

Functional Safety Manual

for Safety Related Systems and SIL 2, SIL 3 Applications

according IEC 61508 & IEC 61511 Standards

G.M. International **D1000 Series** Intrinsically Safe Interface Modules and Switching Power Supply PSD1206, PSD1210

Table of Contents

1	General	4
2	Functional Safety Specifications from EXIDA and TÜV analysis, report according IEC 61508 - IEC 61511	6
3	Definitions	10
	3.1 Failure categories.....	10
	3.1.1 Failure categories for PSD1206 and PSD1210	12
	3.2 General Terms	13
4	Assumptions.....	14
	4.1 Assumption for PSD1206 and PSD1210	15
5	Summary of Data from EXIDA and TÜV analysis.....	16
	5.1 D1010S Isolating Repeater Power Supply, Hart Compatible (Active Input).....	16
	5.2 D1010S Isolating Repeater Power Supply, Hart Compatible (Passive Input)	17
	5.3 D1010D Isolating Repeater Power Supply, Hart Compatible (Active Input).....	18
	5.4 D1010D Isolating Repeater Power Supply, Hart Compatible (Passive Input).....	19
	5.5 D1010S-054 Isolating -5 ÷ +55 mV to 4 ÷ 20 mA Converter	20
	5.6 D1010S-056 Isolating -5 ÷ +35 mV to 4 ÷ 20 mA Converter	21
	5.7 D1010S-057 Isolating -5 ÷ +10 mV to 4 ÷ 20 mA Converter	22
	5.8 D1014S and D1014D Isolating Repeater Power Supplies, Hart Compatible	23
	5.9 D1020S and D1020D Powered Isolating Drivers for I/P, Hart Compatible.....	24
	5.10 D1021S Powered Isolating Driver for I/P, with Fault Detection and Hart Compatible	25
	5.11 D1032D Isolating Switch-Proximity Detector Repeater, Relay Output.....	26
	5.12 D1032Q Isolating Switch-Proximity Detector Repeater, Relay Output.....	27
	5.13 D1033D Isolating Switch-Proximity Detector Repeater, Transistor output.....	28
	5.14 D1033Q Isolating Switch-Proximity Detector Repeater, Transistor output.....	29
	5.15 D1034S and D1034D Isolating Switch-Proximity Detector Interfaces, mA output	30
	5.16 D1040Q, D1042Q, D1043Q, PSD1001(C) Bus Powered Isolating Drivers for NE loads.....	31
	5.17 D1040Q, D1042Q, D1043Q, PSD1001(C) Loop Powered Isolating Drivers for NE loads.....	31
	5.18 D1044S Bus Powered Digital Relay Output for NE or ND loads	32
	5.19 D1044S Loop Powered Digital Relay Output for NE or ND loads	33
	5.20 D1044D Bus Powered (independent channels) Digital Relay Output for NE or ND loads.....	34
	5.21 D1044D Bus Powered (1oo2 channel architecture) Digital Relay Output for NE or ND loads.....	35
	5.22 D1044D Loop Powered (1oo2 channel architecture) Digital Relay Output for NE or ND loads.....	36
	5.23 D1048S Loop Powered Digital Output Driver for NE loads	37

5.24	D1049S Bus Powered Digital Output Driver for NE loads	38
5.25	D1053S Isolating Analog Signals Converter and Trip Amplifiers (using analog output)	39
5.26	D1053S Isolating Analog Signals Converter and Trip Amplifiers (using 2 relay outputs in series)	40
5.27	D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using active input and analog output).....	41
5.28	D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using passive input and analog output).....	42
5.29	D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using active input and 2 relay outputs in series)	43
5.30	D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using passive input and 2 relay outputs in series)	44
5.31	D1072S Isolating Temperature Signal Converter, D1073S Isolating Temperature Signal Converter and Trip Amplifiers (using analog output).....	45
5.32	D1072D Isolating Temperature Signal Converter (using analog output).....	46
5.33	D1073S Isolating Temperature Converter and Trip Amplifiers (using 2 relay outputs in series).....	47
5.34	D1092S and D1092D Relay Output Modules for NE loads	48
5.35	D1092S and D1092D Relay Output Modules for ND loads	49
5.36	D1092S-069 and D1092D-069 Relay Output Modules, NO contact output	50
5.37	D1092S-069 and D1092D-069 Relay Output Modules, NC contact output.....	51
5.38	D1093S Relay Output Module for NE loads, with Line and Load diagnostics.....	52
5.39	D1093S Relay Output Module for ND loads, with Line and Load diagnostics.....	53
5.40	PSD1206 and PSD1210 Isolated Switching Power Supplies for NE loads, single unit.....	54
5.41	PSD1206 and PSD1210 Isolated Switching Power Supplies for ND loads, single unit	55
5.42	PSD1206 and PSD1210 Isolated Switching Power Supplies, 2 units in parallel.....	56
5.42.1	NE loads.....	56
5.42.2	ND loads	57
5.43	PSD1206 and PSD1210 Isolated Switching Power Supplies, 3 units in parallel.....	57
5.43.1	NE loads.....	57
5.43.2	ND loads	57
5.44	PSD1206 and PSD1210 Isolated Switching Power Supplies, fail with over voltage condition.....	58
6	Notes.....	59
7	Possible Proof Tests to reveal Dangerous Undetected Failures	60
7.1	D1010, D1014	60
7.2	D1010S-054, D1010S-056, D1010S-057	60
7.3	D1020, D1021S.....	61
7.4	D1032, D1033	61
7.5	D1034	61
7.6	D1040, D1042, D1043, PSD1001, PSD1001C.....	62
7.7	D1044	62
7.8	D1049S.....	62
7.9	D1053S and D1054S (using analog output)	63
7.10	D1053S and D1054S (using 2 relay outputs in series).....	64
7.11	D1072, D1073S (using analog output).....	64
7.12	D1073S (using 2 relay outputs in series)	65
7.13	D1092	66
7.14	D1092-069.....	66
7.15	D1093S.....	66
7.16	PSD1206, PSD1210.....	67
7.16.1	Test Setup.....	67
7.16.2	Test of single Power Supply or individual unit of “N” unit in parallel.....	67

	7.16.3 Tests required when the unit is used as subsystem of “N” units in parallel	68
8	Impact of Lifetime of Critical Components on Failure Rate.....	71
9	Influence of PFDavg calculation on efficiency of Proof Test for a 1oo1 architecture.	71

1 General

This Safety Manual summarizes the results of hardware assessment carried out on the following Intrinsically Safe modules:

Repeater – Driver – Interface D1010, D1010S-054 (or -056 or -057), D1014, D1020, D1021S, D1032, D1033, D1034, D1040, D1042, D1043, D1048S, D1049S; Analog Signals Converter and Trip Amplifiers D1053S; Repeater and Trip Amplifiers D1054S; Temperature Signal Converter D1072; Temperature Signal Converter and Trip Amplifiers D1073S; Relay Output modules D1044, D1092, D1092-069, D1093S; Power Supply PSD1001(C), PSD1206, PSD1210.

Table 1: Model – Output channels – Safety Function Table

Model	Output channels	Component type	Safety Function
D1010S	1	A	Isolating Repeater Power Supply, HART compatible
D1010D	2	A	Isolating Repeater Power Supply, HART compatible
D1010S-054	1	A	Isolating -5 ÷ +55 mV to 4 ÷ 20 mA Converter
D1010S-056	1	A	Isolating -5 ÷ +35 mV to 4 ÷ 20 mA Converter
D1010S-057	1	A	Isolating -5 ÷ +10 mV to 4 ÷ 20 mA Converter
D1014S	1	A	Isolating Repeater Power Supply, HART compatible
D1014D	2	A	Isolating Repeater Power Supply, HART compatible
D1020S	1	A	Powered Isolating Valve Driver, HART compatible
D1020D	2	A	Powered Isolating Valve Driver, HART compatible
D1021S	1	A	Powered Isolating Valve Driver with Fault Detection, HART compatible
D1032D	2	A	Isolating Switch-Proximity Detector Repeater, Relay output
D1032Q	4	A	Isolating Switch-Proximity Detector Repeater, Relay output
D1033D	2	A	Isolating Switch-Proximity Detector Repeater, O.C. Transistor output
D1033Q	4	A	Isolating Switch-Proximity Detector Repeater, O.C. Transistor output
D1034S	1	A	Isolating Switch-Proximity Detector Interface, mA output
D1034D	2	A	Isolating Switch-Proximity Detector Interface, mA output
D1040Q	4	B	Loop / Bus Powered Isolating Driver for NE loads, 22mA at 13.2V (per ch.)
D1042Q	4	B	Loop / Bus Powered Isolating Driver for NE loads, 22mA at 14.5V (per ch.)
D1043Q	4	B	Loop / Bus Powered Isolating Driver for NE loads, 22mA at 9.8V (per ch.)
D1044S	1	A	Loop / Bus Powered Digital Relay Output for NE or ND loads
D1044D	2	A	Loop / Bus Powered Digital Relay Output for NE or ND loads
D1048S	1	A	Loop Powered Digital Output Driver for NE loads
D1049S	1	A	Bus Powered Digital Output Driver for NE loads
D1053S	1	B	Isolating Analog Signals Converter and Trip Amplifiers
D1054S	1	B	Isolating Repeater Power Supply and Trip Amplifiers, HART compatible
D1072S	1	B	Isolating Temperature Signal Converter, Fully Programmable
D1072D	2	B	Isolating Temperature Signal Converter, Fully Programmable
D1073S	1	B	Isolating Temperature Converter and Trip Amplifiers, Fully Programmable
D1092S	1	A	Relay Output Module for NE or ND loads
D1092D	2	A	Relay Output Module for NE or ND loads
D1092S-069	1	A	NE Relay Output Module with NO and NC contact outputs
D1092D-069	2	A	NE Relay Output Module with NO and NC contact outputs
D1093S	1	A	Relay Output Module for NE or ND loads, with Line and Load diagnostics
PSD1001	4	B	Isolating Power Supply 20 mA at 15 V (per channel)
PSD1001C	1	B	Isolating Power Supply 100 mA at 13.5 V
PSD1206	1	A	Isolated Switching Power Supply 6 A at 24 Vdc
PSD1210	1	A	Isolated Switching Power Supply 10 A at 24 Vdc

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

The failure modes distributions used in this analysis are considered according to RAC FMD-91/97.

According to table 2 of IEC 61508-1, the average PFD for systems operating in low demand mode has to be from $\geq 1.00 \text{ E-}03$ to $< 1.00 \text{ E-}02$ 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 $10\% \div 20\%$ of this range. For SIL 2 application the total PFDavg value of the SIF must be smaller than $1.00 \text{ E-}02$, hence the maximum allowable PFDavg value for the asset modules would then be $1.00 \text{ E-}03$ (for 10% contribution) and $2.00 \text{ E-}03$ (for 20% contribution). A similar consideration can be done for SIL 3 application, where limits are ten times smaller than correspondent limits in SIL 2 application.

The listed modules are considered to be Type A (*) or Type B (**) components, with a hardware fault tolerance of 0.

According to table 2 of IEC 61508-2, for Type A components the SFF has to be:

- less than 60% for SIL 1 (sub-) systems with a hardware fault tolerance of 0;
- equal or more than 60% for SIL 2 (sub-) systems with a hardware fault tolerance of 0;
- less than 60% for SIL 2 (sub-) systems with a hardware fault tolerance of 1;
- equal or more than 90% for SIL 3 (sub-) systems with a hardware fault tolerance of 0;
- equal or more than 60% for SIL 3 (sub-) systems with a hardware fault tolerance of 1.

According to table 3 of IEC 61508-2, for Type B components the SFF has to be:

- equal or more than 60% for SIL 1 (sub-) systems with a hardware fault tolerance of 0;
- equal or more than 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0;
- equal or more than 60% for SIL 2 (sub-) systems with a hardware fault tolerance of 1;
- equal or more than 99% for SIL 3 (sub-) systems with a hardware fault tolerance of 0;
- equal or more than 90% for SIL 3 (sub-) systems with a hardware fault tolerance of 1.

If the requirements of section 11.4.4 of IEC 61511-1 First Edition 2003-01 are fulfilled, a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with Type B components and having a SFF equal or more than between 60%.

Assuming that a logic solver (connected to D1000 module outputs) 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 depending on the application.

At section 5, it's showed the summary of functional safety data for each module, according to the following documents:

- TÜV Analysis: Compliance Certificate C - IS - 183645 – xx and C - IS - 204194 - xx;
- EXIDA Analysis Reports.

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

(**) Type B component: "Complex" component, using micro controller (for details see 7.4.3.1.3 of IEC 61508-2).

2 Functional Safety Specifications from EXIDA and TÜV analysis, report according IEC 61508 - IEC 61511

Table 2: Functional Safety Specifications

Model Number	Safety Function	SFF	PFDavg per year	T Proof Test (Years) for defined SIL value (10% of total safety func.)	T Proof Test (Years) for defined SIL value (20% of total safety func.)	Hardware Fault Tolerance	EXIDA or TÜV analysis	Fail-Safe Output State	λSU (FIT)	λDD (FIT)	λDU (FIT)	MTBF (years)
D1010S 1 Ch. Active	Isolating Repeater Power Supply	91.9%	1.33 E-04	TI = 7 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	202	142	30.5	261
D1010S 1 Ch. Passive	Isolating Repeater Power Supply	91.9%	1.49 E-04	TI = 5 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	229	157	34.1	261
D1010D 2 Ch. Active	Isolating Repeater Power Supply	92.0%	1.34 E-04	TI = 7 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	207	146	30.7	143
D1010D 2 Ch. Passive	Isolating Repeater Power Supply	92.0%	1.50 E-04	TI = 5 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	234	161	34.2	143
D1010S-054 1 Ch.	mV / mA Signal Converter	90.1%	1.58 E-04	TI = 5 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	197	131	36.2	308
D1010S-056 1 Ch.	mV / mA Signal Converter	90.1%	1.58 E-04	TI = 5 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	197	131	36.0	308
D1010S-057 1 Ch.	mV / mA Signal Converter	90.1%	1.58 E-04	TI = 5 SIL 2	TI = 1 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	197	131	36.2	308
D1014S 1 Ch.	Isolating Repeater Power Supply	93.5%	9.91 E-05	TI = 1 SIL 3 TI = 10 SIL 2	TI = 2 SIL 3 TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	166	158	22.6	315
D1014D 2 Ch.	Isolating Repeater Power Supply	93.5%	9.91 E-05	TI = 1 SIL 3 TI = 10 SIL 2	TI = 2 SIL 3 TI = 10 SIL 2	0 - 1	TÜV	<4 mA >20 mA	166	158	22.6	315
D1020S 1 Ch.	Powered Isolating Valve Driver	82.1%	3.08 E-04	TI = 3 SIL 2	TI = 6 SIL 2	0	TÜV	<4 mA	323	0	70.3	282
D1020D 2 Ch.	Powered Isolating Valve Driver	82.1%	3.08 E-04	TI = 3 SIL 2	TI = 6 SIL 2	0 - 1	TÜV	<4 mA	323	0	70.3	282
D1021S 1 Ch.	Powered Isolating Valve Driver (F.D.)	70.7%	5.18 E-04	TI = 1 SIL 2	TI = 3 SIL 2	0	Exida	<4 mA	285	0	118	216
D1032D 2 Ch.	Switch-Proximity Detector Repeat Relay output	81.3%	2.65 E-04	TI = 3 SIL 2	TI = 7 SIL 2	0	TÜV	de-energized	264	0	60.5	232
D1032Q 4 Ch.	Switch-Proximity Detector Repeat Relay output	82.2%	2.65 E-04	TI = 3 SIL 2	TI = 7 SIL 2	0	TÜV	de-energized	280	0	60.4	173
D1033D 2 Ch.	Switch-Proximity Detector Repeat O.C. Trans. output	85.8%	1.63 E-04	TI = 5 SIL 2	TI = 10 SIL 2	0	TÜV	de-energized	224	0	37.2	243
D1033Q 4 Ch.	Switch-Proximity Detector Repeat O.C. Trans. output	86.6%	1.63 E-04	TI = 5 SIL 2	TI = 10 SIL 2	0	TÜV	de-energized	240	0	37.1	179
D1034S 1 Ch.	Switch-Proximity Detector Interface mA output	93.2%	8.41 E-05	TI = 1 SIL 3 TI = 10 SIL 2	TI = 2 SIL 3 TI = 10 SIL 2	0	TÜV	<1.2 mA >7 mA	147	118	19.2	396
D1034D 2 Ch.	Switch-Proximity Detector Interface mA output	93.2%	8.41 E-05	TI = 1 SIL 3 TI = 10 SIL 2	TI = 2 SIL 3 TI = 10 SIL 2	0 - 1	TÜV	<1.2 mA >7 mA	147	118	19.2	396
D1040Q D1042Q D1043Q PSD1001(C) 4 Ch. Bus Powered	Isolating Solenoid Valve Driver for NE loads	80.1%	3.64 E-04	TI = 2 SIL 2	TI = 5 SIL 2	0	Exida	de-energized	334	1	83.0	248
D1040Q D1042Q D1043Q PSD1001(C) 4 Ch. Loop Powered	Isolating Solenoid Valve Driver for NE loads	100%	0.00 E-00	Lifetime = 10 SIL 3	Lifetime = 10 SIL 3	0	Exida	de-energized	418	0	0	248

