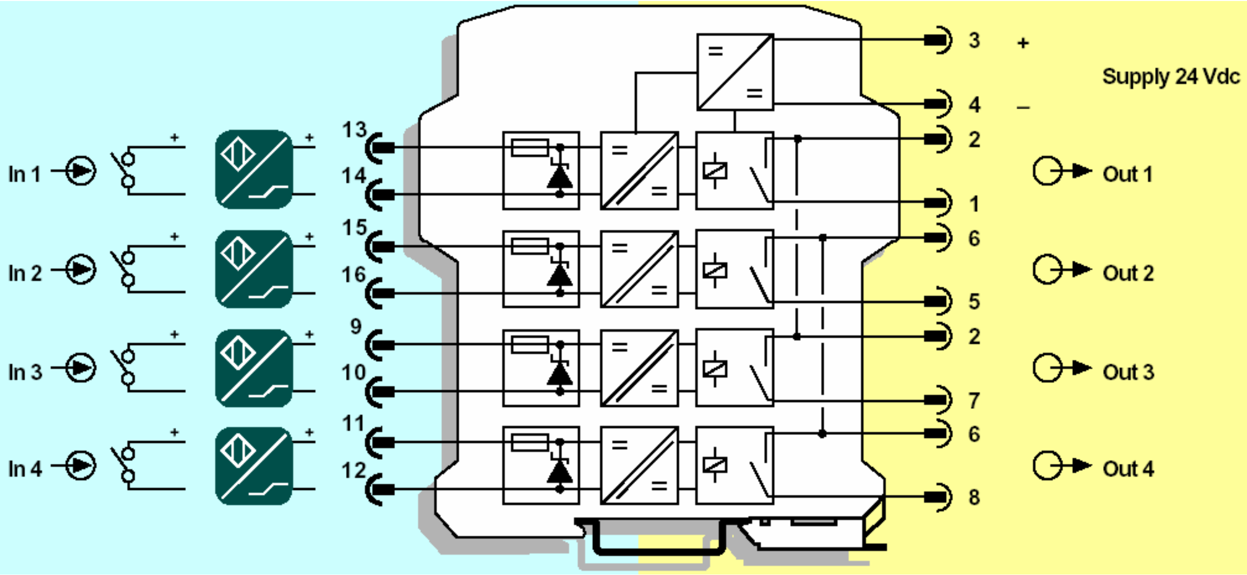


Figure 6: Switch/Proximity Detector Repeater with relay output D1032 Q

3.7 Switch/Proximity Detector Repeater with transistor output D1033

The Switch/Proximity Detector Repeater type D1033 is a DIN Rail unit configurable with two or four channels.

The unit can be configured for contact or proximity detector, NO or NC and for NO or NC opto-coupled open collector transistor output.

Each channel enables a safe area load to be controlled by a switch, or a proximity detector, located in hazardous area.

D1033 Q quad channel type has four input channels and actuates the corresponding output transistor. Two actuation modes can be independently DIP switch configured on each input channel.

Contact or proximity sensor and its connection line short or open circuit fault detection is also DIP switch configurable.

D1033 D dual channel type has two input channels and four output transistors; the unit has two DIP switch configurable operating modes.

2 or 4 channels intrinsically safe switch repeater for contact or DIN 19234 NAMUR proximity sensor provides 3 port isolation (input/output/supply).

The Switch/Proximity Detector Repeater with transistor output D1033 is considered to be a Type A component with a hardware fault tolerance of 0.

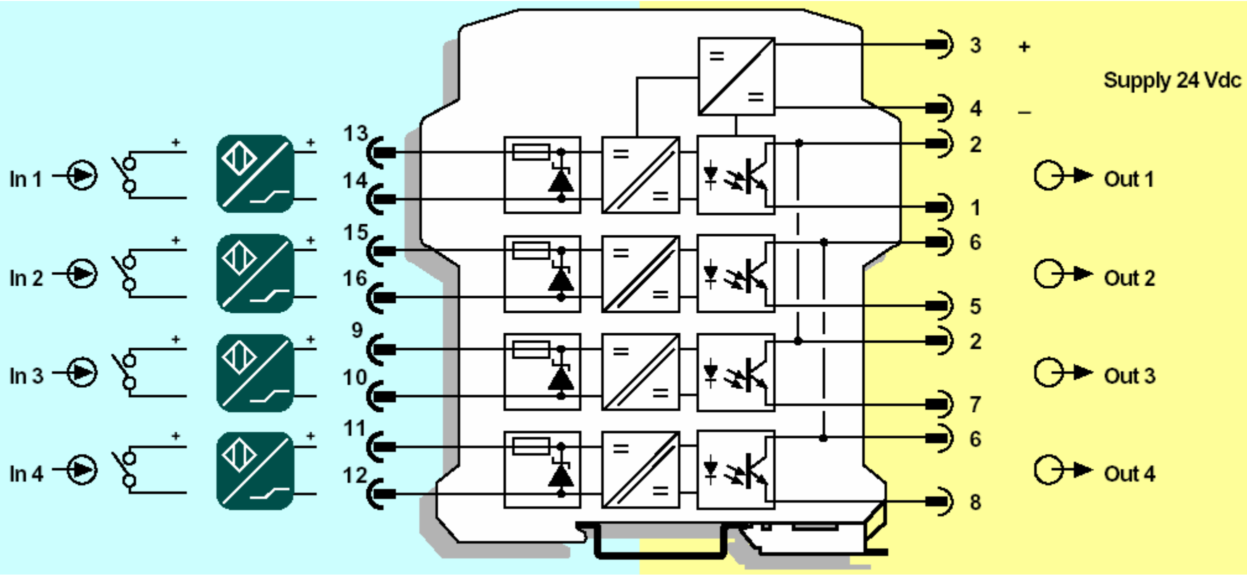


Figure 7: Switch/Proximity Detector Repeater with transistor output D1033 Q

3.8 Contact/Proximity Detector Interface D1034

D1034 is a single (D1034S) or double (D1034D) channel intrinsically safe interface with galvanic isolation, designed to interface contacts or proximity detectors.

Field loop integrity and status (line plus contact or proximity switch) are continuously monitored directly, in a transparent mode, into the PLC, ESD, DCS using their existing input line, without requiring an additional channel for failure detection.

1 or 2 totally independent and isolated channels intrinsically safe for contact or DIN 19234 NAMUR proximity switches provides 3 port isolation (input/output/supply).

The Contact/Proximity Detector Interface D1034 is considered to be a Type A component with a hardware fault tolerance of 0.