Model Number	Safety Function	SFF	PFDavg per year	T Proof Test (Years) for defined SIL value (10% of total safety func.)	T Proof Test (Years) for defined SIL value (20% of total safety func.)	Hardware Fault Tolerance	EXIDA or TÜV analysis	Fail-Safe Output State	λSU (FIT)	λDD (FIT)	λDU (FIT)	MTBF (years)
D1044S 1 Ch. Bus Powered, NE or ND loads	Digital Relay Output	85.9%	1.66 E-04	TI = 6 SIL 2	TI = 10 SIL 2	0	TÜV	relay de-energized with NO contact (for NE load) or with NC contact (for ND load)	232	0	38.0	420
D1044S 1 Ch. Loop Powered, NE or ND loads	Digital Relay Output	88.1%	1.40 E-04	TI = 7 SIL 2	TI = 10 SIL 2	0	TÜV	relay de-energized with NO contact (for NE load) or with NC contact (for ND load)	238	0	32.0	420
D1044D 2 Ch. Independent Bus Powered NE or ND loads	Digital Relay Output	86.7%	1.66 E-04	TI = 6 SIL 2	TI = 10 SIL 2	0	TÜV	relay de-energized with NO contact (for NE load) or with NC contact (for ND load)	247	0	38.0	241
D1044D 1oo2 channel architecture Bus Powered NE or ND loads	Digital Relay Output	99.6%	8.32 E-06	TI = 10 SIL 3	TI = 10 SIL 3	0	TÜV	relay de-energized with 2 NO contacts in series (for NE load) or with 2 NC contacts in parallel (for ND load)	468	0	1.9	241
D1044D 1oo2 channel architecture Loop Powered NE or ND loads	Digital Relay Output	99.7%	7.01 E-06	TI = 10 SIL 3	TI = 10 SIL 3	0	TÜV	relay de-energized with 2 NO contacts in series (for NE load) or with 2 NC contacts in parallel (for ND load)	468	0	1.6	241
D1048S 1 Ch. Loop Powered	Digital Output Driver for NE loads	100%	0.00 E-00	Lifetime = 20 SIL 3	Lifetime = 20 SIL 3	0	TÜV	de-energized	358	0	0	291
D1049S 1 Ch. Bus Powered	Digital Output Driver for NE loads	99.6%	8.32 E-06	TI = 12 SIL 3	TI = 20 SIL 3	0	TÜV	de-energized	442	0	1.9	240
D1053S Analog Output	Isolating Analog Signals Converter & Trip Amplifiers	80.9%	4.16 E-04	TI = 2 SIL 2	TI = 4 SIL 2	0	Exida	<4 mA >20 mA	135	267	95.0	208
D1053S (*) 2 Relay Outputs in Series	Isolating Analog Signals Converter & Trip Amplifiers	82.3%	4.11 E-04	TI = 2 SIL 2	TI = 4 SIL 2	0	Exida	de-energized	437	0	94.0	164

(*) Trip amplifier safety function concerns only the alarm with 2 relay outputs in series (terminal blocks 5-8). The analog output is not part of the safety function. Alarm A and Alarm B must be programmed with the same values.

Model Number	Safety Function	SFF	PFDavg per year	T Proof Test (Years) for defined SIL value (10% of total safety func.)	T Proof Test (Years) for defined SIL value (20% of total safety func.)	Hardware Fault Tolerance	EXIDA or TÜV analysis	Fail-Safe Output State	λSU (FIT)	λDD (FIT)	λDU (FIT)	MTBF (years)
D1054S Active IN, Analog OUT	Isolating Repeater Power Supply	89.9%	1.99 E-04	TI = 5 SIL 2	TI = 10 SIL 2	0	TÜV	<4 mA >20 mA	174	230	45.5	197
D1054S Passive IN, Analog OUT	Isolating Repeater Power Supply	90.5%	2.10 E-04	TI = 4 SIL 2	TI = 8 SIL 2	0	TÜV	<4 mA >20 mA	194	261	48.0	197
D1054S Active IN, (*) 2 Relay Outputs in Series	Isolating Repeater Power Supply & Trip Amplifiers	93.1%	1.47 E-04	TI = 6 SIL 2	TI = 10 SIL 2	0	TÜV	de-energized	454	0	33.5	160
D1054S Passive IN, (*) 2 Relay Outputs in Series	Isolating Repeater Power Supply & Trip Amplifiers	93.7%	1.57 E-04	TI = 6 SIL 2	TI = 10 SIL 2	0	TÜV	de-energized	530	0	35.9	160
D1072S 1 Ch. Analog Output	Isolating Temperature Signal Converter	83.9%	3.33 E-04	TI = 3 SIL 2	TI = 6 SIL 2	0	TÜV	<4 mA >20 mA	154	242	76.0	226
D1072D 2 Ch. Analog Output	Isolating Temperature Signal Converter	86.1%	3.71 E-04	TI = 2 SIL 2	TI = 4 SIL 2	0	TÜV	<4 mA >20 mA	248	274	84.7	151
D1073S Analog Output	Isolating Temperature Signal Converter & Trip Amplifiers	83.9%	3.33 E-04	TI = 3 SIL 2	TI = 6 SIL 2	0	TÜV	<4 mA >20 mA	154	242	76.0	197
D1073S (*) 2 Relay Outputs in Series	Isolating Temperature Signal Converter & Trip Amplifiers	88.7%	2.85 E-04	TI = 3 SIL 2	TI = 6 SIL 2	0	TÜV	de-energized	509	0	65.1	158
D1092S 1 Ch. NE Loads	Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0	TÜV	de-energized	185	0	1.60	611
D1092S 1 Ch. ND Loads	Relay Output module	98.0%	1.14 E-05	TI = 7 SIL 3 TI = 20 SIL 2	TI = 15 SIL 3 TI = 20 SIL 2	0	TÜV	energized	124	0	2.61	898
D1092D 2 Ch. NE Loads	Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0 - 1	TÜV	de-energized	185	0	1.60	611
D1092D 2 Ch. ND Loads	Relay Output module	98.0%	1.14 E-05	TI = 7 SIL 3 TI = 20 SIL 2	TI = 15 SIL 3 TI = 20 SIL 2	0 - 1	TÜV	energized	124	0	2.61	898
D1092S-069 1 Ch. NO contact output	NE Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0	TÜV	relay de-energized with NO contact	182	0	1.60	621
D1092S-069 1 Ch. NC contact output	NE Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0	TÜV	relay de-energized with NC contact	182	0	1.60	621
D1092D-069 2 Ch. NO contact output	NE Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0 - 1	TÜV	relay de-energized with NO contact	182	0	1.60	621
D1092D-069 2 Ch. NC contact output	NE Relay Output module	99.1%	7.01 E-06	TI = 10 SIL 3 TI = 20 SIL 2	TI = 20 SIL 3	0 - 1	TÜV	relay de-energized with NC contact	182	0	1.60	621

(*) Trip amplifier safety function concerns only the alarm with 2 relay outputs in series (terminal blocks 5-8). The analog output is not part of the safety function. Alarm A and Alarm B must be programmed with the same values.

Model Number	Safety Function	SFF	PFDavg per year	T Proof Test (Years) for defined SIL value (10% of total safety func.)	T Proof Test (Years) for defined SIL value (20% of total safety func.)	Hardware Fault Tolerance	EXIDA or TÜV analysis	Fail-Safe Output State	λ SU (FIT)	λ DD (FIT)	λ DU (FIT)	MTBF (years)
D1093S 1 Ch. NE Loads	Relay Output module with Line & Load Diagnostics	99.2%	7.01 E-06	TI = 10 SIL 3	TI = 10 SIL 3	0	TÜV	de-energized	199	0	1.60	236 (with diagn.)
D1093S 1 Ch. ND Loads	Relay Output module with Line & Load Diagnostics	98.1%	1.14 E-05	TI = 7 SIL 3 TI = 10 SIL 2	TI = 10 SIL 3	0	TÜV	energized	138	0	2.61	269 (with diagn.)
PSD1206 PSD1210 Single Unit NE Loads	Isolated Switching Power Supply	80.1%	5.90 E-04	TI = 1 SIL 2	TI = 3 SIL 2	0	Exida	<2V; 20V<... ...<30V	542	0	135	134 (with diagn.)
PSD1206 PSD1210 Single Unit ND Loads	Isolated Switching Power Supply	48.3%	1.53 E-03	TI = 5 SIL 1	TI = 10 SIL 1	0	Exida	20V<... ...<30V	327	0	350	134 (with diagn.)
PSD1206 PSD1210 2 Units in parallel NE Loads	Isolated Switching Power Supplies	99.4%	3.03 E-05	TI = 3 SIL 3 TI = 10 SIL 2	TI = 6 SIL 3 TI = 10 SIL 2	1	Exida	<2V; 20V<... ...<30V	1084	0	6.9	79 (with diagn.)
PSD1206 PSD1210 2 Units in parallel ND Loads	Isolated Switching Power Supplies	97.2%	8.09 E-05	TI = 9 SIL 2	TI = 10 SIL 2	1	Exida	20V<... ...<30V	654	0	18.5	112 (with diagn.)

3 Definitions

3.1 Failure categories

In order to judge the failure behavior of the considered modules (except for PSD1206 and PSD1210, explained in detail at sub-section 3.1.1), the following definitions for the failure of the product must be considered:

- ❑ **Fail-Safe State:**
Fail-safe state is defined as the output reaching the user defined threshold or as output being (de-)energized.
- ❑ **Fail Safe:**
Failure mode that causes the module/(sub)system to go to the defined fail-safe state without a demand from the process.
- ❑ **Fail Dangerous:**
Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
- ❑ **Fail Dangerous Undetected:**
Failure mode that is dangerous and that is not detected by internal diagnostics.
- ❑ **Fail Dangerous Detected:**
Failure mode that is dangerous but that is detected by internal diagnostics (these failures may be converted to the selected fail-safe state).
- ❑ **Fail High:** Failure mode that causes the output signal to go to the maximum limit output value.
- ❑ **Fail Low:** Failure mode that causes the output signal to go to the minimum limit output value.
- ❑ **Fail “No Effect”:**
Failure mode of a component that is part of the safety function but has no effect on the safety function. For the calculation of SFF it is treated like a safe undetected failure.
- ❑ **Fail “Annunciation Undetected”:**
Failure mode that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. For the calculation of SFF it is treated like a safe undetected failure.
- ❑ **Fail “Not part”:**
Failure mode 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 considered for the total failure rate evaluation.

Note: The “No Effect” and the “Annunciation Undetected” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the “No Effect” and “Annunciation Undetected” 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 Functional calculation.
- ❑ **Fail-Safe State for: D1010, D1014 ; D1053S, D1054S, D1072, D1073S (using analog output)**
Depending on the application, the fail-safe state is defined as the current output going to a fail low or fail high. For D1053S, D1054S, D1072 and D1073S, these low and high levels can be programmed from the user, and in this functional safety analysis they are set to 20 mA for high and 4 mA for low.
- ❑ **Fail-Safe State for: D1020, D1021S**
The fail-safe state is defined as the output going to fail low.
- ❑ **Fail-Safe State for: D1032, D1033 ; PSD1001(C), D1040, D1042, D1043, D1048S, D1049S (in loop/bus powered mode) ; D1053S, D1054S, D1073S (using 2 relay outputs in series)**
The fail-safe state is defined as the output being de-energized or relay contacts remaining open. For D1053S, D1054S and D1073S the user can program the trip point value at which relay output must be de-energized.
- ❑ **Fail-Safe State for D1034**
The fail-safe state is defined as the output being below 1.2 mA or above 7 mA.
- ❑ **Fail-Safe State for: D1044**
The fail-safe state is defined as the output relay being de-energized, so that: the NO-COM contact is open and the NC-COM contact is closed.
- ❑ **Fail-Safe State for: D1092, D1093S**
The fail-safe state is defined as:
 - the output being de-energized for Normally Energized (NE) loads; or
 - the output being energized for Normally De-energized (ND) loads.

- ❑ **Fail-Safe State for: D1092-069**
 The fail-safe state is defined as the relay being de-energized, so that:

 - the SPST-NO contact remains open; **and**
 - the SPST-NC contact remains closed.
- ❑ **Fail Dangerous for: D1010, D1014 ; D1020, D1021S ; D1053S, D1054S, D1072, D1073S (using analog out)**
 Failure mode 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 % of full span ($> \pm 0.8$ mA), for D1010, D1014, D1020, D1021S and D1054S;
 - 3 % of full span ($> \pm 0.6$ mA), for D1053S, D1072 and D1073S.
- ❑ **Fail Dangerous for: D1032, D1033 ; PSD1001(C), D1040, D1042, D1043, D1049S (in loop/bus powered mode) ; D1053S, D1054S, D1073S (using 2 relay outputs in series)**
 Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that the output remains energized or the relay contacts remain closed.
 For D1053S, D1054S and D1073S this failure leads to a measurement error of more than 3 % (of full span for D1053S and D1073S) or 5 % (of full span for D1054S) respect to the correct value and therefore the relay contacts remains closed (they don't respond to a process demand).
- ❑ **Fail Dangerous for D1034**
 Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or the output current remains between 1.2 mA and 7 mA.
- ❑ **Fail Dangerous for D1044**
 Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) so that the output relay remains energized, keeping the NO-COM contact closed and the NC-COM contact open.
- ❑ **Fail Dangerous for: D1092, D1093S**
 Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) so that the output remains:

 - energized for Normally Energized (NE) loads; **or**
 - de-energized for Normally De-energized (ND) loads.
- ❑ **Fail Dangerous for: D1092-069**
 Failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) so that the relay remains energized, keeping the SPST-NO contact closed and the SPST-NC contact open.
- ❑ **Fail High for: D1010, D1014 ; D1020, D1021S ; D1053S, D1054S, D1072, D1073S (using analog output)**
 Failure mode that causes the output signal to go above the maximum output current (i.e. > 20 mA, which has been chosen in the functional safety analysis as programmed value for D1053S, D1054S, D1072 and D1073S).
- ❑ **Fail High for D1034**
 Failure mode that causes the output signal to go above 7 mA (short circuit).
- ❑ **Fail Low for: D1010, D1014 ; D1020, D1021S ; D1053S, D1054S, D1072, D1073S (using analog output)**
 Failure mode that causes the output signal to go below the minimum output current (i.e. < 4 mA, which has been chosen in the functional safety analysis as programmed value for D1053S, D1054S, D1072 and D1073S).
- ❑ **Fail Low for D1034**
 Failure mode that causes the output signal to go below 0.35 mA (lead breakage).
- ❑ **Fail "No Effect" for: D1010, D1014; D1020, D1021S ; D1053S, D1054S, D1072, D1073S (using analog out)**
 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 ($< \pm 0.8$ mA) for D1010, D1014, D1020, D1021S and D1054S;
 - 3 % of full span ($< \pm 0.6$ mA) for D1053S, D1072 and D1073S.
 For the calculation of SFF it is treated like a safe undetected failure.