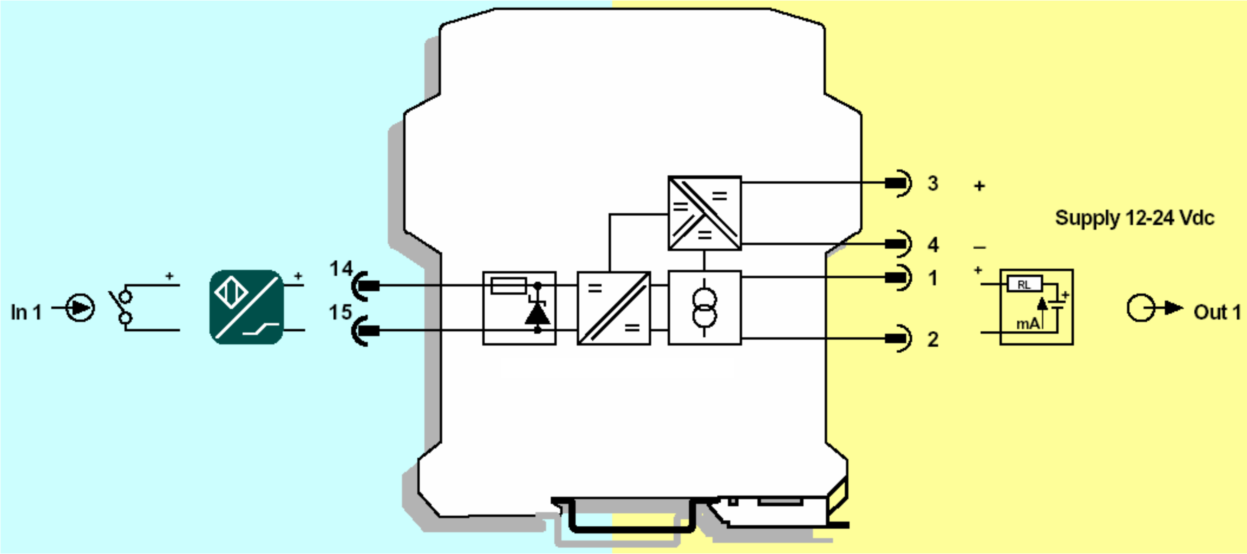


Figure 8: Contact/Proximity Detector Interface D1034 S

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis together with practical tests was done by G.M. International s.r.l (see [D1] to [D3] and [D27] to [D32]) and reviewed by *exida*. The results of the review are documented in [R1] to [R9].

4.1 Description of the failure categories

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

D1010, D1014:

Fail-Safe State — Depending on the application the fail-safe state is defined as the output going to fail low or fail high.

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

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 5% full span (+/- 0.8mA).

Fail High — Failure that causes the output signal to go to the maximum output current (> 21 mA)

Fail Low — Failure that causes the output signal to go to the minimum output current (< 3,6 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 5% of full span. For the calculation of the SFF it is treated like a safe undetected failure.

D1020, D1021:

Fail-Safe State — The fail-safe state is defined as the output going to fail low.

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

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 5% full span (+/- 0.8mA).

Fail High — Failure that causes the output signal to go to the maximum output current (> 21 mA)

Fail Low — Failure that causes the output signal to go to the minimum output current (< 3,6 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 5% of full span. For the calculation of the SFF it is treated like a safe undetected failure.

D1032, D1033:

Fail-Safe State — The fail-safe state is defined as the output being de-energized.

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

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).

D1034:

Fail-Safe State
The fail-safe state is defined as the output being below 1.2mA or above 7mA.

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

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; the output current remains between 2.1mA and 7mA).

Fail High
Failure that causes the output signal to go above 7mA (short circuit).

Fail Low
Failure that causes the output signal to go below 0.35 mA (lead breakage).

General:

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

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 (SD) 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. In IEC 61508, Edition 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 extensions to identify online diagnostic 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 from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The time to restoration 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-HDBK-217F. Alternatively, the assumed environment is similar to:
    - IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- All modules are operated in the low demand mode of operation.
- At the D1010, D1014, D1020, D1021, and D1034 boards only the current output is used for safety applications.
- For the D1032 and D1033 boards the de-energized state is assumed to be the safe state.
- For the D1020 and D1021 boards the default fail-safe state is "fail low".
- External power supply failure rates are not included.
- Only one input and one output are part of the safety function.
- The 4..20 mA output signal is fed to a SIL 3 compliant analog input board of a safety PLC.
- The application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

5 Results of the assessment

exida reviewed the FMEDAs done by G.M. International s.r.l.

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:

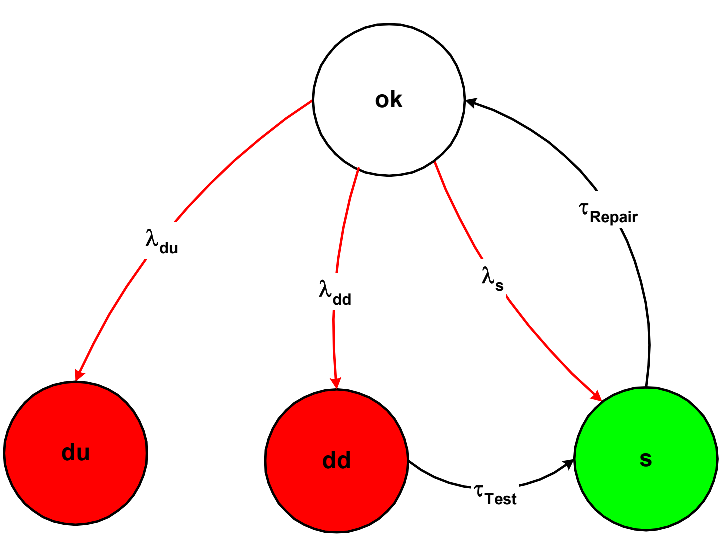
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect}$

$SFF = 1 – \lambda_{DU} / \lambda_{total}$

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 FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.



Abbreviations:

du	The system has failed dangerous undetected
dd	The system has failed dangerous detected
s	The system has failed safe
λ_{du}	Failure rate of dangerous undetected failures
λ_{dd}	Failure rate of dangerous detected failures
λ_s	Failure rate of safe failures
T_{Test}	Test time
τ_{Test}	Test rate (1 / T_{Test})
T_{Repair}	Repair time
τ_{Repair}	Repair rate (1 / T_{Repair})

Figure 9: Markov model for a 1oo1D structure

5.1 D1010 – active input

The FMEDA carried out on the Repeater Power Supply D1010 with active input leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 9,00E-10 1/h

λ_{du} = 3,60E-08 1/h

λ_{high} = 3,36E-08 1/h

λ_{low} = 9,07E-08 1/h

$\lambda_{no\ effect}$ = 2,01E-07 1/h

λ_{total} = 3,62E-07 1/h

$\lambda_{not\ part}$ = 6,90E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 265 years

These failure rates can be converted into the following typical failure rates:

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**126**
Fail dangerous detected (internal diagnostics or indirectly[19])	1
Fail high (detected by the logic solver)	34
Fail low (detected by the logic solver)	91
Fail Dangerous Undetected	**36**
No Effect	**201**
Not part	**69**
MTBF = MTTF + MTTR	**265 years**

Under the assumptions described in section 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [20]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
0 FIT	201 FIT	126 FIT	36 FIT	90,05%	0%	77%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,58E-04	PFD_{AVG} = 7,88E-04	PFD_{AVG} = 1,58E-03

[19] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[20] Note that the SU category includes failures that do not cause a spurious trip

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

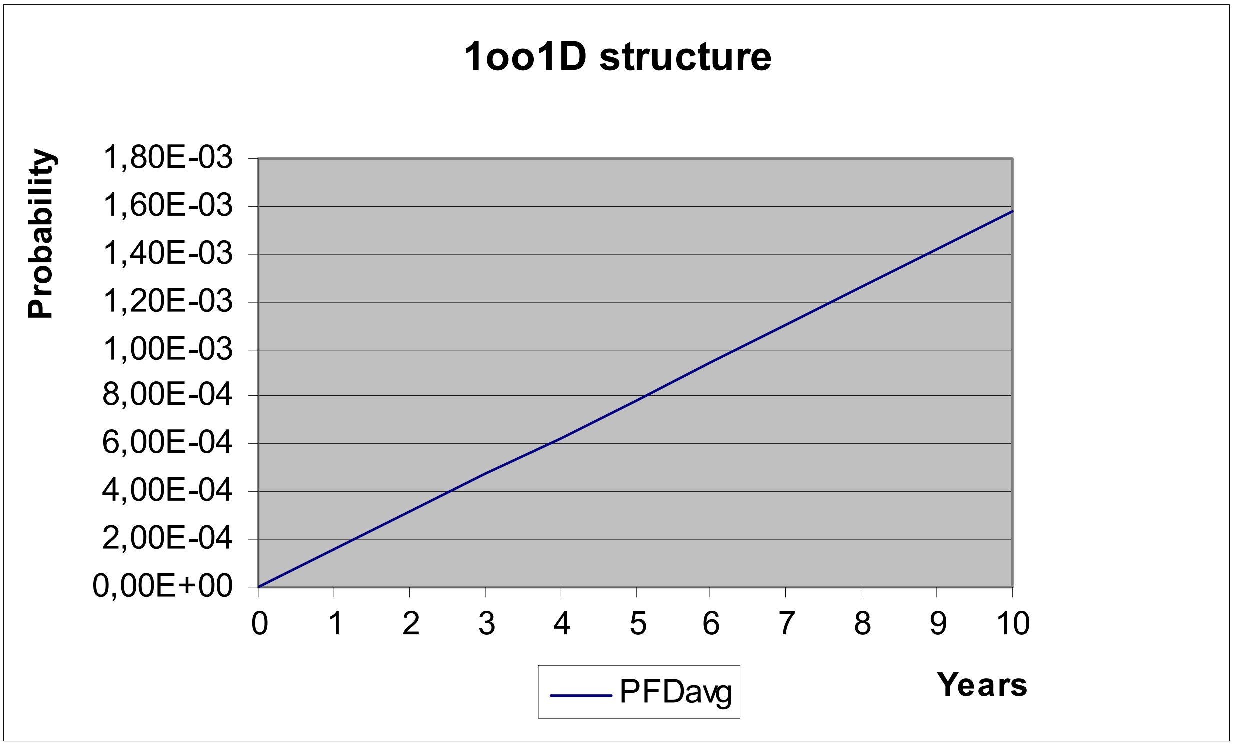


Figure 10: PFD$_{AVG}$(t)

5.2 D1010 – passive input

The FMEDA carried out on the Repeater Power Supply D1010 with passive input leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 9,00E-10 1/h

λ_{du} = 4,08E-08 1/h

λ_{high} = 3,41E-08 1/h

λ_{low} = 1,07E-07 1/h

$\lambda_{no\ effect}$ = 2,36E-07 1/h

λ_{total} = 4,18E-07 1/h

$\lambda_{not\ part}$ = 1,26E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 265 years

These failure rates can be converted into the following typical failure rates:

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**142**
Fail dangerous detected (internal diagnostics or indirectly[21])	1
Fail high (detected by the logic solver)	34
Fail low (detected by the logic solver)	107
Fail Dangerous Undetected	**41**
No Effect	**236**
Not part	**13**
MTBF = MTTF + MTTR	**265 years**

Under the assumptions described in section 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [22]	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
0 FIT	236 FIT	142 FIT	41 FIT	90,25%	0%	77%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,79E-04	PFD_{AVG} = 8,92E-04	PFD_{AVG} = 1,78E-03

[21] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[22] Note that the SU category includes failures that do not cause a spurious trip

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

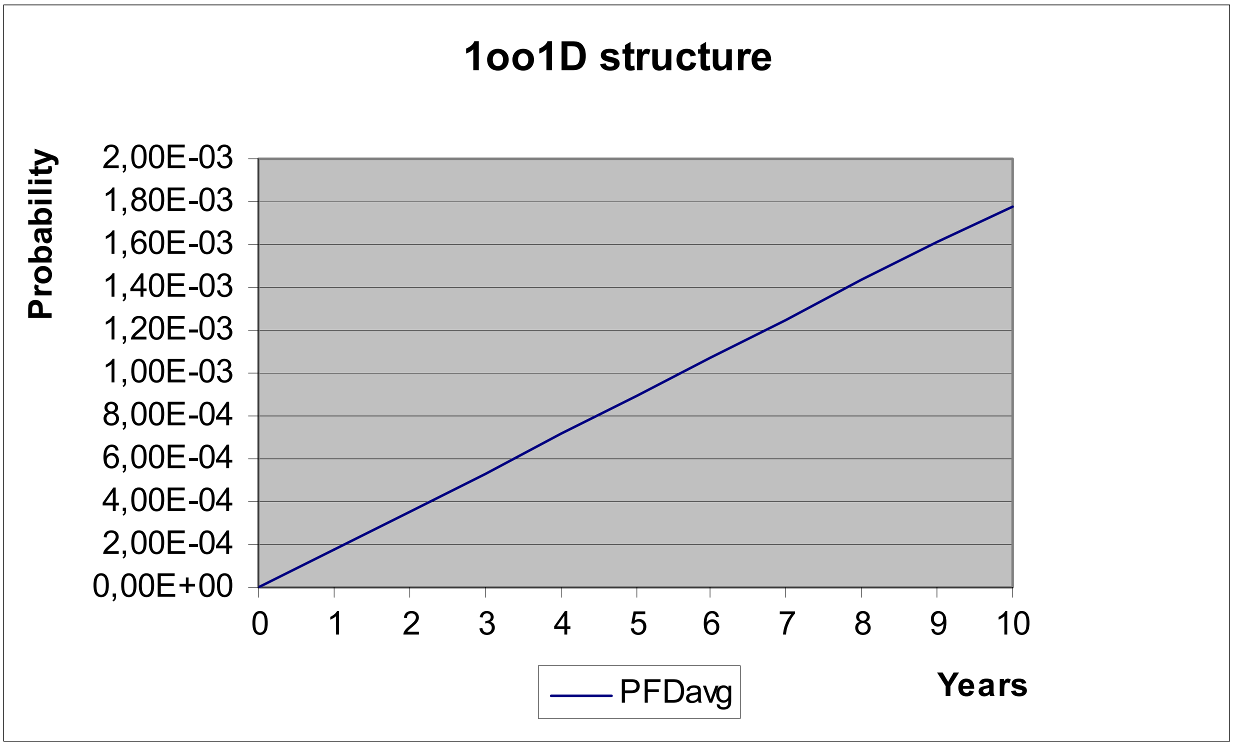


Figure 11: PFD_{AVG}(t)

5.3 D1010S-054, -056, -057

The FMEDA carried out on the Repeater Power Supply D1010S-054, -056, -057 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 9,00E-10 1/h

λ_{du} = 3,79E-08 1/h

λ_{high} = 3,58E-08 1/h

λ_{low} = 8,19E-08 1/h

$\lambda_{no\ effect}$ = 2,00E-07 1/h

λ_{total} = 3,56E-07 1/h

$\lambda_{not\ part}$ = 6,20E-09 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 315 years

These failure rates can be converted into the following typical failure rates:

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**119**
Fail dangerous detected (internal diagnostics or indirectly[23])	1
Fail high (detected by the logic solver)	36
Fail low (detected by the logic solver)	82
Fail Dangerous Undetected	**38**
No Effect	**200**
Not part	**6**
MTBF = MTTF + MTTR	**315 years**

Under the assumptions described in section 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [24]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
0 FIT	200 FIT	119 FIT	38 FIT	89,35%	0%	75%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,66E-04	PFD_{AVG} = 8,30E-04	PFD_{AVG} = 1,66E-03

[23] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[24] Note that the SU category includes failures that do not cause a spurious trip