3.1.1 Failure categories for PSD1206 and PSD1210

In order to judge the failure behavior of the PSD1206 and PSD1210, the following definitions for the failure of the product must be considered:

- ❑ **Fail-Safe State:** The fail-safe state is defined as the output reaching the user defined threshold.
In normally energized (NE) loads, is defined as the output being between 20 V and 30 V (load current up to 80% of rated) or lower than 2V.
In normally de-energized (ND) loads, is defined as the output being between 20 V and 30 V (load current up to 80% of rated).
- ❑ **Fail Safe:** Failure that causes the output to go to the defined fail-safe state without a demand from the process.
- ❑ **Fail Dangerous:**
With normally energized (NE) loads, failure that leads to an output higher than 30 V or between 2 V and 20 V.
With normally de-energized (ND) loads, failure that leads to an output higher than 30 V or lower than 20 V.
- ❑ **Fail High:** Failure mode that leads to an over voltage condition (> 30 V).
- ❑ **Fail Low:** Failure mode that leads to an under voltage condition (< 2 V).
- ❑ **Fail “No Effect”:** Failure mode of a component that is part of the safety function but has no effect on the safety function. For the calculation of SFF it is treated like a safe undetected failure.
- ❑ **Fail “Annunciation Undetected”:** Failure mode that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. For the calculation of SFF it is treated to 1 % as a dangerous failure and to 99 % as a no effect failure as in this system there are 3 different over voltage protection mechanism.
- ❑ **Fail “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 considered for the total failure rate evaluation.

3.2 General Terms

- **DC:** Diagnostic coverage (safe or dangerous) of the safety logic solver for the considered module.
- **DCs:** Diagnostic coverage for safe failures = $\lambda_{sd} / (\lambda_{sd} + \lambda_{su})$.
- **DCd:** Diagnostic coverage for dangerous failures = $\lambda_{dd} / (\lambda_{dd} + \lambda_{du})$.
- **FIT:** Failure In Time (1×10^{-9} failures per hour).
- **Failure Rates:**
The failure rate data used in the FMEDA analysis 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, and 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.
- **FMEA:**
Failure Modes and Effects Analysis 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.
- **FMEDA:**
Failure Modes Effects and Diagnostic Analysis is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure mode 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 modules. The format for the FMEDA is an extension of the FMEA format MIL STD 1629A.
- **Low demand mode:**
Mode where the frequency of demands for operation made on Safety-related system is no greater than one per year and no greater than twice the proof test frequency.
- **MTBF:** Mean Time Between Failure.
- **MTTF:** Mean Time To Failure.
- **MTTF_s:** Mean Time To safe Failure.
- **MTTF_D:** Mean Time To dangerous Failure.
- **MTTR:** Mean Time To Repair.
- **PFD_{avg}:** Average Probability of Failure on Demand.
- **SFF:**
Safe Failure Fraction, according IEC 61508 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.

$$SFF = \frac{\lambda_{DD} + \lambda_{SD} + \lambda_{SU}}{\lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU}} = 1 - \frac{\lambda_{DU}}{\lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU}}$$

with: λ_{DD} : Dangerous Detected failure rate; λ_{DU} : Dangerous Undetected failure rate
 λ_{SD} : Safe Detected failure rate; λ_{SU} : Safe Undetected failure rate

- **SIF:** Safety Instrumented Function.
- **SIS:** Safety Instrumented System.
- **SIL:** Safety Integrity Level.
- **T Proof Test & Maintenance (TI) :**
Proof Test Interval (for example 1 - 5 - 10 years, with 1 year = 8760 hours).
Maintenance time is considered 8 hours.

4 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Repeater/Driver/Interface/Converter/Relay Modules D1010, D1014, D1020, D1021S, D1032, D1033, D1034, D1040, D1042, D1043, D1044, D1048S, D1049S, D1053S, D1054S, D1072, D1073S, D1092, D1092-069, D1093S and PSD1001(C) power supply.

- ❑ Failure rates are constant, wear out mechanisms are not included. Propagation of failures is not relevant.
- ❑ Failures during parameterization are not considered.
- ❑ The HART protocol is only used for setup, calibration, and diagnostic purposes, not for safety critical operation.
- ❑ The time to restoration or repair time after a safe failure is 8 hours, as MTTR.
- ❑ All modules are operated in the low demand mode of operation.
- ❑ External power supply failure rates are not included.
- ❑ 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 654-1, 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.
- ❑ 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 40°C. 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.
- ❑ Only one input and one output are part of the safety function.
- ❑ For D1010, D1014 and D1053S, D1054S, D1072, D1073S (using analog output) modules, only the current output is used for safety applications.
- ❑ For D1053S, D1054S and D1073S (using 2 relay outputs in series) modules, the trip amplifier safety function concerns only the alarm with 2 relay outputs in series (terminal blocks 5-8). Therefore the analog output is not part of this safety function. In addition, the common cause factor (β) for the 2 relays in series is considered to be 5 %. Then, the 2 relay outputs connected in series can be protected by appropriate mean (e.g. a fuse) which initiates at 60% of the rated current to avoid contact welding.
- ❑ For D1032 - D1033 modules, only the 2nd actuation mode configuration (NO input → ND relay or NO transistor output (or its equivalent NC input → NE relay or NC transistor output)) can be used for safety application. Then, input line short - open fault detection has been enabled to de-energized output relay - transistor in case of fault.
- ❑ For D1049S module, only the 1st operating mode (direct In/Out transfer function: "input high or 24 Vdc → output is energized" or its equivalent "input low or 0 Vdc → output is de-energized") can be used for safety application. For both D1048S and D1049S modules, the override functionality has been disabled, so that the Safety PLC or DCS driving/control signal is the only signal that operates on the channel. In addition, the line and load fault (output short or open circuit) detection has been enabled to de-energized the load in case of fault, until normal condition is restored.
- ❑ The application program in the safety logic solver is configured in such a way that fail low (under-range failure) and fail high (over-range failure) are detected regardless of the effect, safe or dangerous, on the safety function.
- ❑ The 4-20 mA output signal is fed to a SIL 2 - SIL 3 compliant analog input board of a safety PLC.
- ❑ Sufficient test are performed prior to shipment to verify the absence of vendor and/or manufacturing defects, that prevent proper operation of specified functionality to product specifications or cause operation different from design analyzed.
- ❑ Safety Integrity Levels as defined in IEC 61508 and IEC 61511:

SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand)	RRF Risk Reduction Factor	PFDavg Average probability of dangerous failure on demand per hour (high demand)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	from 100000 to 10000	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	from 10000 to 1000	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	From 1000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	From 100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

4.1 Assumption for PSD1206 and PSD1210

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Switching Power Supply Types PSD1206 and PSD1210.

- ❑ Failure rates are constant, wear out mechanisms are not included.
- ❑ Propagation of failures is not relevant.
- ❑ Failures during parameterization are not considered.
- ❑ Sufficient test are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from design analyzed.
- ❑ The device is operated in the low demand mode of operation.
- ❑ The time to restoration or repair time after a safe failure is 8 hours, as MTTR.
- ❑ Only the described versions are used for safety applications.
- ❑ Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- ❑ The fault output is not part of the safety function.
- ❑ The common cause factor β between the two crowbars is estimated at be 5 %.
- ❑ The stress levels are average for an industrial environment and 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 40 °C. 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 40 °C. 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.
- ❑ Over-voltage protection has a diagnostic coverage of 99 %.

5 Summary of Data from EXIDA and TÜV analysis

Note:
in the following “PFDavg vs T[Proof]” tables with determination of SIL, green color indicates that PFDavg of the unit is less than or equal to 10% or 20% of the PFDavg required by its SIL level (see table at section 4), while yellow color indicates that PFDavg of the unit is more than 10% or 20% of the PFDavg required by its SIL level.

5.1 D1010S Isolating Repeater Power Supply, Hart Compatible (Active Input)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 3: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	141.58
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.83
↳ Fail High (detected by the logic solver)	30.50
↳ Fail Low (detected by the logic solver)	109.25
Total Fail Dangerous Undetected = λ_{du}	30.47
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail “No Effect”	201.95
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	374.00
Fail “Not Part” = $\lambda_{notpart}$	62.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	436.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	261 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	565 years
$MTTF_D = 1/\lambda_{du}$	3746 years

Table 4: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	201.95 FIT	141.58 FIT	30.47 FIT	91.85%	0.00%	82.29%

Table 5: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 1.33 E-04 Valid for SIL 2	PFDavg = 9.34 E-04 Valid for SIL 2	PFDavg = 1.33 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 6: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.33 E-04 Valid for SIL 3	PFDavg = 1.33 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.2 D1010S Isolating Repeater Power Supply, Hart Compatible (Passive Input)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 7: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	157.07
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.83
↳ Fail High (detected by the logic solver)	35.04
↳ Fail Low (detected by the logic solver)	120.20
Total Fail Dangerous Undetected = λ_{du}	34.08
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	229.05
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	420.20
Fail "Not Part" = $\lambda_{notpart}$	16.40
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	436.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	261 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	498 years
$MTTF_D = 1/\lambda_{du}$	3350 years

Table 8: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	229.05 FIT	157.07 FIT	34.08 FIT	91.89%	0.00%	82.17%

Table 9: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.49 E-04 Valid for SIL 2	PFDavg = 7.46 E-04 Valid for SIL 2	PFDavg = 1.49 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 10: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.49 E-04 Valid for SIL 3	PFDavg = 1.49 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.3 D1010D Isolating Repeater Power Supply, Hart Compatible (Active Input)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1010D module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the other channel on the first one.

Table 11: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	145.60
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.83
↳ Fail High (detected by the logic solver)	30.50
↳ Fail Low (detected by the logic solver)	113.27
Total Fail Dangerous Undetected = λ_{du}	30.67
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	206.93
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	383.20
Fail "Not Part" = $\lambda_{notpart}$	417.40
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	800.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	143 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	552 years
$MTTF_D = 1/\lambda_{du}$	3722 years

Table 12: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	206.93 FIT	145.60 FIT	30.67 FIT	92.00%	0.00%	82.60%

Table 13: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 1.34 E-04 Valid for SIL 2	PFDavg = 9.40 E-04 Valid for SIL 2	PFDavg = 1.34 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 14: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.34 E-04 Valid for SIL 3	PFDavg = 1.34 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.4 D1010D Isolating Repeater Power Supply, Hart Compatible (Passive Input)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1010D module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the other channel on the first one.

Table 15: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	161.14
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.78
↳ Fail High (detected by the logic solver)	35.16
↳ Fail Low (detected by the logic solver)	124.20
Total Fail Dangerous Undetected = λ_{du}	34.23
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	234.03
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	429.40
Fail "Not Part" = $\lambda_{notpart}$	371.20
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	800.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	143 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	488 years
$MTTF_D = 1/\lambda_{du}$	3335 years

Table 16: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	234.03 FIT	161.14 FIT	34.23 FIT	92.03%	0.00%	82.48%

Table 17: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.50 E-04 Valid for SIL 2	PFDavg = 7.50 E-04 Valid for SIL 2	PFDavg = 1.50 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 18: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.50 E-04 Valid for SIL 3	PFDavg = 1.50 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.5 D1010S-054 Isolating -5 ÷ +55 mV to 4 ÷ 20 mA Converter

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 19: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	130.93
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.90
↳ Fail High (detected by the logic solver)	28.00
↳ Fail Low (detected by the logic solver)	101.03
Total Fail Dangerous Undetected = λ_{du}	36.15
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	197.32
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	364.40
Fail "Not Part" = $\lambda_{notpart}$	6.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	371.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	308 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	579 years
$MTTF_D = 1/\lambda_{du}$	3158 years

Table 20: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	197.32 FIT	130.93 FIT	36.15 FIT	90.08%	0.00%	78.36%

Table 21: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 2	PFDavg = 7.92 E-04 Valid for SIL 2	PFDavg = 1.58 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 22: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 3	PFDavg = 1.58 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.6 D1010S-056 Isolating -5 ÷ +35 mV to 4 ÷ 20 mA Converter

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 23: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	130.88
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.83
↳ Fail High (detected by the logic solver)	27.88
↳ Fail Low (detected by the logic solver)	101.17
Total Fail Dangerous Undetected = λ_{du}	36.03
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	197.29
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	364.20
Fail "Not Part" = $\lambda_{notpart}$	6.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	370.80
MTBF = MTTF + MTTR = $1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	308 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	579 years
$MTTF_D = 1/\lambda_{du}$	3168 years

Table 24: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	197.29 FIT	130.88 FIT	36.03 FIT	90.11%	0.00%	78.41%

Table 25: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 2	PFDavg = 7.89 E-04 Valid for SIL 2	PFDavg = 1.58 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 26: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 3	PFDavg = 1.58 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.7 D1010S-057 Isolating -5 ÷ +10 mV to 4 ÷ 20 mA Converter

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 27: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	130.90
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.83
↳ Fail High (detected by the logic solver)	27.90
↳ Fail Low (detected by the logic solver)	101.17
Total Fail Dangerous Undetected = λ_{du}	36.18
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	197.32
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	364.40
Fail "Not Part" = $\lambda_{notpart}$	6.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	371.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	308 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	579 years
$MTTF_D = 1/\lambda_{du}$	3155 years

Table 28: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	197.32 FIT	130.90 FIT	36.18 FIT	90.07%	0.00%	78.35%

Table 29: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 2	PFDavg = 7.92 E-04 Valid for SIL 2	PFDavg = 1.58 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 30: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.58 E-04 Valid for SIL 3	PFDavg = 1.58 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 7 Section 6

5.8 D1014S and D1014D Isolating Repeater Power Supplies, Hart Compatible

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1014D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1014S (single ch.) are also valid for each channel of D1014D (double ch.).

Table 31: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	158.31
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	1.89
↳ Fail High (detected by the logic solver)	45.89
↳ Fail Low (detected by the logic solver)	110.53
Total Fail Dangerous Undetected = λ_{du}	22.64
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	166.06
↳ Fail Safe Undetected	0.68
↳ Fail "No Effect"	165.38
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	347.01
Fail "Not Part" = $\lambda_{notpart}$	15.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	362.01
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	315 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	687 years
$MTTF_D = 1/\lambda_{du}$	5042 years

Table 32: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	166.06 FIT	158.31 FIT	22.64 FIT	93.48%	0.00%	87.49%

Table 33: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 9.91 E-05 Valid for SIL 3	PFDavg = 9.90 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 2 Section 6

Table 34: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 9.91 E-05 Valid for SIL 3	PFDavg = 1.98 E-04 Valid for SIL 3	PFDavg = 9.90 E-04 Valid for SIL 2
See Note 6 Section 6	See Note 6 Section 6	See Note 7 Section 6

5.9 D1020S and D1020D Powered Isolating Drivers for I/P, Hart Compatible

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1020D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1020S (single ch.) are also valid for each channel of D1020D (double ch.).