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

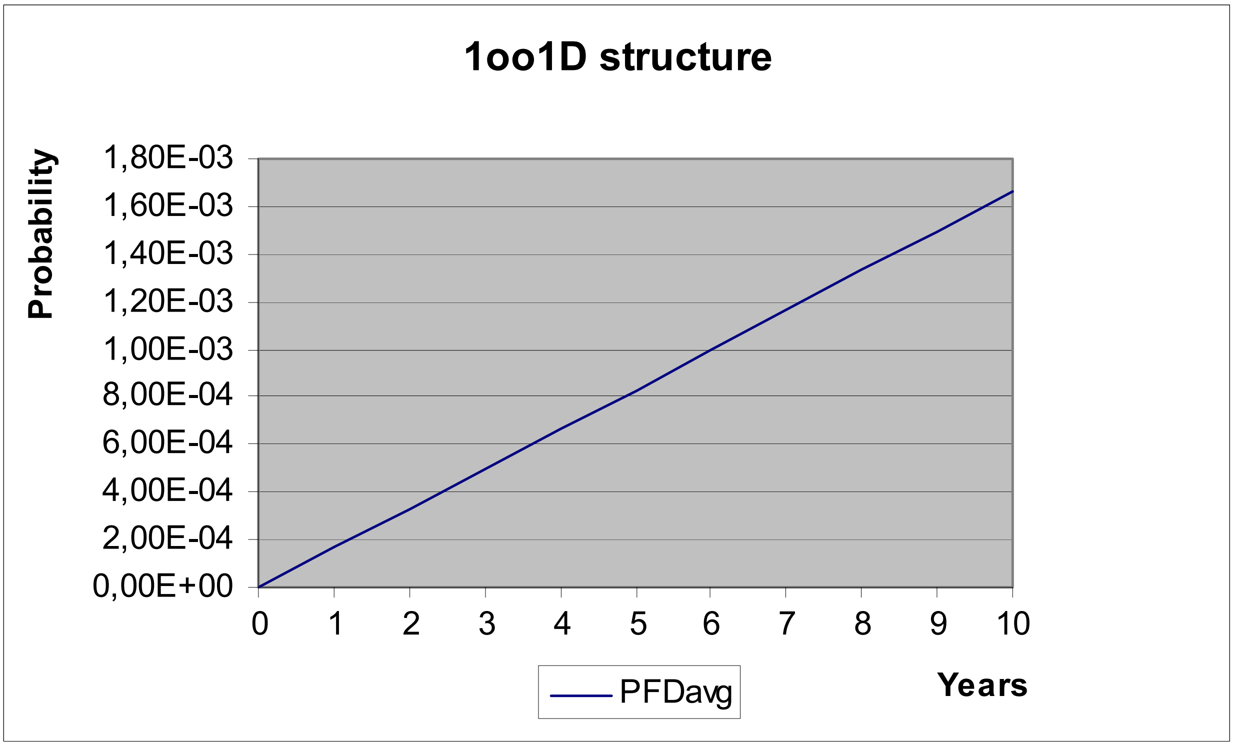


Figure 12: PFD_{AVG}(t)

5.4 D1014

The FMEDA carried out on the Repeater Power Supply D1014 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 2,15E-08 1/h

λ_{high} = 4,16E-08 1/h

λ_{low} = 1,05E-07 1/h

$\lambda_{no\ effect}$ = 1,82E-07 1/h

λ_{total} = 3,51E-07 1/h

$\lambda_{not\ part}$ = 1,50E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 312 years

These failure rates can be converted into the following typical failure rates:

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**147**
Fail dangerous detected (internal diagnostics or indirectly[25])	0
Fail high (detected by the logic solver)	42
Fail low (detected by the logic solver)	105
Fail Dangerous Undetected	**22**
No Effect	**182**
Not part	**15**
MTBF = MTTF + MTTR	**312 years**

Under the assumptions described in section 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [26]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
0 FIT	182 FIT	147 FIT	22 FIT	93,86%	0%	87%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,43E-05	PFD_{AVG} = 4,71E-04	PFD_{AVG} = 9,42E-04

[25] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[26] Note that the SU category includes failures that do not cause a spurious trip

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04. 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 do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04. Figure 13 shows the time dependent curve of PFD_{AVG}.

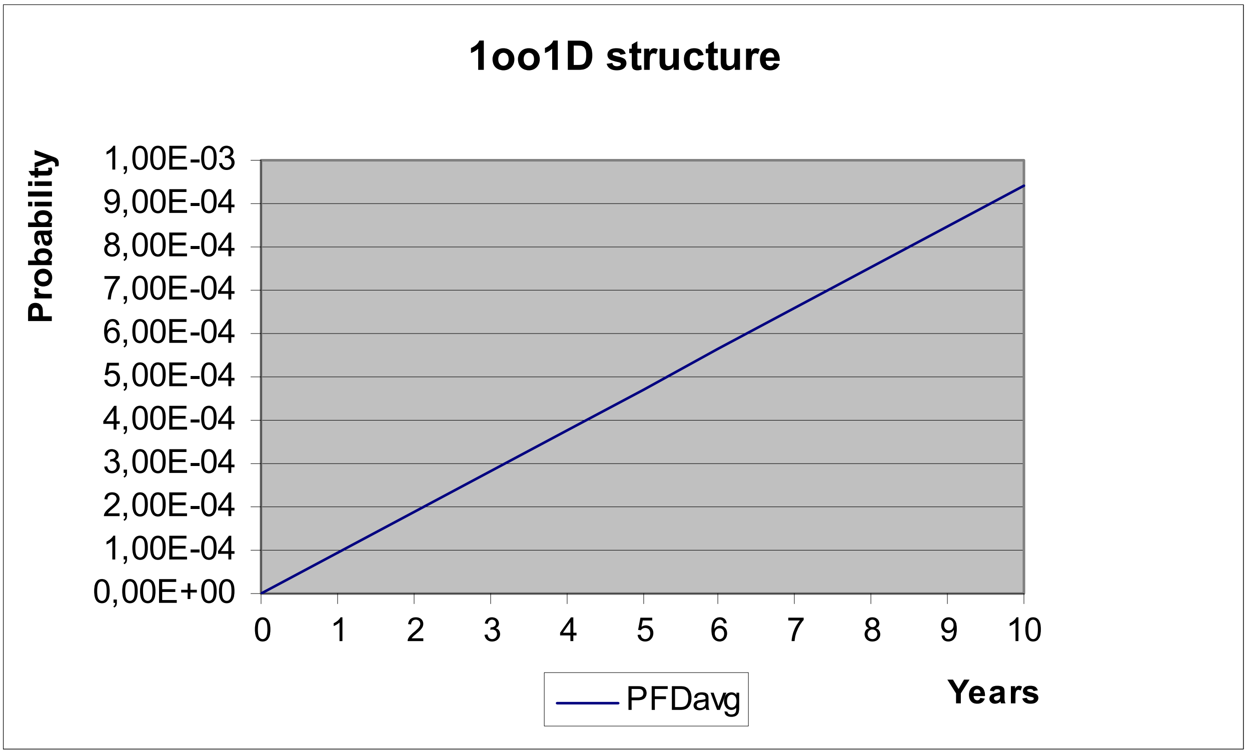


Figure 13: PFD_{AVG}(t)

5.5 D1020

The FMEDA carried out on the Powered Isolating Driver D1020 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

$\lambda_{su} = \lambda_{low} + \lambda_{no\ effect}$ = 7,82E-08 1/h + 2,14E-07 1/h = 2,92E-07 1/h

λ_{dd} = 0,00E-00 1/h

$\lambda_{du} = \lambda_{du} + \lambda_{high}$ = 5,42E-08 1/h + 3,21E-08 1/h = 8,63E-08 1/h

λ_{total} = 3,79E-07 1/h

$\lambda_{not\ part}$ = 1,50E-08 1/h

MTBF = MTTF + MTTR = 1 / ($\lambda_{total} + \lambda_{not\ part}$) + 8 h = 290 years

Under the assumptions described in section 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	292 FIT	0 FIT	86 FIT	77,21%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 3,78E-04	PFD_{AVG} = 1,89E-03	PFD_{AVG} = 3,77E-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 14 shows the time dependent curve of PFD_{AVG}.

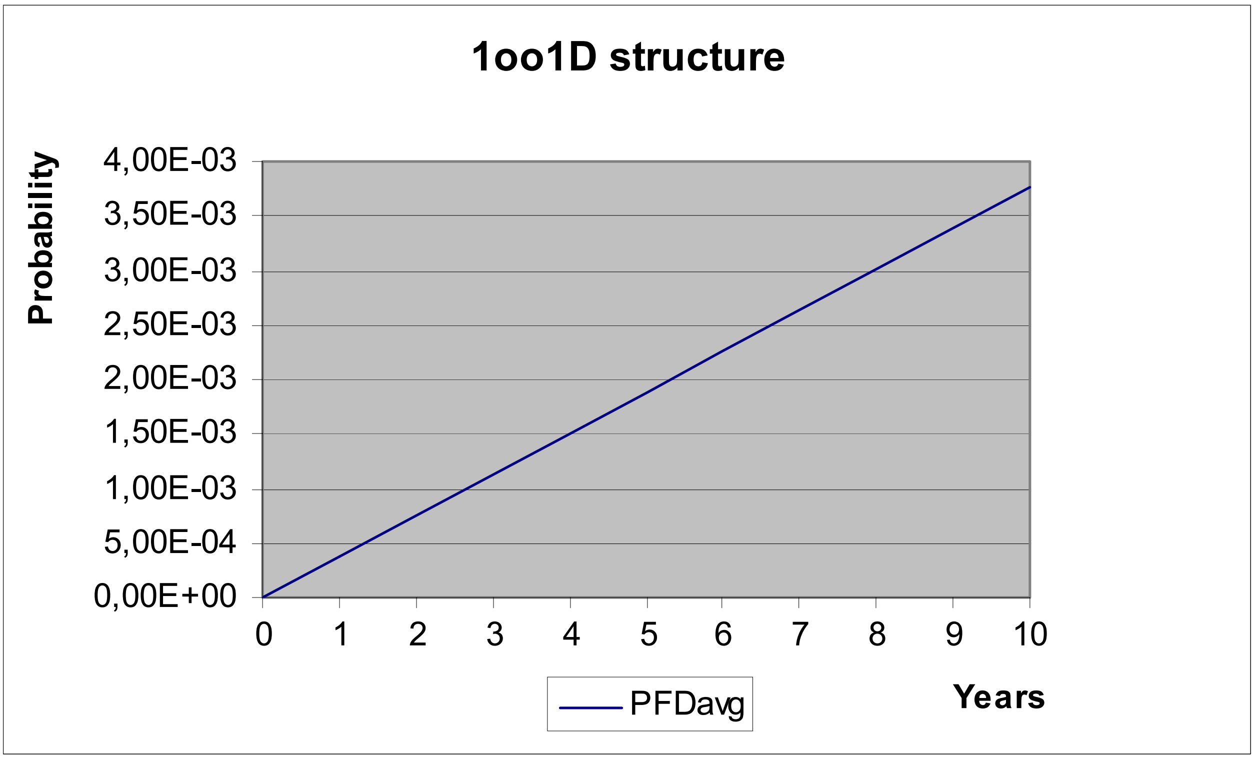


Figure 14: PFD$_{AVG}$(t)

5.6 D1021

The FMEDA carried out on the Powered Isolating Driver with fault detection D1021 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

$\lambda_{su} = \lambda_{low} + \lambda_{no\ effect}$ = 1,09E-07 1/h + 1,76E-07 1/h = 2,85E-07 1/h

λ_{dd} = 0,00E-00 1/h

$\lambda_{du} = \lambda_{du} + \lambda_{high}$ = 8,53E-08 1/h + 3,30E-08 1/h = 1,18E-07 1/h

λ_{total} = 4,03E-07 1/h

$\lambda_{not\ part}$ = 1,26E-07 1/h

MTBF = MTTF + MTTR = 1 / ($\lambda_{total} + \lambda_{not\ part}$) + 8 h = 216 years

Under the assumptions described in section 5 the following table shows the failure rates according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0 FIT	285 FIT	0 FIT	118 FIT	70,66%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 5,18E-04	PFD_{AVG} = 2,59E-03	PFD_{AVG} = 5,16E-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 15 shows the time dependent curve of PFD_{AVG}.

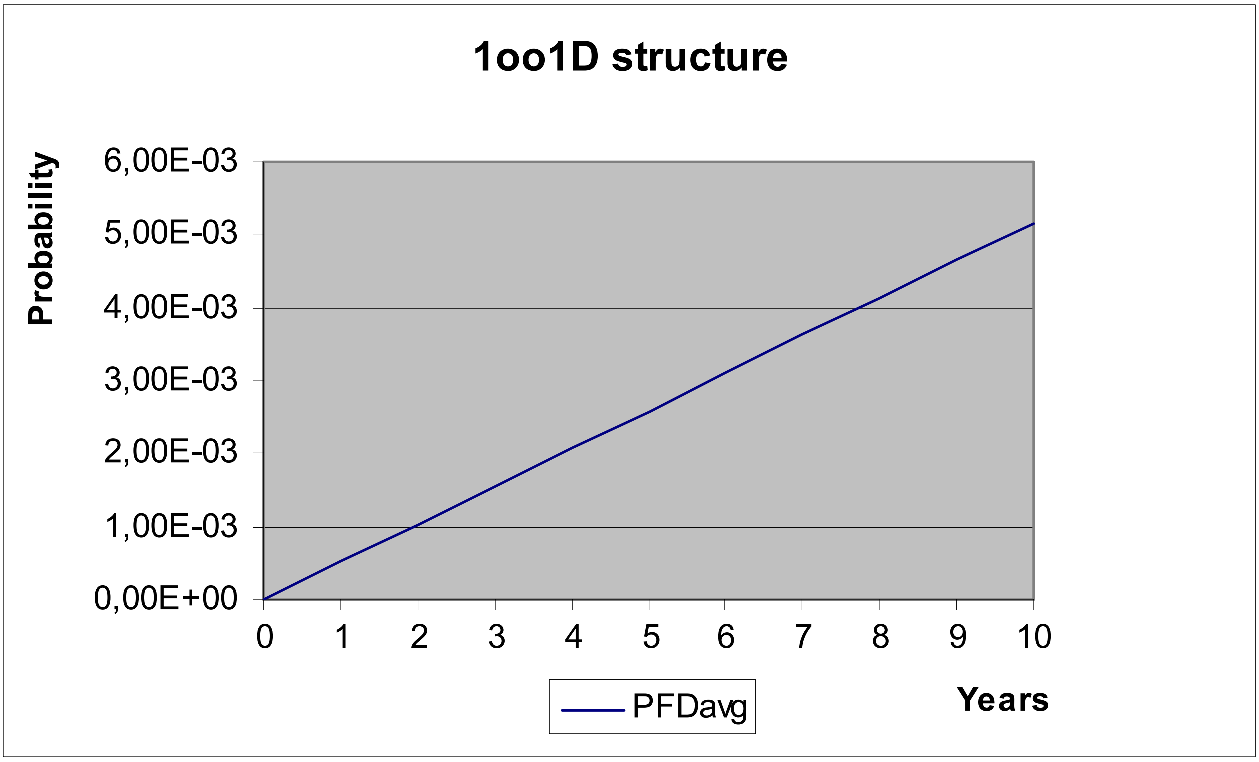


Figure 15: $PFD_{AVG}(t)$

5.7 D1032

The FMEDA carried out on the Switch/Proximity Detector Repeater D1032 with relay output leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,02E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 2,75E-08 1/h