Table 35: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	70.32
↪ Fail Dangerous Undetected	49.92
↪ Fail High	20.40
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	323.00
↪ Fail Low	90.14
↪ Fail "No Effect"	231.15
↪ Fail Dangerous Detected	1.71
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	393.32
Fail "Not Part" = $\lambda_{notpart}$	10.88
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	404.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	282 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	353 years
$MTTF_D = 1/\lambda_{du}$	1623 years

Table 36: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	323.00 FIT	0.00 FIT	70.32 FIT	82.12%

Table 37: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 3.08 E-04 Valid for SIL 2	PFDavg = 9.24 E-04 Valid for SIL 2	PFDavg = 3.08 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 38: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 3.08 E-04 Valid for SIL 2	PFDavg = 1.85 E-03 Valid for SIL 2	PFDavg = 3.08 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.10 D1021S Powered Isolating Driver for I/P, with Fault Detection and Hart Compatible

In the following tables are shown functional safety data, as defined in EXIDA Report GM 03/07-24 R001 Version V2, Revision R1.

Table 39: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	118.30
↳ Fail Dangerous Undetected	85.30
↳ Fail High	33.00
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	285.00
↳ Fail Low	109.00
↳ Fail "No Effect"	176.00
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	403.30
Fail "Not Part" = $\lambda_{notpart}$	126.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	529.30
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	216 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	400 years
$MTTF_D = 1/\lambda_{du}$	965 years

Table 40: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	285.00 FIT	0.00 FIT	118.30 FIT	70.66%

Table 41: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 5.18 E-04 Valid for SIL 2	PFDavg = 1.55 E-03	PFDavg = 5.18 E-03
See Note 2 Section 6	See Note 3 and Note 4 Section 6	See Note 3 and Note 4 Section 6

Table 42: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 5.18 E-04 Valid for SIL 2	PFDavg = 1.55 E-03 Valid for SIL 2	PFDavg = 5.18 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.11 D1032D Isolating Switch-Proximity Detector Repeater, Relay Output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1032D module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the other channel on the first one.

Table 43: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	60.51
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	263.79
↪ Fail Safe Undetected	147.17
↪ Fail "No Effect"	114.97
↪ Fail "Annunciation Undetected"	0.16
↪ Fail Dangerous Detected	1.49
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	324.30
Fail "Not Part" = $\lambda_{notpart}$	167.40
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	491.70
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	232 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	433 years
$MTTF_D = 1/\lambda_{du}$	1887 years

Table 44: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	263.79 FIT	0.00 FIT	60.51 FIT	81.34%

Table 45: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 2.65 E-04 Valid for SIL 2	PFDavg = 7.95 E-04 Valid for SIL 2	PFDavg = 2.65 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 46: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 2.65 E-04 Valid for SIL 2	PFDavg = 1.86 E-03 Valid for SIL 2	PFDavg = 2.65 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.12 D1032Q Isolating Switch-Proximity Detector Repeater, Relay Output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 4 channels of D1032Q module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the others channels on the first one.

Table 47: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	60.43
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	279.63
↪ Fail Safe Undetected	151.55
↪ Fail "No Effect"	126.55
↪ Fail "Annunciation Undetected"	0.16
↪ Fail Dangerous Detected	1.37
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	340.06
Fail "Not Part" = $\lambda_{notpart}$	319.45
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	659.51
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	173 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	408 years
$MTTF_D = 1/\lambda_{du}$	1889 years

Table 48: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	279.63 FIT	0.00 FIT	60.43 FIT	82.23%

Table 49: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 2.65 E-04 Valid for SIL 2	PFDavg = 7.94 E-04 Valid for SIL 2	PFDavg = 2.65 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 50: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 2.65 E-04 Valid for SIL 2	PFDavg = 1.85 E-03 Valid for SIL 2	PFDavg = 2.65 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.13 D1033D Isolating Switch-Proximity Detector Repeater, Transistor output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1033D module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the other channel on the first one.

Table 51: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	37.21
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	224.09
↵ Fail Safe Undetected	107.29
↵ Fail "No Effect"	115.15
↵ Fail "Annunciation Undetected"	0.16
↵ Fail Dangerous Detected	1.49
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	261.30
Fail "Not Part" = $\lambda_{notpart}$	209.20
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	470.50
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	243 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	509 years
$MTTF_D = 1/\lambda_{du}$	3068 years

Table 52: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	224.09 FIT	0.00 FIT	37.21 FIT	85.76%

Table 53: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.63 E-04 Valid for SIL 2	PFDavg = 8.15 E-04 Valid for SIL 2	PFDavg = 1.63 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 54: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.63 E-04 Valid for SIL 2	PFDavg = 1.63 E-03 Valid for SIL 2
See Note 7 Section 6	See Note 7 Section 6

5.14 D1033Q Isolating Switch-Proximity Detector Repeater, Transistor output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 4 channels of D1033Q module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the others channels on the first one.

Table 55: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	37.13
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	239.93
↪ Fail Safe Undetected	111.67
↪ Fail "No Effect"	126.73
↪ Fail "Annunciation Undetected"	0.16
↪ Fail Dangerous Detected	1.37
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	277.06
Fail "Not Part" = $\lambda_{notpart}$	361.25
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	638.31
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	179 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	476 years
$MTTF_D = 1/\lambda_{du}$	3074 years

Table 56: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	239.93 FIT	0.00 FIT	37.13 FIT	86.60%

Table 57: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.63 E-04 Valid for SIL 2	PFDavg = 8.13 E-04 Valid for SIL 2	PFDavg = 1.63 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 58: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.63 E-04 Valid for SIL 2	PFDavg = 1.63 E-03 Valid for SIL 2
See Note 7 Section 6	See Note 7 Section 6

5.15 D1034S and D1034D Isolating Switch-Proximity Detector Interfaces, mA output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1034D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1034S (single ch.) are also valid for each channel of D1034D (double ch.).

Table 59: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	117.83
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	0.29
↳ Fail High (detected by the logic solver)	36.83
↳ Fail Low (detected by the logic solver)	80.71
Total Fail Dangerous Undetected = λ_{du}	19.20
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su} = Fail "No Effect"	147.17
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	284.20
Fail "Not Part" = $\lambda_{notpart}$	4.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	288.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	396 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	776 years
$MTTF_D = 1/\lambda_{du}$	5946 years

Table 60: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	147.17 FIT	117.83 FIT	19.20 FIT	93.24%	0.00%	85.99%

Table 61: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 8.41 E-05 Valid for SIL 3	PFDavg = 8.41 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 2 Section 6

Table 62: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 8.41 E-05 Valid for SIL 3	PFDavg = 1.68 E-04 Valid for SIL 3	PFDavg = 8.41 E-04 Valid for SIL 2
See Note 6 Section 6	See Note 6 Section 6	See Note 7 Section 6

5.16 D1040Q, D1042Q, D1043Q, PSD1001(C) Bus Powered Isolating Drivers for NE loads

In the following tables are shown functional safety data, as defined in EXIDA Report GM 04/10-26 R002 Version V1, Revision R1.

Table 63: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	1.49
Total Fail Dangerous Undetected = λ_{du}	83.20
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	333.40
↪ Fail Safe Undetected	196.00
↪ Fail "No Effect"	135.00
↪ Fail "Annunciation Undetected"	2.40
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	418.09
Fail "Not Part" = $\lambda_{notpart}$	42.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	460.69
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	248 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	342 years
$MTTF_D = 1/\lambda_{du}$	1372 years

Table 64: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	333.40 FIT	1.49 FIT	83.20 FIT	80.12%

Table 65: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 3.64 E-04 Valid for SIL 2	PFDavg = 7.28 E-04 Valid for SIL 2	PFDavg = 3.63 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 66: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 3.64 E-04 Valid for SIL 2	PFDavg = 1.82 E-03 Valid for SIL 2	PFDavg = 3.63 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.17 D1040Q, D1042Q, D1043Q, PSD1001(C) Loop Powered Isolating Drivers for NE loads

In the following tables are shown functional safety data, as defined in EXIDA Report GM 04/10-26 R002 Version V1, Revision R1.

Because the loop powered modules are directly driven from the digital output of a safety PLC, there is no additional power supply which can keep the output energized in case of an internal fault. Thus all internal faults have either no effect on the safety function or lead to a safe state, as reported in the following table.

Table 67: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	$\lambda_{notpart}$	MTBF
0.00 FIT	418.09 FIT ("No Effect" = 137.40 FIT)	0.00 FIT	0.00 FIT	100.00%	42.60 FIT	248 years

Considering that the PFDavg value is always equal to zero because $\lambda_{du} = 0.00$ FIT, the SFF > 99% and the hardware fault tolerance is 0, then the Digital Output Modules D1040, D1042, D1043, PSD1001, PSD1001C, when configured in loop powered mode, can be used for SIL 3 safety applications, during their lifetime (up to 10 years).

5.18 D1044S Bus Powered Digital Relay Output for NE or ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 68: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	37.99
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	231.81
↪ Fail Safe Undetected	125.73
↪ Fail "No Effect"	106.08
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	269.80
Fail "Not Part" = $\lambda_{notpart}$	2.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	271.80
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	420 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	492 years
$MTTF_D = 1/\lambda_{du}$	3005 years

Table 69: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	231.81 FIT	0.00 FIT	37.99 FIT	85.92%

Table 70: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 1.66 E-04 Valid for SIL 2	PFDavg = 9.98 E-04 Valid for SIL 2	PFDavg = 1.66 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 71: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.66 E-04 Valid for SIL 2	PFDavg = 1.66 E-03 Valid for SIL 2
See Note 2 Section 6	See Note 2 Section 6

5.19 D1044S Loop Powered Digital Relay Output for NE or ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 72: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	32.00
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	237.80
↪ Fail Safe Undetected	130.22
↪ Fail "No Effect"	107.58
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	269.80
Fail "Not Part" = $\lambda_{notpart}$	2.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	271.80
MTBF = MTTF + MTTR = $1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	420 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	480 years
$MTTF_D = 1/\lambda_{du}$	3567 years

Table 73: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	237.80 FIT	0.00 FIT	32.00 FIT	88.14%

Table 74: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 1.40 E-04 Valid for SIL 2	PFDavg = 9.81 E-04 Valid for SIL 2	PFDavg = 1.40 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 75: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.40 E-04 Valid for SIL 2	PFDavg = 1.40 E-03 Valid for SIL 2
See Note 2 Section 6	See Note 2 Section 6

5.20 D1044D Bus Powered (independent channels) Digital Relay Output for NE or ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 76: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	37.99
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	246.81
↪ Fail Safe Undetected	131.33
↪ Fail "No Effect"	115.48
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	284.80
Fail "Not Part" = $\lambda_{notpart}$	188.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	473.40
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	241 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	462 years
$MTTF_D = 1/\lambda_{du}$	3005 years

Table 77: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	246.81 FIT	0.00 FIT	37.99 FIT	86.66%

Table 78: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 1.66 E-04 Valid for SIL 2	PFDavg = 9.98 E-04 Valid for SIL 2	PFDavg = 1.66 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 79: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.66 E-04 Valid for SIL 2	PFDavg = 1.66 E-03 Valid for SIL 2
See Note 2 Section 6	See Note 2 Section 6

5.21 D1044D Bus Powered (1oo2 channel architecture) Digital Relay Output for NE or ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 80: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.90
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	467.50
↪ Fail Safe Undetected	291.56
↪ Fail "No Effect"	175.94
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	469.40
Fail "Not Part" = $\lambda_{notpart}$	4.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	473.40
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	241 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	244 years
$MTTF_D = 1/\lambda_{du}$	60082 years

Table 81: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	467.50 FIT	0.00 FIT	1.90 FIT	99.59%

Table 82: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% or more of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 8.32 E-06 Valid for SIL 3	PFDavg = 8.32 E-05 Valid for SIL 3
See Note 1 Section 6	See Note 1 Section 6

5.22 D1044D Loop Powered (1oo2 channel architecture) Digital Relay Output for NE or ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 83: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.60
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	467.80
↪ Fail Safe Undetected	288.86
↪ Fail "No Effect"	178.94
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	469.40
Fail "Not Part" = $\lambda_{notpart}$	4.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	473.40
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	241 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	244 years
$MTTF_D = 1/\lambda_{du}$	71347 years

Table 84: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	467.80 FIT	0.00 FIT	1.60 FIT	99.66%

Table 85: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% or more of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3
See Note 1 Section 6	See Note 1 Section 6

5.23 D1048S Loop Powered Digital Output Driver for NE loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

D1048S Loop Powered module is directly supplied from the digital output of the Safety PLC or DCS. If this imposes a shutdown state of the module, there is no additional power supply which can keep the D1048S output energized in case of an internal fault. Thus all internal faults of this module have either “No Effect” on the safety function or lead to the Safe State, according to the definitions in the section 4.

Table 86: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	0.00
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	357.90
↳ Fail Safe Undetected	141.45
↳ Fail “No Effect”	216.45
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	357.90
Fail “Not Part” = $\lambda_{notpart}$	33.70
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	391.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	291 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	319 years
SFF (%) = $1 - (\lambda_{du} / \lambda_{tot\ safe})$	100%
PFDavg = $\frac{1}{2} \lambda_{du}$	0.00 E-00

Therefore, the D1048S module has SIL 3 level for T-proof test interval (TI) of 20 years, equivalent to the product lifetime.

5.24 D1049S Bus Powered Digital Output Driver for NE loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 01.

Table 87: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.90
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	441.90
↳ Fail Safe Undetected	189.19
↳ Fail "No Effect"	252.71
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	443.80
Fail "Not Part" = $\lambda_{notpart}$	31.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	475.40
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	240 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	258 years
$MTTF_D = 1/\lambda_{du}$	60081 years

Table 88: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	441.90 FIT	0.00 FIT	1.90 FIT	99.57%

Table 89: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 12 years	T[Proof] = 20 years
PFDavg = 8.32 E-06 Valid for SIL 3	PFDavg = 9.99 E-05 Valid for SIL 3	PFDavg = 1.66 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 90: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 8.32 E-06 Valid for SIL 3	PFDavg = 1.66 E-04 Valid for SIL 3
See Note 1 Section 6	See Note 1 Section 6

5.25 D1053S Isolating Analog Signals Converter and Trip Amplifiers (using analog output)

In the following tables are shown functional safety data, as defined in EXIDA Report GM 04/10-27 R003 Version V2, Revision R0.

Table 91: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	267.00
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	65.00
↳ Fail High (detected by the logic solver)	82.00
↳ Fail Low (detected by the logic solver)	120.00
Total Fail Dangerous Undetected = λ_{du}	95.00
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	135.00
↳ Fail "No Effect"	134.00
↳ Fail "Annunciation Undetected"	1.00
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	497.00
Fail "Not Part" = $\lambda_{notpart}$	51.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	548.00
MTBF = MTTF + MTTR = $1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	208 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	846 years
$MTTF_D = 1/\lambda_{du}$	1202 years

Table 92: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	135.00 FIT	267.00 FIT	95.00 FIT	80.89%	0.00%	73.76%

Table 93: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 4.16 E-04 Valid for SIL 2	PFDavg = 8.32 E-04 Valid for SIL 2	PFDavg = 4.15 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 94: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 4 years	T[Proof] = 10 years
PFDavg = 4.16 E-04 Valid for SIL 2	PFDavg = 1.66 E-03 Valid for SIL 2	PFDavg = 4.15 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.26 D1053S Isolating Analog Signals Converter and Trip Amplifiers (using 2 relay outputs in series)

In the following tables are shown functional safety data, as defined in EXIDA Report GM 04/10-27 R003 Version V2, Revision R0.