$\lambda_{no\ effect}$ = 1,08E-07 1/h

λ_{total} = 2,37E-07 1/h

$\lambda_{not\ part}$ = 2,81E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 430 years

Under the assumptions described in section 5 the following table shows the failure rates according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	**SFF**
0 FIT	210 FIT	0 FIT	28 FIT	88,41%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,20E-04	PFD_{AVG} = 6,02E-04	PFD_{AVG} = 1,20E-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 16 shows the time dependent curve of PFD_{AVG}.

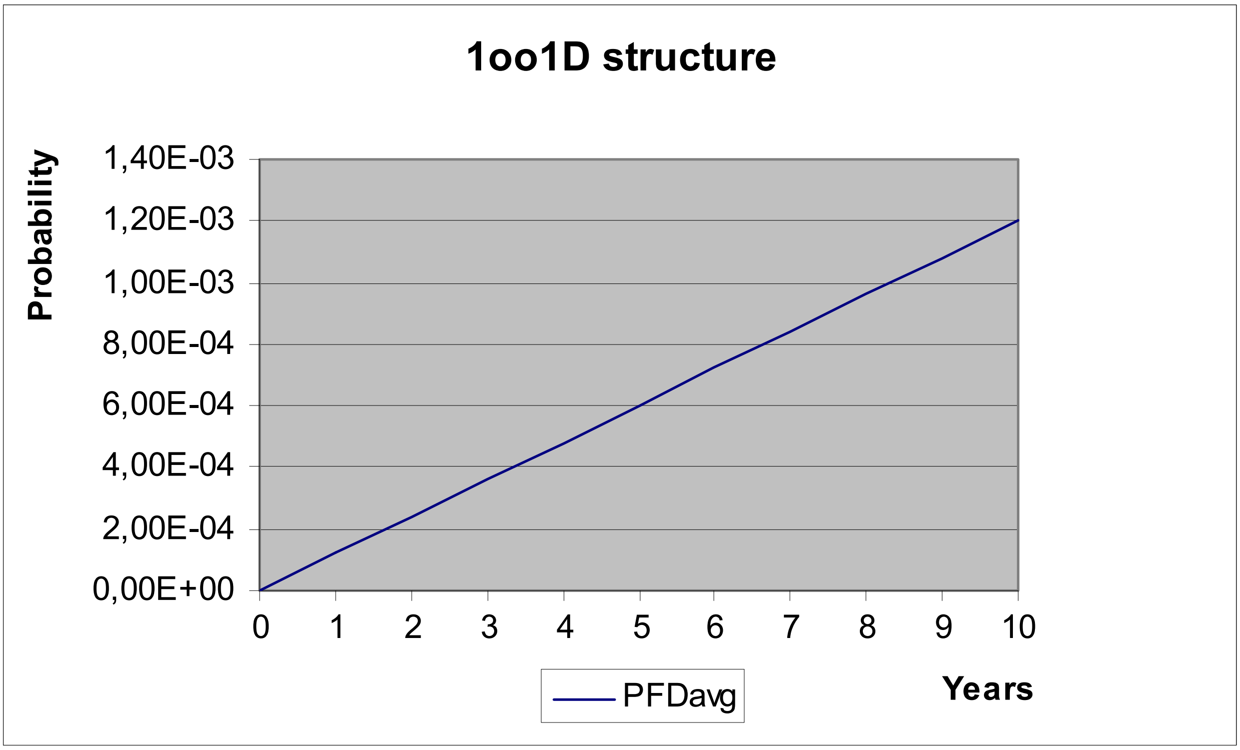


Figure 16: PFD$_{AVG}$(t)

5.8 D1033

The FMEDA carried out on the Switch/Proximity Detector Repeater D1033 with transistor output leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,06E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 3,53E-08 1/h

$\lambda_{no\ effect}$ = 1,06E-07 1/h

λ_{total} = 2,47E-07 1/h

$\lambda_{not\ part}$ = 2,79E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 415 years

Under the assumptions described in section 5 the following table shows the failure rates according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	**SFF**
0 FIT	212 FIT	0 FIT	35 FIT	85,72%

The PFD$_{AVG}$ was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD$_{AVG}$ = 1,55E-04	PFD$_{AVG}$ = 7,72E-04	PFD$_{AVG}$ = 1,54E-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 17 shows the time dependent curve of PFD$_{AVG}$.

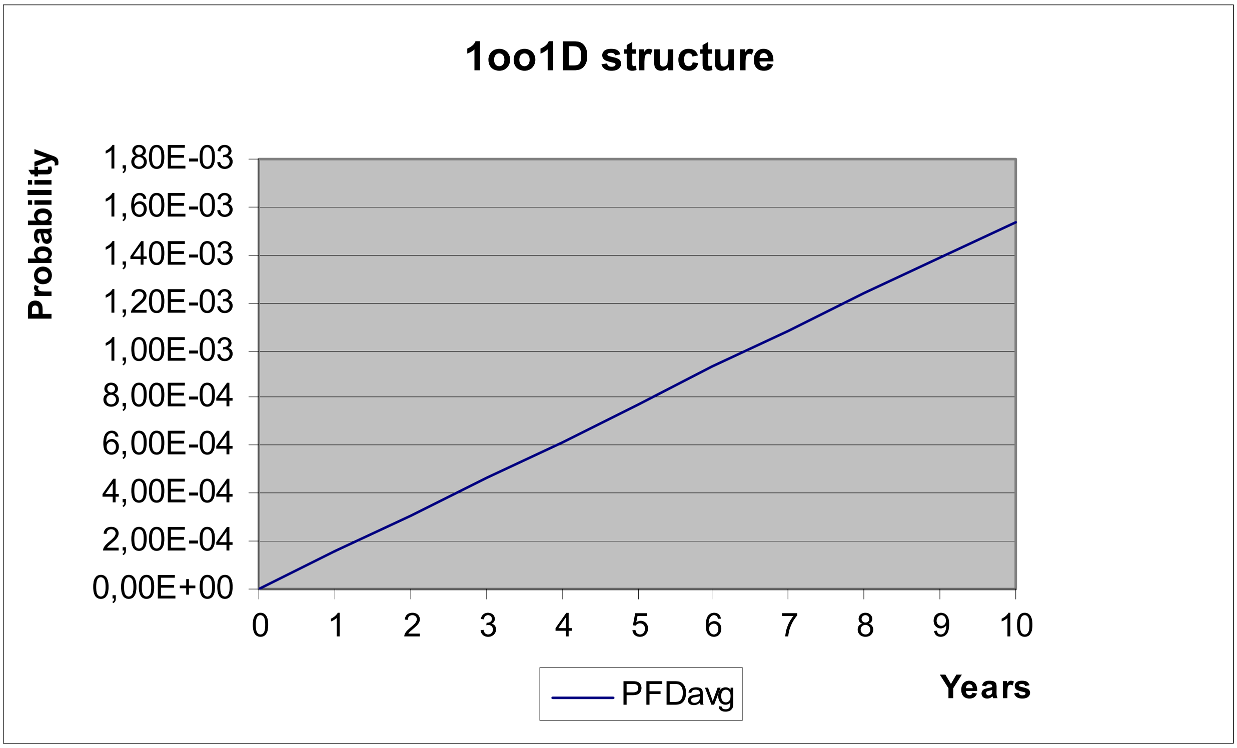


Figure 17: PFD$_{AVG}$(t)

5.9 D1034

The FMEDA carried out on the Contact/Proximity Detector Interface D1034 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 1,99E-08 1/h

λ_{high} = 3,76E-08 1/h

λ_{low} = 6,40E-08 1/h

$\lambda_{no\ effect}$ = 1,85E-07 1/h

λ_{total} = 3,07E-07 1/h

$\lambda_{not\ part}$ = 6,20E-09 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 365 years

These failure rates can be converted into the following typical failure rates:

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**102**
Fail dangerous detected (internal diagnostics or indirectly[27])	0
Fail high (detected by the logic solver)	38
Fail low (detected by the logic solver)	64
Fail Dangerous Undetected	**20**
No Effect	**185**
Not part	**6**
MTBF = MTTF + MTTR	**365 years**

Under the assumptions described in section 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [28]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
0 FIT	185 FIT	102 FIT	20 FIT	93,53%	0%	83%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 9.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,70E-05	PFD_{AVG} = 4,35E-04	PFD_{AVG} = 8,69E-04

[27] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[28] Note that the SU category includes failures that do not cause a spurious trip

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04. 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 do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04. Figure 18 shows the time dependent curve of PFD_{AVG}.

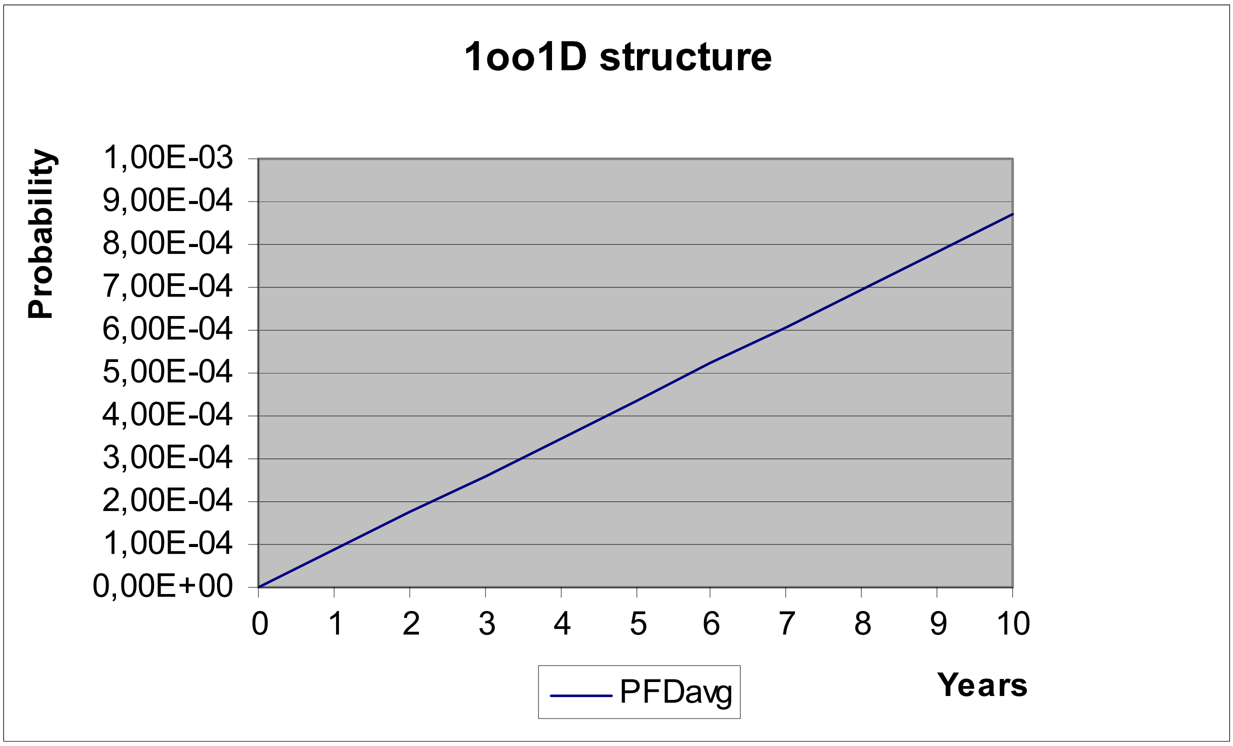


Figure 18: $PFD_{AVG}(t)$

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
HART	Highway Addressable Remote Transducer
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
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.
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.

7.2 Releases

Version:	V2	
Revision:	R1	
Version History:	V0, R1.0:	Initial version; March 23, 2004
	V1, R1.0:	Review comments integrated; April 20, 2004
	V2, R0:	Updates after modifications on several modules; November 3, 2006
	V2, R1:	Color marking for PFD_{AVG} values corrected; November 7, 2006
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Glisente Landrini (G.M); April 6, 2004
		Rachel Amkreutz (exida.com); April 13, 2004
	V2, R0:	Glisente Landrini (G.M); November 6, 2006
Release status:	Released to G.M. International s.r.l	

7.3 Release Signatures

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

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

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

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

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

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

Table 25 to Table 33 show an importance analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Table 25: Importance Analysis of "du" failures – D1010 – active input

Component	% of total λ_{du}	Detection through
IC10 - ICLS002	6,67%	100% functional test with different expected output signals over the entire range
IC3A - ICLS006	5,00%	100% functional test with different expected output signals over the entire range
IC4A - ICRS003	5,00%	100% functional test with different expected output signals over the entire range
IC6A - ICRS003	5,00%	100% functional test with different expected output signals over the entire range
IC12A - ICLS002	5,00%	100% functional test with different expected output signals over the entire range
C28A - CMCS005	4,44%	100% functional test with different expected output signals over the entire range
C38 - CMCS005	4,44%	100% functional test with different expected output signals over the entire range
IC2A - ICLS005	4,17%	100% functional test with different expected output signals over the entire range
IC5A - ICLS006	4,17%	100% functional test with different expected output signals over the entire range
IC7A - ICLS005	4,17%	100% functional test with different expected output signals over the entire range

Table 26: Importance Analysis of “du” failures – D1010 – passive input

Component	% of total λ_{du}	Detection through
IC10 - ICLS002	5,89%	100% functional test with different expected output signals over the entire range
IC3A - ICLS006	4,42%	100% functional test with different expected output signals over the entire range
IC4A - ICRS003	4,42%	100% functional test with different expected output signals over the entire range
IC6A - ICRS003	4,42%	100% functional test with different expected output signals over the entire range
IC12A - ICLS002	4,42%	100% functional test with different expected output signals over the entire range
C11A - CMCS005	3,93%	100% functional test with different expected output signals over the entire range
C28A - CMCS005	3,93%	100% functional test with different expected output signals over the entire range
C38 - CMCS005	3,93%	100% functional test with different expected output signals over the entire range
IC2A - ICLS005	3,68%	100% functional test with different expected output signals over the entire range
IC5A - ICLS006	3,68%	100% functional test with different expected output signals over the entire range