Table 95: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	94.00
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	437.00
↪ Fail Safe Undetected	270.00
↪ Fail "No Effect"	114.00
↪ Fail "Annunciation Undetected"	28.00
↪ Fail Dangerous Detected (by internal diagnostics and converted into Fail Safe Undetected)	25.00
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	531.00
Fail "Not Part" = $\lambda_{notpart}$	160.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	691.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	164 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	261 years
$MTTF_D = 1/\lambda_{du}$	1214 years

Table 96: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	437.00 FIT	0.00 FIT	94.00 FIT	82.30%

Table 97: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 4.11 E-04 Valid for SIL 2	PFDavg = 8.22 E-04 Valid for SIL 2	PFDavg = 4.10 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 98: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 4 years	T[Proof] = 10 years
PFDavg = 4.11 E-04 Valid for SIL 2	PFDavg = 1.64 E-03 Valid for SIL 2	PFDavg = 4.10 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.27 D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using active input and analog output)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 99: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	229.70
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	23.98
↳ Fail High (detected by the logic solver)	35.43
↳ Fail Low (detected by the logic solver)	170.29
Total Fail Dangerous Undetected = λ_{du}	45.52
↳ Fail Dangerous Undetected	45.45
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	174.18
↳ Fail "No Effect"	172.93
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	449.40
Fail "Not Part" = $\lambda_{notpart}$	127.80
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	577.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	197 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	655 years
$MTTF_D = 1/\lambda_{du}$	2507 years

Table 100: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	174.18 FIT	229.70 FIT	45.52 FIT	89.87%	0.00%	83.50%

Table 101: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 1.99 E-04 Valid for SIL 2	PFDavg = 9.97 E-04 Valid for SIL 2	PFDavg = 1.99 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 102: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.99 E-04 Valid for SIL 2	PFDavg = 1.99 E-03 Valid for SIL 2
See Note 7 Section 6	See Note 7 Section 6

5.28 D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using passive input and analog output)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 103: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	261.05
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	25.18
↳ Fail High (detected by the logic solver)	35.43
↳ Fail Low (detected by the logic solver)	200.44
Total Fail Dangerous Undetected = λ_{du}	48.00
↳ Fail Dangerous Undetected	47.93
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	193.95
↳ Fail "No Effect"	192.70
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	503.00
Fail "Not Part" = $\lambda_{notpart}$	74.20
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	577.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	197 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	588 years
$MTTF_D = 1/\lambda_{du}$	2378 years

Table 104: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	193.95 FIT	261.05 FIT	48.00 FIT	90.46%	0.00%	84.50%

Table 105: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 4 years	T[Proof] = 10 years
PFDavg = 2.10 E-04 Valid for SIL 2	PFDavg = 8.41 E-04 Valid for SIL 2	PFDavg = 2.10 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 106: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 8 years	T[Proof] = 10 years
PFDavg = 2.10 E-04 Valid for SIL 2	PFDavg = 1.68 E-03 Valid for SIL 2	PFDavg = 2.10 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.29 D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using active input and 2 relay outputs in series)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 107: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	33.46
↳ Fail Dangerous Undetected	33.39
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	454.34
↳ Fail Safe Undetected	334.42
↳ Fail "No Effect"	118.67
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	487.80
Fail "Not Part" = $\lambda_{notpart}$	225.40
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	713.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	160 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	251 years
$MTTF_D = 1/\lambda_{du}$	3411 years

Table 108: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	454.34 FIT	0.00 FIT	33.46 FIT	93.14%

Table 109: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 1.47 E-04 Valid for SIL 2	PFDavg = 8.79 E-04 Valid for SIL 2	PFDavg = 1.47 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 110: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.47 E-04 Valid for SIL 2	PFDavg = 1.47 E-03 Valid for SIL 2
See Note 7 Section 6	See Note 7 Section 6

5.30 D1054S Isolating Repeater Power Supply and Trip Amplifiers, Hart Compatible (using passive input and 2 relay outputs in series)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 111: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	35.94
↳ Fail Dangerous Undetected	35.87
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	530.46
↳ Fail Safe Undetected	367.07
↳ Fail "No Effect"	162.14
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	566.40
Fail "Not Part" = $\lambda_{notpart}$	146.80
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	713.20
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	160 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	215 years
$MTTF_D = 1/\lambda_{du}$	3176 years

Table 112: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	530.46 FIT	0.00 FIT	35.94 FIT	93.65%

Table 113: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 1.57 E-04 Valid for SIL 2	PFDavg = 9.45 E-04 Valid for SIL 2	PFDavg = 1.57 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 114: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.57 E-04 Valid for SIL 2	PFDavg = 1.57 E-03 Valid for SIL 2
See Note 7 Section 6	See Note 7 Section 6

5.31 D1072S Isolating Temperature Signal Converter, D1073S Isolating Temperature Signal Converter and Trip Amplifiers (using analog output)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 115: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	242.35
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	43.23
↳ Fail High (detected by the logic solver)	78.75
↳ Fail Low (detected by the logic solver)	120.37
Total Fail Dangerous Undetected = λ_{du}	76.01
↳ Fail Dangerous Undetected	75.94
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	154.04
↳ Fail "No Effect"	152.79
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	472.40
<u>D1072S</u> : Fail "Not Part" = $\lambda_{notpart}$	31.40
<u>D1073S</u> : Fail "Not Part" = $\lambda_{notpart}$	107.60
<u>D1072S</u>: Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	503.80
<u>D1073S</u>: Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	580.00
<u>D1072S</u>: MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	226 years
<u>D1073S</u>: MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	197 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	741 years
$MTTF_D = 1/\lambda_{du}$	1502 years

Table 116: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	154.04 FIT	242.35 FIT	76.01 FIT	83.91%	0.00%	76.1%

Table 117: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 3.33 E-04 Valid for SIL 2	PFDavg = 9.99 E-04 Valid for SIL 2	PFDavg = 3.33 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 118: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 3.33 E-04 Valid for SIL 2	PFDavg = 1.998 E-03 Valid for SIL 2	PFDavg = 3.33 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.32 D1072D Isolating Temperature Signal Converter (using analog output)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

The 2 channels of D1072D module should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are not completely independent each other, containing common components. This analysis was executed always considering that the safety function is carried out via 1 input and 1 output channel, but considering also the influence of the other channel on the first one.

Table 119: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	274.16
↳ Fail Dangerous Detected (internal diagnostics or indirectly)	43.23
↳ Fail High (detected by the logic solver)	103.20
↳ Fail Low (detected by the logic solver)	127.73
Total Fail Dangerous Undetected = λ_{du}	84.66
↳ Fail Dangerous Undetected	84.59
↳ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	248.18
↳ Fail "No Effect"	246.93
↳ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	607.00
Fail "Not Part" = $\lambda_{notpart}$	145.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	752.60
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	151 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	460 years
$MTTF_D = 1/\lambda_{du}$	1348 years

Table 120: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCd
0.00 FIT	248.18 FIT	274.16 FIT	84.66 FIT	86.05%	0.00%	76.4%

Table 121: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 10 years
PFDavg = 3.71 E-04 Valid for SIL 2	PFDavg = 7.42 E-04 Valid for SIL 2	PFDavg = 3.71 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 122: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 4 years	T[Proof] = 10 years
PFDavg = 3.71 E-04 Valid for SIL 2	PFDavg = 1.48 E-03 Valid for SIL 2	PFDavg = 3.71 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.33 D1073S Isolating Temperature Converter and Trip Amplifiers (using 2 relay outputs in series)

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 204194 - 02.

Table 123: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	65.13
⚡ Fail Dangerous Undetected	65.06
⚡ 5% * Fail "Annunciation Undetected"	0.07
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	509.07
⚡ Fail Safe Undetected	379.60
⚡ Fail "No Effect"	128.22
⚡ 95% * Fail "Annunciation Undetected"	1.25
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	574.20
Fail "Not Part" = $\lambda_{notpart}$	145.80
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	720.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	158 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	224 years
$MTTF_D = 1/\lambda_{du}$	1752 years

Table 124: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	509.07 FIT	0.00 FIT	65.13 FIT	88.66%

Table 125: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 2.85 E-04 Valid for SIL 2	PFDavg = 8.56 E-04 Valid for SIL 2	PFDavg = 2.85 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 126: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 2.85 E-04 Valid for SIL 2	PFDavg = 1.71 E-03 Valid for SIL 2	PFDavg = 2.85 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6

5.34 D1092S and D1092D Relay Output Modules for NE loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1092D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1092S (single ch.) are also valid for each channel of D1092D (double ch.).

Table 127: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.60
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	185.20
↳ Fail Safe Undetected	156.63
↳ Fail "No Effect"	28.57
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	186.80
Fail "Not Part" = $\lambda_{notpart}$	0.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	186.80
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	611 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	616 years
$MTTF_D = 1/\lambda_{du}$	71347 years

Table 128: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	185.20 FIT	0.00 FIT	1.60 FIT	99.14%

Table 129: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 130: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 3
See Note 6 Section 6	See Note 6 Section 6

5.35 D1092S and D1092D Relay Output Modules for ND loads

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1092D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1092S (single ch.) are also valid for each channel of D1092D (double ch.).

Table 131: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	2.61
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	124.48
↳ Fail Safe Undetected	96.00
↳ Fail "No Effect"	28.48
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	127.09
Fail "Not Part" = $\lambda_{notpart}$	0.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	127.09
MTBF = MTTF + MTTR = $1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	898 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	917 years
$MTTF_D = 1/\lambda_{du}$	43738 years

Table 132: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	124.48 FIT	0.00 FIT	2.61 FIT	97.95%

Table 133: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 20 years
PFDavg = 1.14 E-05 Valid for SIL 3	PFDavg = 8.00 E-05 Valid for SIL 3	PFDavg = 2.29 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 134: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 15 years	T[Proof] = 20 years
PFDavg = 1.14 E-05 Valid for SIL 3	PFDavg = 1.71 E-04 Valid for SIL 3	PFDavg = 2.29 E-04 Valid for SIL 2
See Note 6 Section 6	See Note 6 Section 6	See Note 7 Section 6

5.36 D1092S-069 and D1092D-069 Relay Output Modules, NO contact output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1092D-069 module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1092S-069 (single ch.) are also valid for each channel of D1092D-069 (double ch.).

Table 135: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.60
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	182.20
↳ Fail Safe Undetected	153.63
↳ Fail "No Effect"	28.57
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	183.80
Fail "Not Part" = $\lambda_{notpart}$	0.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	183.80
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	621 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	627 years
$MTTF_D = 1/\lambda_{du}$	71347 years

Table 136: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	182.20 FIT	0.00 FIT	1.60 FIT	99.13%

Table 137: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 138: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 3
See Note 6 Section 6	See Note 6 Section 6

5.37 D1092S-069 and D1092D-069 Relay Output Modules, NC contact output

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx. The 2 channels of D1092D-069 module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D1092S-069 (single ch.) are also valid for each channel of D1092D-069 (double ch.).

Table 139: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.60
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	182.20
↳ Fail Safe Undetected	153.63
↳ Fail "No Effect"	28.57
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	183.80
Fail "Not Part" = $\lambda_{notpart}$	0.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	183.80
MTBF = MTF + MTTR = $1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	621 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	627 years
$MTTF_D = 1/\lambda_{du}$	71347 years

Table 140: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	182.20 FIT	0.00 FIT	1.60 FIT	99.13%

Table 141: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 142: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 1.40 E-04 Valid for SIL 3
See Note 6 Section 6	See Note 6 Section 6

5.38 D1093S Relay Output Module for NE loads, with Line and Load diagnostics

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 143: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	1.60
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	198.80
↵ Fail Safe Undetected	156.63
↵ Fail "No Effect"	42.17
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	200.40
Fail "Not Part" = $\lambda_{notpart}$	283.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	484.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	236 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	574 years
$MTTF_D = 1/\lambda_{du}$	71347 years

Table 144: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	198.80 FIT	0.00 FIT	1.60 FIT	99.20%

Table 145: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3
See Note 1 Section 6	See Note 1 Section 6

Table 146: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 7.01 E-06 Valid for SIL 3	PFDavg = 7.01 E-05 Valid for SIL 3
See Note 6 Section 6	See Note 6 Section 6

5.39 D1093S Relay Output Module for ND loads, with Line and Load diagnostics

In the following tables are shown functional safety data, as defined in TÜV Compliance Certificate C - IS - 183645 - xx.

Table 147: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	2.61
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	138.08
↪ Fail Safe Undetected	96.00
↪ Fail "No Effect"	42.08
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	140.69
Fail "Not Part" = $\lambda_{notpart}$	283.60
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	424.29
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	269 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	827 years
$MTTF_D = 1/\lambda_{du}$	43738 years

Table 148: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	138.08 FIT	0.00 FIT	2.61 FIT	98.14%

Table 149: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 7 years	T[Proof] = 10 years
PFDavg = 1.14 E-05 Valid for SIL 3	PFDavg = 8.00 E-05 Valid for SIL 3	PFDavg = 1.14 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

Table 150: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.14 E-05 Valid for SIL 3	PFDavg = 1.14 E-04 Valid for SIL 3
See Note 6 Section 6	See Note 6 Section 6

5.40 PSD1206 and PSD1210 Isolated Switching Power Supplies for NE loads, single unit

In the following tables are shown functional safety data, as defined in EXIDA Report GMI 06/11-20 R004 Version V1, Revision R0.

Table 151: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	134.80
↳ Fail Dangerous Undetected	134.00
↳ Fail High (1% of Total Fail High)	0.21
↳ Fail "Annunciation Undetected" (1% of Total Fail "Ann. Undet.")	0.59
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	542.20
↳ Fail Safe Undetected	34.00
↳ Fail "No Effect"	214.00
↳ Fail High (99% of Total Fail High)	20.79
↳ Fail Low	215.00
↳ Fail "Annunciation Undetected" (99% of Total Fail "Ann. Undet.")	58.41
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	677.00
Fail "Not Part" = $\lambda_{notpart}$	174.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	851.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	134 years
$MTTF_S = 1/(\lambda_{sd} + \lambda_{su})$	210 years
$MTTF_D = 1/\lambda_{du}$	847 years

Table 152: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	542.20 FIT	0.00 FIT	134.80 FIT	80.09%

Table 153: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 5.90 E-04 Valid for SIL 2	PFDavg = 1.77 E-03	PFDavg = 3.54 E-03	PFDavg = 5.90 E-03
See Note 2 Section 6	See Note 3 and Note 4 Section 6	See Note 3 and Note 4 Section 6	See Note 3 and Note 4 Section 6

Table 154: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 5.90 E-04 Valid for SIL 2	PFDavg = 1.77 E-03 Valid for SIL 2	PFDavg = 3.54 E-03	PFDavg = 5.90 E-03
See Note 7 Section 6	See Note 7 Section 6	See Note 8 and Note 9 Section 6	See Note 8 and Note 9 Section 6

5.41 PSD1206 and PSD1210 Isolated Switching Power Supplies for ND loads, single unit

In the following tables are shown functional safety data, as defined in EXIDA Report GMI 06/11-20 R004 Version V1, Revision R0.

Table 155: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λ_{dd}	0.00
Total Fail Dangerous Undetected = λ_{du}	349.80
⚡ Fail Dangerous Undetected	134.00
⚡ Fail High (1% of Total Fail High)	0.21
⚡ Fail Low	215.00
⚡ Fail "Annunciation Undetected" (1% of Total Fail "Ann. Undet.")	0.59
Total Fail Safe Detected = λ_{sd}	0.00
Total Fail Safe Undetected = λ_{su}	327.20
⚡ Fail Safe Undetected	34.00
⚡ Fail "No Effect"	214.00
⚡ Fail High (99% of Total Fail High)	20.79
⚡ Fail "Annunciation Undetected" (99% of Total Fail "Ann. Undet.")	58.41
Total Failure Rate (Safety Function) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$	677.00
Fail "Not Part" = $\lambda_{notpart}$	174.00
Total Failure Rate (Device) = $\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}$	851.00
MTBF = $MTTF + MTTR = 1/(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du} + \lambda_{notpart}) + MTTR$	134 years
$MTTF_s = 1/(\lambda_{sd} + \lambda_{su})$	349 years
$MTTF_D = 1/\lambda_{du}$	326 years

Table 156: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	327.20 FIT	0.00 FIT	349.80 FIT	48.33%

Table 157: PFDavg vs T[Proof], with determination of SIL supposing module contributes 10% of entire safety function

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 9 years	T[Proof] = 10 years
PFDavg = 1.53 E-03 Valid for SIL 1	PFDavg = 7.66 E-03 Valid for SIL 1	PFDavg = 1.38 E-02	PFDavg = 1.53 E-02
See Note 4 Section 6	See Note 4 Section 6	See Note 5 Section 6	See Note 5 Section 6

Table 158: PFDavg vs T[Proof], with determination of SIL supposing module contributes 20% of entire safety function

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 1.53 E-03 Valid for SIL 1	PFDavg = 1.53 E-02 Valid for SIL 1
See Note 9 Section 6	See Note 9 Section 6

5.42 PSD1206 and PSD1210 Isolated Switching Power Supplies, 2 units in parallel

One way to calculate the PFDavg of a system with 2 power supply units in parallel architecture is by using the fault tree as presented in Figure 1.

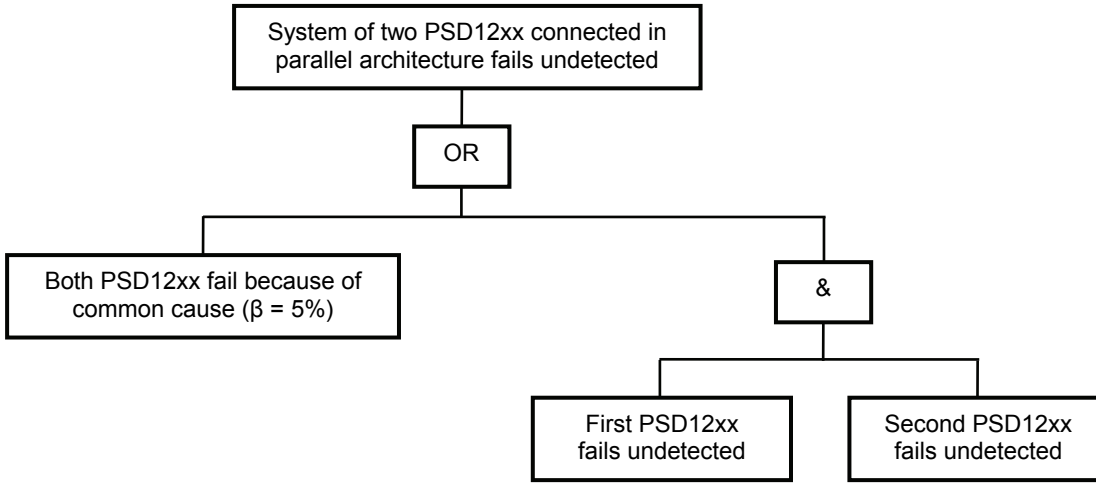


Figure 1: Fault tree diagram for 2 power supply units in parallel (two PSD1210 or two PSD1206 models).

The probability of this system to fail is calculated as follows, considering 5 % β common cause factor, between the two power supply units PSD12xx:

$$\begin{aligned}
 PFD_{AVG_System}(TI = x \text{ years}) &= \beta \cdot PFD_{AVG_PSD12xx}(TI = x \text{ years}) + \left((1 - \beta) \cdot PFD_{AVG_PSD12xx}(TI = x \text{ years}) \right)^2 = \\
 &= \beta \cdot \lambda_{DU} \cdot \frac{TI}{2} + \left((1 - \beta) \cdot \lambda_{DU} \cdot \frac{TI}{2} \right)^2
 \end{aligned}$$

where, λ_{DU} = Dangerous Undetected failure rate of PSD12xx; TI = Proof Test Interval .

5.42.1 NE loads

For 2 power supply units in parallel architecture driving NE loads, it's possible to calculate the system probability to fail for different TI values by using previous $PFD_{AVG_System}(TI = x \text{ years})$ equation and replacing

$PFD_{AVG_PSD12xx}(TI = x \text{ years})$ with values in Table 153 and Table 154 (for 10% and 20% contribution to total SIF) or replacing λ_{DU} with value in Table 152.

Table 159: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 10% of total SIF

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 3.03 E-05 Valid for SIL 3	PFDavg = 9.34 E-05 Valid for SIL 3	PFDavg = 1.90 E-04 Valid for SIL 2	PFDavg = 3.41 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6	See Note 2 Section 6

Table 160: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 20% of total SIF

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 6 years	T[Proof] = 10 years
PFDavg = 3.03 E-05 Valid for SIL 3	PFDavg = 9.34 E-05 Valid for SIL 3	PFDavg = 1.90 E-04 Valid for SIL 3	PFDavg = 3.41 E-04 Valid for SIL 2
See Note 6 Section 6	See Note 6 Section 6	See Note 6 Section 6	See Note 7 Section 6

5.42.2 ND loads

For 2 power supply units in parallel architecture driving ND loads, it's possible to calculate the system probability to fail for different TI values by using previous $PFD_{AVG_System}(TI = x \text{ years})$ equation and replacing $PFD_{AVG_PSD12xx}(TI = x \text{ years})$ with values in Table 157 and Table 158 (for 10% and 20% contribution to total SIF) or replacing λ_{DU} with value in Table 156.

Table 161: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 10% of total SIF

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 9 years	T[Proof] = 10 years
PFDavg = 8.09 E-05 Valid for SIL 2	PFDavg = 4.65 E-04 Valid for SIL 2	PFDavg = 9.40 E-04 Valid for SIL 2	PFDavg = 1.10 E-03
See Note 2 Section 6	See Note 2 Section 6	See Note 2 Section 6	See Note 3 and Note 4 Section 6

Table 162: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 20% of total SIF

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 8.09 E-05 Valid for SIL 2	PFDavg = 1.10 E-03 Valid for SIL 2
See Note 6 Section 6	See Note 6 Section 6

5.43 PSD1206 and PSD1210 Isolated Switching Power Supplies, 3 units in parallel

For 3 power supply units in parallel architecture, it's possible to calculate the system probability to fail for different TI values by using the following equation:

$$PFD_{AVG_System}(TI = x \text{ years}) \cong \beta \cdot \lambda_{DU} \cdot \frac{TI}{2} + \frac{((1-\beta) \cdot \lambda_{DU} \cdot TI)^3}{4}$$

where, $\beta = 5\%$; λ_{DU} = Dangerous Undetected failure rate of PSD12xx; TI = Proof Test Interval .

5.43.1 NE loads

Use previous $PFD_{AVG_System}(TI = x \text{ years})$ equation and replace λ_{DU} with value in Table 152.

Table 163: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 10% of total SIF

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 10 years
PFDavg = 2.99 E-05 Valid for SIL 3	PFDavg = 8.96 E-05 Valid for SIL 3	PFDavg = 2.99 E-04 Valid for SIL 2
See Note 1 Section 6	See Note 1 Section 6	See Note 2 Section 6

5.43.2 ND loads

Use previous $PFD_{AVG_System}(TI = x \text{ years})$ equation and replace λ_{DU} with value in Table 156.

Table 164: $PFD_{AVG_System}(TI = x \text{ years})$, with determination of SIL supposing module contributes 10% of total SIF

T[Proof] = 1 year	T[Proof] = 10 years
PFDavg = 7.80 E-05 Valid for SIL 2	PFDavg = 7.87 E-04 Valid for SIL 2
See Note 2 Section 6	See Note 2 Section 6

5.44 PSD1206 and PSD1210 Isolated Switching Power Supplies, fail with over voltage condition

One way to calculate the probability that the Isolated Switching Power Supply types PSD1206 and PSD1210 fail with an over voltage condition is by using the fault tree as presented in Figure 2. When using fault trees, the PFD should be calculated for multiple time steps (e.g. each hour) and then averaged over the time period of interest.

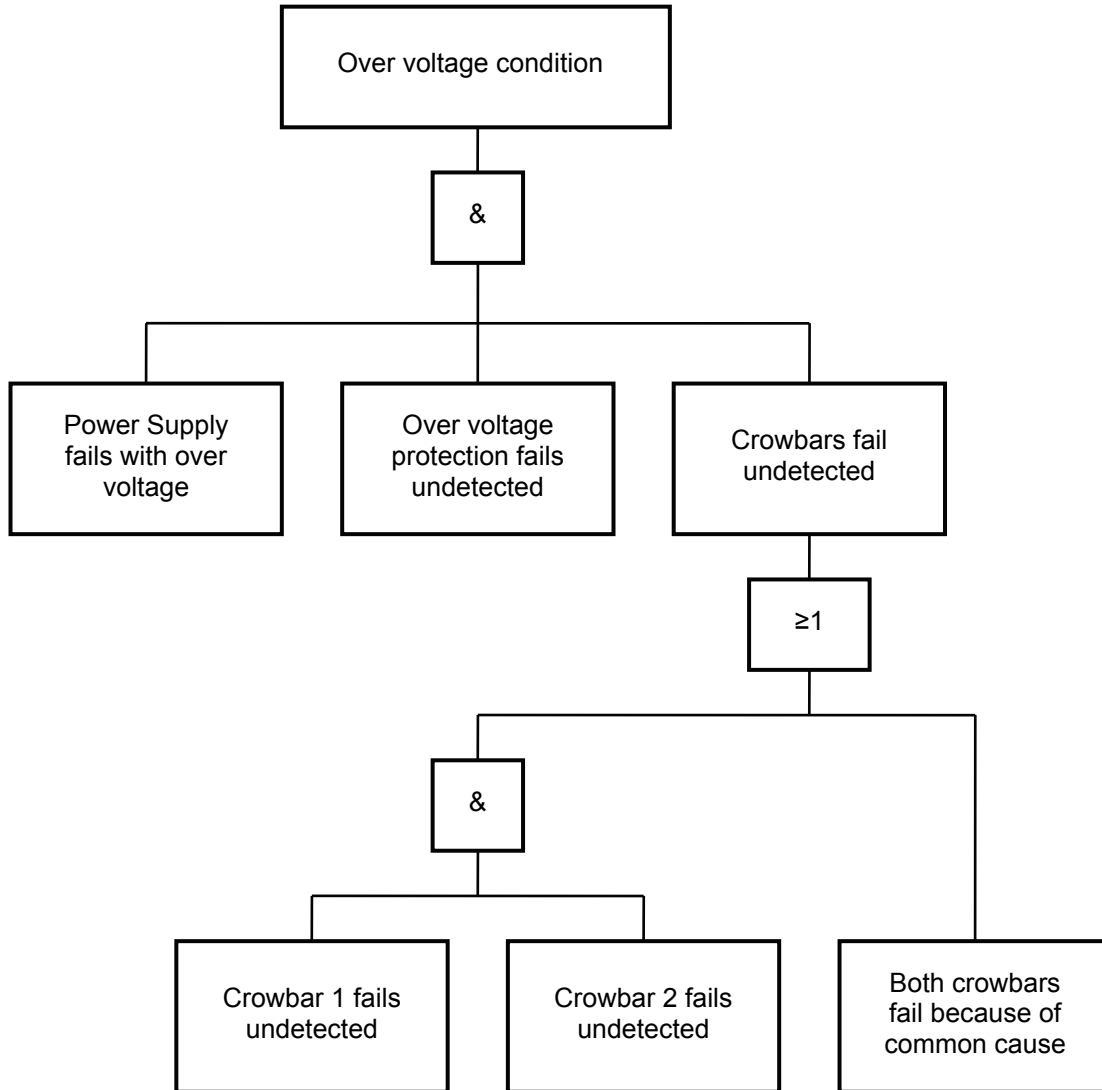


Figure 2: Fault tree for the probability to fail with an over voltage condition.

The probability of the system to fail with an over voltage condition is calculated as follows for each time step:

$$PFD_{AVG_OC_Sys} = PFD_{OC_PS} * PFD_{OP} * PFD_{CB}$$

$$PFD_{CB} = PFD_{CB1} * PFD_{CB2} + \beta * PFD_{CB12}$$

$$PFD_{OC_PS} (T_{proof} = 1 \text{ year}) = 1.84 \text{ E-}04$$

$$PFD_{OP} (T_{proof} = 1 \text{ year}) = 9.64 \text{ E-}05$$

$$PFD_{CB1} (T_{proof} = 1 \text{ year}) = PFD_{CB2} (T_{proof} = 1 \text{ year}) = 2.10 \text{ E-}04$$

$$PFD_{CB12} (T_{proof} = 1 \text{ year}) = 2.11 \text{ E-}04$$

$$\beta * PFD_{CB12} (T_{proof} = 1 \text{ year}) = 0.05 * 2.11 \text{ E-}04 = 1.05 \text{ E-}05$$

$$PFD_{CB} (T_{proof} = 1 \text{ year}) = 1.06 \text{ E-}05$$

$$PFD_{AVG_OC_Sys} (T_{proof} = 1 \text{ year}) = 9.36 \text{ E-}14$$

6 Notes

- **Note 1:**
 Considering a SIL 3 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-03}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 10% of the entire SIF, the PFDavg value of the module must be $\leq 1.00 \text{ E-04}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 3 application.
- **Note 2:**
 Considering a SIL 2 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-02}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 10% of the entire SIF, the PFDavg value of the module must be $\leq 1.00 \text{ E-03}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 2 application.
- **Note 3:**
 Considering a SIL 2 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-02}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 10% of the entire SIF, the PFDavg value of the module must be $\leq 1.00 \text{ E-03}$. This limit is NOT satisfied from the calculated PFDavg value, therefore the module is NOT valid for SIL 2 application, but it's ok for SIL 1.
- **Note 4:**
 Considering a SIL 1 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-01}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 10% of the entire SIF, the PFDavg value of the module must be $\leq 1.00 \text{ E-02}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 1 application.
- **Note 5:**
 Considering a SIL 1 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-01}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 10% of the entire SIF, the PFDavg value of the module must be $\leq 1.00 \text{ E-02}$. This limit is NOT satisfied from the calculated PFDavg value, therefore the module is NOT valid for SIL 1 application.
- **Note 6:**
 Considering a SIL 3 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-03}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 20% of the entire SIF, the PFDavg value of the module must be $\leq 2.00 \text{ E-04}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 3 application.
- **Note 7:**
 Considering a SIL 2 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-02}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 20% of the entire SIF, the PFDavg value of the module must be $\leq 2.00 \text{ E-03}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 2 application.
- **Note 8:**
 Considering a SIL 2 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-02}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 20% of the entire SIF, the PFDavg value of the module must be $\leq 2.00 \text{ E-03}$. This limit is NOT satisfied from the calculated PFDavg value, therefore the module is NOT valid for SIL 2 application, but it's ok for SIL 1.
- **Note 9:**
 Considering a SIL 1 application, the total PFDavg value of the SIF must be $< 1.00 \text{ E-01}$ according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996. However, as the module under consideration contributes for only 20% of the entire SIF, the PFDavg value of the module must be $\leq 2.00 \text{ E-02}$. This limit is satisfied from the calculated PFDavg value, therefore the module is valid for SIL 1 application.
- **Note 10:**
 It is important to realize that the "No Effect" failures and the "Annunciation Undetected" failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures themselves will not affect system reliability or safety, and should not be included in spurious trip calculations.

7 Possible Proof Tests to reveal Dangerous Undetected Failures

According to section 7.4.3.2.2 f) of IEC 61508-2 proof test shall be performed to reveal dangerous failures which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected failures, which have been noted during the FMECA, can be detected during proof testing.

Proof tests should be carried out by qualified service instrumentation technicians.

Any failures or faults should be reported to G.M. International srl (see last page for contact details).

7.1 D1010, D1014

Table 165: Steps for the **Proof test 1**

Steps	Action
1	Bypass the safety-related 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 test 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-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the repeater.

Table 166: Steps for the **Proof test 2**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 165).
3	Perform a two-point calibration (i.e. down and full scale) of the connected transmitter and verify that the current output value stays within the specified values. This requires that the transmitter has already been tested without the repeater and does not contain any dangerous undetected faults.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the repeater.