Table 27: Importance Analysis of “du” failures – D1010S-054, -056, -057

Component	% of total λ_{du}	Detection through
IC10 - ICLS002	6,33%	100% functional test with different expected output signals over the entire range
IC1A - ICAS010	4,74%	100% functional test with different expected output signals over the entire range
IC3A - ICLS006	4,74%	100% functional test with different expected output signals over the entire range
IC4A - ICRS003	4,74%	100% functional test with different expected output signals over the entire range
IC6A - ICRS003	4,74%	100% functional test with different expected output signals over the entire range
IC12A - ICLS002	4,74%	100% functional test with different expected output signals over the entire range
C38 - CMCS005	4,22%	100% functional test with different expected output signals over the entire range
IC2A - ICLS005	3,95%	100% functional test with different expected output signals over the entire range
IC5A - ICLS006	3,95%	100% functional test with different expected output signals over the entire range
IC7A - ICLS005	3,95%	100% functional test with different expected output signals over the entire range

Table 28: Importance Analysis of "du" failures – D1014

Component	% of total λ_{du}	Detection through
TR6A	16,26%	100% functional test with different expected output signals over the entire range
IC1A	8,36%	100% functional test with different expected output signals over the entire range
TR7A	7,66%	100% functional test with different expected output signals over the entire range
D4A	7,43%	100% functional test with different expected output signals over the entire range
TR9A	6,97%	100% functional test with different expected output signals over the entire range
IC2A	6,50%	100% functional test with different expected output signals over the entire range
IC6A	5,57%	100% functional test with different expected output signals over the entire range
C2A	4,64%	100% functional test with different expected output signals over the entire range
C33A	4,64%	100% functional test with different expected output signals over the entire range
IC5A	4,64%	100% functional test with different expected output signals over the entire range

Table 29: Importance Analysis of "du" failures – D1020

Component	% of total λ_{du}	Detection through
IC11 - ICVS001	7,38%	100% functional test with different expected output signals over the entire range
IC4A - ICLS006	5,54%	100% functional test with different expected output signals over the entire range
IC5A - ICLS006	5,54%	100% functional test with different expected output signals over the entire range
IC8A - ICLS005	5,54%	100% functional test with different expected output signals over the entire range
IC12A - ICLS002	5,54%	100% functional test with different expected output signals over the entire range
T1A - TFRT039	4,61%	100% functional test with different expected output signals over the entire range
IC3A - ICRS003	4,43%	100% functional test with different expected output signals over the entire range
IC7A - ICRS003	4,43%	100% functional test with different expected output signals over the entire range
IC10 - ICLS002	4,43%	100% functional test with different expected output signals over the entire range
TR11 - TRPS001	4,15%	100% functional test with different expected output signals over the entire range

Table 30: Importance Analysis of “du” failures – D1021

Component	% of total λ_{du}	Detection through
P1	35,15%	100% functional test with different expected output signals over the entire range
P2	35,15%	100% functional test with different expected output signals over the entire range
IC10	4,10%	100% functional test with different expected output signals over the entire range
TR9	1,93%	100% functional test with different expected output signals over the entire range
TR1	1,76%	100% functional test with different expected output signals over the entire range
TR10	1,76%	100% functional test with different expected output signals over the entire range
IC3	1,64%	100% functional test with different expected output signals over the entire range
IC4	1,41%	100% functional test with different expected output signals over the entire range
IC5	1,41%	100% functional test with different expected output signals over the entire range
IC8	1,41%	100% functional test with different expected output signals over the entire range

Table 31: Importance Analysis of “du” failures – D1032

Component	% of total λ_{du}	Detection through
RL1A	23,64%	100% functional test
TR6A	12,73%	100% functional test
IC1A	11,64%	100% functional test
IC3	6,55%	100% functional test
IC5	6,55%	100% functional test
SW1	5,82%	100% functional test
D9A	5,82%	100% functional test
TR5A	5,46%	100% functional test
IC4	4,37%	100% functional test
IC6	3,64%	100% functional test

Table 32: Importance Analysis of “du” failures – D1033

Component	% of total λ_{du}	Detection through
D11A	19,84%	100% functional test
OT1A	12,75%	100% functional test
TR6A	9,92%	100% functional test
IC1A	9,07%	100% functional test
IC3	5,10%	100% functional test
IC5	5,10%	100% functional test
TR7A	4,68%	100% functional test
SW1	4,53%	100% functional test
D9A	4,53%	100% functional test
TR5A	4,25%	100% functional test

Table 33: Importance Analysis of “du” failures – D1034

Component	% of total λ_{du}	Detection through
IC5A	15,11%	100% functional test with different expected output signals over the entire range
TR3A	12,59%	100% functional test with different expected output signals over the entire range
TR5A	12,59%	100% functional test with different expected output signals over the entire range
IC1A	6,05%	100% functional test with different expected output signals over the entire range
IC6A	6,05%	100% functional test with different expected output signals over the entire range
C24A	5,04%	100% functional test with different expected output signals over the entire range
C5A	3,02%	100% functional test with different expected output signals over the entire range
C6A	3,02%	100% functional test with different expected output signals over the entire range
C32A	2,52%	100% functional test with different expected output signals over the entire range
D4A	2,52%	100% functional test with different expected output signals over the entire range

Appendix 1.1: Possible proof tests to detect dangerous undetected faults in the D1010, D1014, D1032, D1033 and D1034 boards

Proof test 1 consists of the following steps, as described in Table 34.

Table 34 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the repeater to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3	Send a HART command to the repeater to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 50% of possible “du” failures in the repeater.

Proof test 2 consists of the following steps, as described in Table 35.

Table 35 Steps for Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Perform a two-point calibration of the connected transmitter This requires that the transmitter has already been tested without the repeater and does not contain any dangerous undetected faults anymore.
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures in the repeater.

Appendix 1.2: Possible proof tests to detect dangerous undetected faults in the D1020 and D1021 boards

Proof test 1 consists of the following steps, as described in Table 34.

Table 36 Steps for Proof Test 1

Step	Action
1	Take appropriate action to avoid a false trip
2	Provide a 4mA control signal to the driver to open/close the valve and verify that the valve is open/closed. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures. It requires, however, that the positioner has already been tested without the driver and does not contain any dangerous undetected faults anymore.
3	Provide a 20mA control signal to the driver to close/open the valve and verify that the valve is closed/open. This tests for possible quiescent current related failures. It requires, however, that the positioner has already been tested without the driver and does not contain any dangerous undetected faults anymore.
4	Restore the loop to full operation
5	Restore normal operation

This test will detect approximately 70% of possible “du” failures in the driver.

Proof test 2 consists of the following steps, as described in Table 35.

Table 37 Steps for Proof Test 2

Step	Action
1	Take appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Perform a two-point calibration of the positioner It requires, however, that the positioner has already been tested without the driver and does not contain any dangerous undetected faults anymore.
4	Restore the loop to full operation
5	Restore normal operation

This test will detect approximately 95% of possible “du” failures in the driver.

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[29] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore 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, electrolytic 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.

Table 38 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 38: Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Name	Board	Useful life at 40°C
Capacitor (electrolytic) - Aluminum electrolytic, solid electrolyte	C22A	D1020	Appr. 90 000 Hours[30]
	C30	D1021	

As the capacitors are the limiting factors with regard to the useful lifetime of the system, the useful lifetime for the D1020 and D1021 boards should be limited to 10 years.

The circuits of the other assessed boards 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.

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

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

[30] The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.