7.2 D1010S-054, D1010S-056, D1010S-057

Table 167: Steps for the **Proof test 1**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Send a mV signal to the mV / mA converter to go to the full scale current output and verify that the analog current reaches that value. This test 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 mV signal to the mV / mA converter to go to the low scale current output and verify that the analog current reaches that value. This test for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the mV / mA converter.

Table 168: Steps for the **Proof test 2**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 167).
3	Perform a two-point calibration of the mV / mA converter (i.e.: -5mV and +55 mV for D1010S-054; -5mV and +35 mV for D1010S-056; -5mV and +10 mV for D1010S-057) and verify that the output current from the module is within the specified accuracy.
4	Restore the current loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the mV / mA converter.

7.3 D1020, D1021S

Table 169: Steps for the **Proof test 1**

Steps	Action
1	Take appropriate action to avoid a false trip.
2	Provide a 20mA control signal to the driver to open/close the valve and verify that the valve is open/closed. This test for compliance voltage problems such as a 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.
3	Provide a 4mA control signal to the driver to close/open the valve and verify that the valve is closed/open. This test 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.
4	Restore the loop to full operation.
5	Restore normal operation.

This test will detect approximately 70 % of possible Dangerous Undetected failures in the repeater.

Table 170: Steps for the **Proof test 2**

Steps	Action
1	Take appropriate action to avoid a false trip.
2	Perform step 2 and 3 of Proof Test 1 (on Table 169).
3	Perform a two-point calibration of the positioner (i.e. 4mA and 20mA) and verify that the output current from the module is within the specified accuracy. It requires, however, that the positioner has already been tested without the driver and does not contain any dangerous undetected faults.
4	Restore the loop to full operation.
5	Restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the repeater.

7.4 D1032, D1033

Note for contacts input: to detect a broken wire, or a short circuit condition, in the input connections it is necessary to mount, close to the contacts, 1K Ω resistor in series and 10K Ω resistor in parallel to the contacts.

Table 171: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Vary the state conditions of the input sensors/contacts coming from field and verify that relay/transistor outputs change from energized to de-energized and vice versa, and check that the de-energized state condition correspond to the required safety – related function.
3	Disconnect the input wiring coming from the field sensor/contact and check that the proper wire break alarm output is de-energized. Short the input connections and verify that the same output remains de-energized. In both case the proper alarm LEDs, on the front panel, will become red.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the repeater.

7.5 D1034

Note for contacts input: to detect a broken wire, or a short circuit condition, in the input connections it is necessary to mount, close to the contacts, 1K Ω resistor in series and 10K Ω resistor in parallel to the contacts.

Table 172: Steps for the **Proof test**

Steps	Action
1	Take appropriate action to avoid a false trip.
2	Contacts input: Vary the state conditions of the input sensors/contacts connected in the field and verify that the value of output current is about 4mA for closed contacts and about 0.66 mA for open contacts. Proximity input: Vary the state conditions of the proximity switches connected in the field from ON to OFF conditions and verify that the these conditions are correctly transferred to the PLC.
3	Disconnect the input wiring coming from the field sensor/contact and check that the output for open connection conditions is equal or less 0.35mA, and for short circuit conditions equal or above 6.8 mA.
4	Restore the loop to full operation.
5	Restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the repeater.

7.6 D1040, D1042, D1043, PSD1001, PSD1001C

Table 173: Steps for the **Proof test**

Steps	Action
1	Take appropriate action to avoid a false trip.
2	Provide a control signal to the Digital Output Modules D104* and PSD1001 (C) to open/close the driven output and verify that the driven output is open/closed.
3	Restore the loop to full operation.
4	Restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in these Digital Output Modules.

7.7 D1044

Table 174: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	<p>For the single channel, verify the input-to-output channel functionality:</p> <ul style="list-style-type: none"> <input type="checkbox"/> For NO contact, the output load is normally energized (NE) when the input channel is on, while the de-activation (safe state) of the input channel de-energizes the load; <input type="checkbox"/> For NC contact, the output load is normally de-energized (ND) when the input channel is on, while the de-activation (safe state) of the input channel energizes the load. <p>The channel functionality must be verified in the 20 to 30 Vdc supply voltage range of the module. To enable or disable the input channel, connect a DC power supply to the input terminals. To check the ohmic continuity of the NO and NC contacts, connect an ohmmeter in series to NO-COM output contact and another one in series to NC-COM output contact. Execute the following procedure:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Do not enable (DC power supply voltage $\leq 1V$) the input channel (terminals "5" & "6" or "7" & "8") of the unit under test and verify that the ohmic continuity is absent at the NO-COM output contact (terminals "13/14" & "15" or "9/10" & "11"), while it is present at the NC-COM output contact (terminals "16" & "15" or "12" & "11"), so that the 1st requisite is verified; <input type="checkbox"/> Enable (DC power supply voltage $\geq 6V$) the input channel (terminals "5" & "6" or "7" & "8") of the unit under test and verify that the ohmic continuity is present at the NO-COM output contact (terminals "13/14" & "15" or "9/10" & "11"), while it is absent at the NC-COM output contact (terminals "16" & "15" or "12" & "11"), so that the 2nd requisite is verified.
3	Remove the bypass from the safety-related PLC or restore normal operation.

This test detects almost 100 % of all possible Dangerous Undetected failures in the digital relay module.

7.8 D1049S

Table 175: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	<p>Set the following configuration for:</p> <ul style="list-style-type: none"> <input type="checkbox"/> SW1 dip-switch: SW1-1 = OFF (to disable the field line and load fault detection), SW1-2 = SW1-3 = SW1-4 = ON or OFF (because not used); <input type="checkbox"/> SW2 dip-switch: SW2-1 = ON (direct IN/OUT transfer function), SW2-2 = ON , SW2-3 = OFF , SW2-4 = OFF (to enable fault output and disable override input functionality). <p>The series connection of 1 kΩ load resistor with an ammeter must be connected in parallel with a voltmeter to an output of module (starting with Out A, then going on with Out B and finally proceeding with Out C). Supply the module at 24 Vdc. Then, apply the control signal to the input channel of module, which can have the following two states:</p> <ul style="list-style-type: none"> <input type="checkbox"/> OFF = 0 Vdc, implying that load current is 0 mA and load voltage is 0 V because the 1 kΩ load resistor must be de-energized in accordance with OFF state of control input signal; <input type="checkbox"/> ON = 24 Vdc, so that the 1 kΩ load resistor must be energized, with the following current and voltage values: 17.5÷18.5 mA and 17.5÷18.5 V (for Out A); 16.5÷17.5 mA and 16.5÷17.5 V (for Out B); 16÷17 mA and 16÷17 V (for Out C). <p>In addition, disconnect the 1 kΩ load resistor from the output channel in order to generate an open / short output circuit, when line and load fault detection is disabled and control signal = ON:</p> <ul style="list-style-type: none"> <input type="checkbox"/> open circuit: connect only the voltmeter in parallel to output, so that out voltage is 21÷21.5 V; <input type="checkbox"/> short circuit: connect only the ammeter in parallel to output, so that out current is 53÷57 mA. <p><i>(to be continued in the following page)</i></p>

3	<p>(follows from previous page)</p> <p>Consider the configuration setup defined in the previous proof test step (2) and change the dip-switch SW1-1 from OFF to ON position in order to enable the field line and load fault detection. Supply the module at 24 Vdc, apply 24 Vdc = ON control signal to the input channel of module, then connect an ohmmeter to the fault output and another one to the fault bus output. In presence of the 1 kΩ load resistor connected to the output channel, the fault red LED is turned off, the fault output is closed (presence of ohmic continuity) and the fault bus output is open (absence of ohmic continuity) because no line or load fault is detected. Now, disconnect the 1 kΩ load resistor from the output channel in order to generate a line or load fault (open / short circuit fault), so that fault red LED is turned on, the fault output is open (absence of ohmic continuity) and the fault bus output is closed (presence of ohmic continuity). Therefore, generate an open or short output circuit fault executing the following setup changes:</p> <ul style="list-style-type: none"> <input type="checkbox"/> open circuit: connect only the voltmeter in parallel to output of module, so that load voltage is 4÷4.5 V (diagnostic open circuit voltage); <input type="checkbox"/> short circuit: connect only the ammeter in parallel to output of module, so that load current is < 1 mA (diagnostic short circuit current). <p>These results are also valid when the control signal state = OFF and the channel is turned off, because fault diagnostic circuit (if enabled) is always active independently from channel state.</p>
4	<p>Consider the configuration setup defined in the previous proof test step (2) and change the dip-switch SW1-1 from OFF to ON position in order to enable the field line and load fault detection. Substitute the series connection of 1 kΩ load resistor and an ammeter with a current calibrator (set to 45 mA). This generator and a voltmeter are connected in parallel to an output (starting with Out A, then going on with Out B and finally proceeding with Out C). Supply the module at 24 Vdc and apply 24 Vdc = ON control signal to the input channel of module, verifying the following load voltage values: 13÷13.5 V (for Out A), 10.2÷10.7 V (for Out B) and 8.5÷9 V (for Out C).</p>
5	Restore the loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test detects almost 100 % of all possible Dangerous Undetected failures in the digital output module.

7.9 D1053S and D1054S (using analog output)

Table 176: Steps for the **Proof test 1**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	<p><u>For D1053S</u>: send a command to the analog signals converter to go to the full scale current output and verify that the analog current reaches that value.</p> <p><u>For D1054S</u>: by HART command or other technique, set the transmitter connected to the input of the repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.</p>
3	<p><u>For D1053S</u>: send a command to the analog signals converter to go to the low scale current output and verify that the analog current reaches that value. This test for possible quiescent current related failures.</p> <p><u>For D1054S</u>: by HART command or other technique, set the transmitter connected to the input of the repeater in order to go to low alarm current and verify that the output current of repeater reaches that value. This tests for possible quiescent current related failures.</p>
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the analog signals converter or the repeater.

Table 177: Steps for the **Proof test 2**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 176).
3	<p><u>For D1053S</u>: perform a two-point calibration of the analog signals converter (i.e. 4mA and 20mA) and verify that the output current from the module is within the specified accuracy.</p> <p><u>For D1054S</u>: perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the input of the repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.</p>
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the analog signals converter or the repeater.

7.10 D1053S and D1054S (using 2 relay outputs in series)

Table 178: Steps for the **Proof test 1**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Send a command to the analog converter or to the repeater to go to the high alarm current output and verify that the relay contacts (between terminal blocks 5-8) trip.
3	Send a command to the analog converter or to the repeater to go to the low alarm current output and verify that the relay contacts (between terminal blocks 5-8) trip.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the analog signals converter or the repeater and trip amplifiers.

Table 179: Steps for the **Proof test 2**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 178).
3	Perform a two-point calibration of the analog trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 5-8) trip.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 90 % of possible Dangerous Undetected failures in the analog signals converter or the repeater and trip amplifiers.

Table 180: Steps for the **Proof test 3**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Remove the jumper between terminal blocks 6-7.
3	Perform a two-point calibration of the analog trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 5-6) trip.
4	Perform a two-point calibration of the analog trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 7-8) trip.
5	Restore the jumper between terminal blocks 6-7.
6	Restore the loop to full operation.
7	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the analog signals converter or the repeater and trip amplifiers.

7.11 D1072, D1073S (using analog output)

Table 181: Steps for the **Proof test 1**

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Send a command to the temperature converter to go to the full scale current output and verify that the analog current reaches that value. This test 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 command to the temperature converter to go to the low scale current output and verify that the analog current reaches that value. This test for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the temperature signal converter.

Table 182: Steps for the Proof test 2

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 181).
3	Perform a two-point calibration of the temperature converter (i.e. 4mA and 20mA) and verify that the output current from the module is within the specified accuracy.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the temperature signal converter.

7.12 D1073S (using 2 relay outputs in series)

Table 183: Steps for the Proof test 1

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Send a command to the temperature converter to go to the high alarm current output and verify that the relay contacts (between terminal blocks 5-8) trip.
3	Send a command to the temperature converter to go to the low alarm current output and verify that the relay contacts (between terminal blocks 5-8) trip.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 50 % of possible Dangerous Undetected failures in the temperature signal converter and trip amplifiers.

Table 184: Steps for the Proof test 2

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 (on Table 183).
3	Perform a two-point calibration of the temperature trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 5-8) trip.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 90 % of possible Dangerous Undetected failures in the temperature signal converter and trip amplifiers.

Table 185: Steps for the Proof test 3

Steps	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Remove the jumper between terminal blocks 6-7.
3	Perform a two-point calibration of the temperature trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 5-6) trip.
4	Perform a two-point calibration of the temperature trip amplifier (i.e. 4mA and 20mA) and verify that the relay contacts (between terminal blocks 7-8) trip.
5	Restore the jumper between terminal blocks 6-7.
6	Restore the loop to full operation.
7	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the temperature signal converter and trip amplifiers.

7.13 D1092

Table 186: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each D1092D channel or for D1092S single channel, verify input-output functionality for two different application: <ul style="list-style-type: none"> <input type="checkbox"/> normally energized (NE) loads (terminals "1" and "2" for 1st Channel Output; terminals "5" and "6" for 2nd Channel Output): supply each input channel (terminals "13" and "14" for 1st Channel Input; terminals "15" and "16" for 2nd Channel Input) and verify that corresponding load is energized; then shutdown each input channel and verify that corresponding load is de-energized (safe state). <input type="checkbox"/> normally de-energized (ND) loads (terminals "3" and "4" for 1st Channel Output; terminals "7" & "8" for 2nd Channel Output): supply each input channel (terminals "13" and "14" for 1st Channel Input; terminals "15" and "16" for 2nd Channel Input) and verify that corresponding load is energized (safe state); then shutdown each input channel and verify that corresponding load is de-energized.
3	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 90% of possible Dangerous Undetected failures in the relay module.

7.14 D1092-069

Table 187: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each D1092D-069 channel or for D1092S-069 single channel, verify input-output functionality for two different application: <ul style="list-style-type: none"> <input type="checkbox"/> SPST NO contact (terminals "1" and "2" for 1st Ch. Output; terminals "5" and "6" for 2nd Ch. Output): supply each input channel (terminals "13" and "14" for 1st Ch. Input; terminals "15" and "16" for 2nd Ch. Input) and verify that corresponding SPST NO contact is closed; then shutdown each input channel and verify that corresponding SPST NO contact is open (safe state). <input type="checkbox"/> SPST NC contact (terminals "3" and "4" for 1st Ch. Output; terminals "7" and "8" for 2nd Ch. Output): supply each input channel (terminals "13" and "14" for 1st Ch. Input; terminals "15" and "16" for 2nd Ch. Input) and verify that corresponding SPST NC contact is open; then shutdown each input channel and verify that corresponding SPST NC contact is closed (safe state).
3	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 90% of possible Dangerous Undetected failures in the relay module.

7.15 D1093S

Table 188: Steps for the **Proof test**

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Supply diagnostic circuit (terminals "9-11" and "10-12") and watch LEDs or fault output for verification. For D1093S single channel, verify input-output functionality for two different application: <ul style="list-style-type: none"> <input type="checkbox"/> normally energized (NE) loads (terminals "5" and "6"): supply input channel (terminals "13" & "14") and verify that load is energized; then shutdown input channel and verify that load is de-energized (safe state). In both cases, if load is disconnected (fault condition), the fault red LED must be lit and the fault output must be de-energized. <input type="checkbox"/> normally de-energized (ND) loads (terminals "7" & "8"): supply input channel (terminals "13" & "14") and verify that load is energized (safe state); then shutdown input channel and verify that load is de-energized. In both cases, if load is disconnected (fault condition), the fault red LED must be lit and the fault output must be de-energized.
3	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 90% of possible Dangerous Undetected failures in the relay module.

7.16 PSD1206, PSD1210

This procedure specifies the type of test that must be carried on the supply unit at the end of the T-proof period of operation to verify the correct operation of protection circuits in the supply unit required to restore the SIL (Safety Integrity Level) required. The estimated efficiency of the test is 60 % for the power supply itself and 99 % for the protective means (over voltage protection and crowbars).

The functions to be tested are:

- Output current capability.
- Crowbar A operation.
- Crowbar B operation.
- Over voltage limiting.
- Paralleling diode operation.
- Current sharing capability.

7.16.1 Test Setup

Equipments items required to perform the test are:

- Ampere meter with a range 0 to 10 A with a resolution of 0.1 A or better.
- 300 W variable power resistor, adjustable between 2 and 25 Ω , with a current capability of 10 A for testing of model PSD1210 or 150 W variable power resistor, adjustable between 4 and 25 Ω , with a current capability of 6 A to test model PSD1206.
- A 10 K Ω trimmer.

7.16.2 Test of single Power Supply or individual unit of “N” unit in parallel

Make sure that the power supply unit under test can be disconnected without creating operational malfunctions or damages to the system. Then connect the test circuit set-up components according to the test set-up schematic.

Table 189: Steps for the **Proof test 1 (Output current capability)**

Steps	Action
1	Set the load resistor to 25 Ω for minimum loading.
2	Connect the mains power connections and apply power to the test circuit, wait 30 minutes for warm-up and stabilization.
3	Check voltage at output terminals to be within the limits (23.6 Vdc to 24.4 Vdc) and adjust the voltage regulating trimmer if required.
4	Adjust load current to 10 A for PSD1210 or 6 A for PSD1206.
5	Check voltage at output terminals to be within the limits (23.6 Vdc to 24.4 Vdc) and load current to be as above.

Table 190: Steps for the **Proof test 2 (Crowbar A operation)**

Steps	Action
1	Connect a jumper between test terminals B1 and B2 to disable over voltage protection.
2	Connect a jumper between test terminals S2 and COM to disable crowbar B.
3	Turn the trimmer to have the maximum resistance.
4	Connect the 10 K Ω trimmer between terminals C1 and C2.
5	Monitor output voltage that should be above 24 V nominal at 80% of full load, slowly turn the trimmer to decrease its resistance and observe the corresponding output voltage that should increase.
6	At some point the crowbar A will fire shorting the output voltage to < 2 V. The maximum voltage obtained just before the crowbar firing point should be between 27.0 V and 29.0 V.
7	Shutdown the power supply to reset the crowbar.
8	Turn the trimmer fully to have the maximum resistance.
9	Disconnect the jumper from test terminals S2 and COM.

Table 191: Steps for the **Proof test 3 (Crowbar B operation)**

Steps	Action
1	Switch on the power supply.
2	Connect a jumper between test terminals S1 and COM to disable crowbar A.
3	Monitor output voltage that should be above 24 V nominal at 80% of full load, slowly turn the trimmer to decrease its resistance and observe the corresponding output voltage that should increase.
4	At some point the crowbar B will fire shorting the output voltage to < 2 V. The maximum voltage obtained just before the crowbar firing point should be between 27.0 V and 29.0 V.
5	Shutdown the power supply to reset the crowbar.
6	Disconnect the trimmer from terminals C1 and C2.
7	Disconnect the jumper from test terminals S1 and COM.
8	Disconnect the jumper between test terminals B1 and B2 to enable the over voltage protection.

Table 192: Steps for the **Proof test 4 (Over-voltage Protection operation)**

Steps	Action
1	Switch on the power supply.
2	Connect a jumper between test terminals S1 and COM to disable crowbar A.
3	Connect a jumper between test terminals S2 and COM to disable crowbar B.
4	Connect a jumper between test terminals A1 and A2 to disable voltage regulation circuit.
5	Verify output voltage that should be between 25.5 V and 28 V nominal at 80% of full load.
6	Disconnect the jumper from test terminals S1 and COM.
7	Disconnect the jumper from test terminals S2 and COM.
8	Disconnect the jumper from test terminals A1 and A2.

7.16.3 Tests required when the unit is used as subsystem of “N” units in parallel

This test is required only if the power supply unit is used in parallel configuration and may be skipped otherwise. However if the system is updated the test must be performed before start-up.

Table 193: Steps for the **Proof test 5 (Paralleling diode operation)**

Steps	Action
1	Shutdown the other Power Supply units.
2	Connect the mains power connections and apply power to the power supply under test, wait 30 minutes for warm-up and stabilization.
3	Adjust load current to 10 A for PSD1210 or 6 A for PSD1206.
4	Connect a voltmeter across the paralleling diode terminals D2(+) and D1(-) and check that voltage drop is within limits (0.3 V to 0.7 V).
5	Switch on at least one other power supply.
6	Switch off the supply under test.
7	Check that the voltage across paralleling diode to be within limits (-22 V to -26 V).

Table 194: Steps for the **Proof test 6 (Current sharing capability)**

Steps	Action
1	Connect to the output of each power supply an ampere meter in order to measure the individual output current.
2	Connect the output in parallel to the required load.
3	Connect the current sharing terminal blocks (CS).
4	Connect the mains power to all the units under test.
5	Check voltage at output terminals to be within the limits (23.6 Vdc to 24.4 Vdc).
6	Adjust load current to the maximum required by the system.
7	Check the output current from each unit, which should have a spread not greater than 10%.

To maintain the power supply system safety integrity level, SIL 2 (ND loads) or SIL 3 (NE loads), also during the T-proof periodic test, in addition two redundant units for each system are required.

If N is the number of power supply units connected in parallel, for the maximum load current required to the power supply system without redundancy, the total number of modules must be N+2.

In the following, the PSD1210 model is used (10 A at 24 Vdc), but the concept is also applicable to PSD1206 model (6 A at 24 Vdc).

Table 195: Number of power supply units connected in parallel for different maximum load currents required to the power supply system.

Maximum load current required to the power supply system (A)	Number of power supply units at least required to satisfy maximum load current N	Number of power supply units, with redundancy required for normal operation of system N+1	Number of power supply units, with redundancy required for normal operation and during T-proof periodic test of system N+2
10	1	2	3
20	2	3	4
30	3	4	5
40	4	5	6
50	5	6	7
	<p><u>For NE load:</u> a) SIL 2 with T-proof = 1 year; b) SIL 2 with T-proof = 3 years.</p> <p><u>For ND load:</u> c) SIL 1 with T-proof = 5 years; d) SIL 1 with T-proof = 10 years.</p> <p>During T-proof of each power supply unit, the power supply system can not sustain the maximum load current because redundancy (N+1) is absent.</p>	<p><u>For NE load:</u> a) SIL 3 with T-proof = 3 years or SIL 2 with T-proof = 10 years; b) SIL 3 with T-proof = 6 years or SIL 2 with T-proof = 10 years.</p> <p><u>For ND load:</u> c) SIL 2 with T-proof = 9 years or SIL 1 with T-proof = 10 years; d) SIL 2 with T-proof = 10 years.</p> <p>During T-proof of each power supply unit, the power supply system can sustain the maximum load current but SIL value changes from SIL 3 to SIL 2 (for NE load) or from SIL 2 to SIL 1 (for ND load), because redundancy (N+2) is absent.</p>	<p><u>For NE load:</u> a) SIL 3 with T-proof = 3 years; b) SIL 3 with T-proof = 6 years.</p> <p><u>For ND load:</u> c) SIL 2 with T-proof = 9 years; d) SIL 2 with T-proof = 10 years.</p> <p>During T-proof of each power supply unit, the power supply system can sustain the maximum load current and maintain SIL 3 value (for NE load) or SIL 2 value (for ND load), because redundancy (N+2) is present.</p>

Where: a) or c) supposing that power supply system doesn't contribute more than 10 % of total SIF dangerous failure;
b) or d) supposing that power supply system doesn't contribute more than 20 % of total SIF dangerous failure.

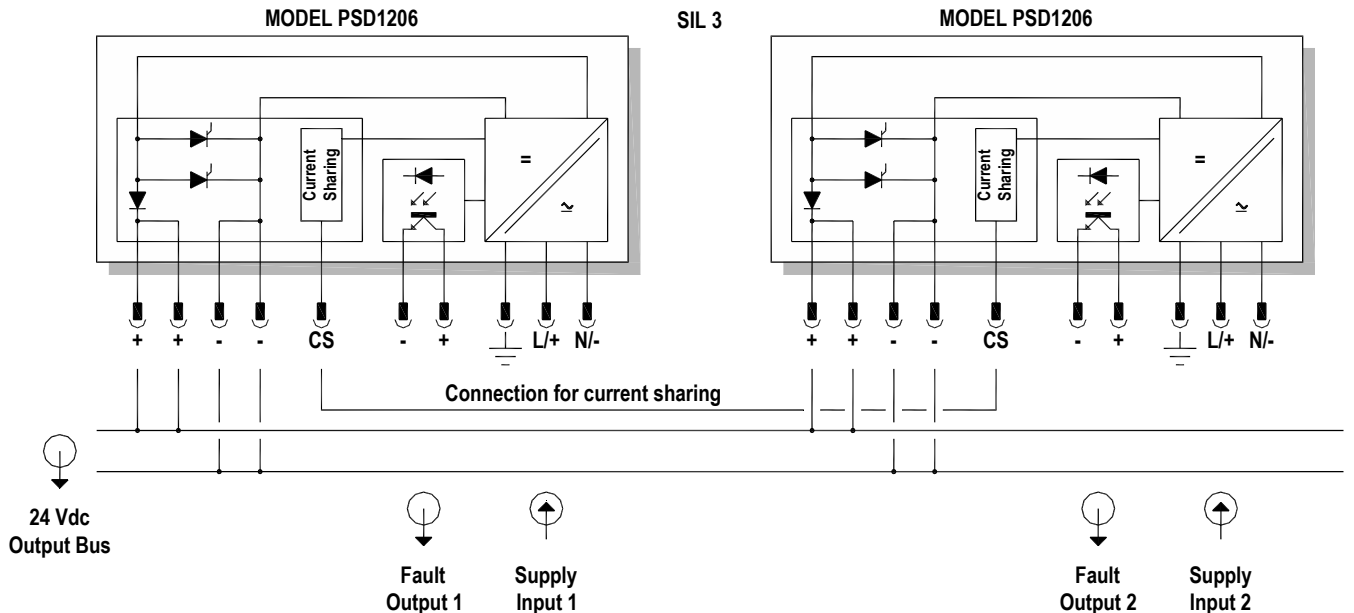


Figure 3: Draft about connection of 2 units PSD1206 in parallel mode.

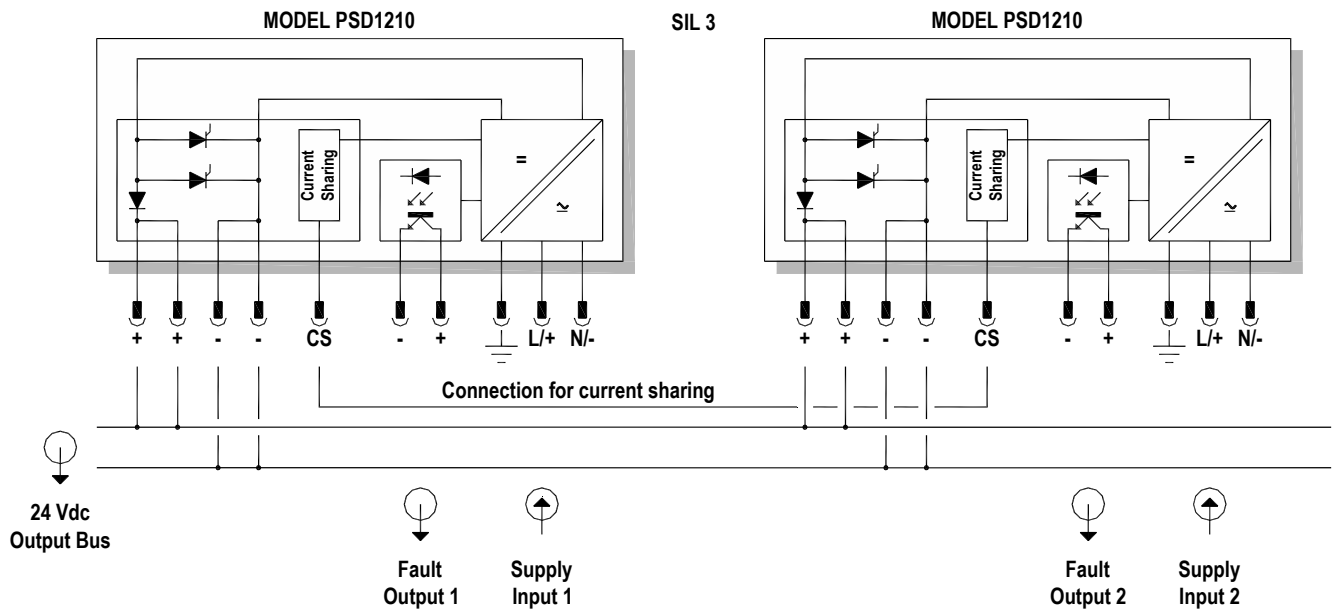


Figure 4: Draft about connection of 2 units PSD1210 in parallel mode.

8 Impact of Lifetime of Critical Components on Failure Rate

Although a constant failure rate is assumed by the probabilistic estimation method (see section 3 and 4) this only applies provided that the useful lifetime of components is not exceeded. Beyond this 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 to temperature).

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 PFDavg 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.

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 the IEC 61508-2 experience has shown that the useful lifetime often lies within a range of about 10-15 years.

9 Influence of PFDavg calculation on efficiency of Proof Test for a 1oo1 architecture.

The equation of PFDavg, applicable when the component or sub-system is new and when λ_{du} are 99 % known by proof test is:

$$PFD_{avg} = \lambda_{du} \times \frac{TI}{2}$$

When these tests do not detect at least 99 % of λ_{du} the same equation changes to:

$$PFD_{avg} = (Et \times \lambda_{du} \times \frac{TI}{2}) + (1 - Et) \times \lambda_{du} \times \frac{SL}{2}$$

where:

Et is the effectiveness of proof test (0-100 %)

SL can be intended as one of the following:

- 1) Time between two proof tests with 99-100 % effectiveness;
- 2) Time between two replacements;
- 3) Component Lifetime if no substitution and no proof test is meant to be done.

For $TI = 1$ year the equation becomes:

$$PFD_{avg} = \left(Et \times \frac{\lambda_{du}}{2} \right) + (1 - Et) \times \lambda_{du} \times \frac{SL}{2}$$

Example 1:

$\lambda_{du} = 0.01 / \text{yr}$; $TI = 1 \text{ yr}$; $SL = 12 \text{ yrs}$; $Et = 90 \% = 0.9$; $PFD_{avg} = 0.0002 / \text{yr}$

At installation: $PFD_{avg} = 0.01 / 2 = 0.005 / \text{yr}$; $RRF = 1 / PFD_{avg} = 1 / 0.005 = 200$ (Suitable for SIL 2)

After 1 yr: $PFD_{avg} = (0.9 \times 0.01/2) + (0.1 \times 0.01 \times 6) = 0.0105$; $RRF = 95$ (Suitable for SIL 1)

Example 2:

$\lambda_{du} = 0.01 / \text{yr}$; $TI = 1 \text{ yr}$; $SL = 12 \text{ yrs}$; $Et = 99 \% = 0.99$; $PFD_{avg} = 0.0002 / \text{yr}$

At installation: $PFD_{avg} = 0.01 / 2 = 0.005 / \text{yr}$; $RRF = 1 / PFD_{avg} = 1 / 0.005 = 200$ (Suitable for SIL 2)

After 1 yr: $PFD_{avg} = (0.99 \times 0.01/2) + (0.01 \times 0.01 \times 6) = 0.0056$; $RRF = 178$ (Suitable for SIL 2)