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

This Safety Manual summarizes the results of hardware assessment carried out on the following Intrinsically Safe modules:
Repeater – Driver – Interface D1010S-054 (or -056 or -057), D1021S, D1034, D1040, D1042, D1043; Analog Signals Converter and Trip Amplifier D1053S;Relay Output module, Power Supply PSD1001(C), PSD1206, PSD1210.

Table 1: Model – Output channels – Safety Function Table

Model	Output channels	Component type	Safety Function
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
D1021S	1	A	Powered Isolating Valve Driver with Fault Detection, HART compatible
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.)
D1053S	1	B	Isolating Analog Signals Converter and Trip Amplifiers
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 the table 2 of IEC 61508-1, the average PFD for systems operating in low demand mode has to be from ≥ 1.00 E-03 to < 1.00 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% ÷ 20% of this range. For SIL 2 application the total PFDavg value of the SIF must be smaller than 1.00 E-02, hence the maximum allowable PFDavg value for the asset modules would then be 1.00 E-03 (for 10% contribution) and 2.00 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-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
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
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
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
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.)

(*) 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.

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: D1053S, (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, 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: PSD1001(C), D1040, D1042, D1043, (in loop/bus powered mode) ; D1053S, (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 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 Dangerous for: D1021S; D1053S (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 (> ± 0.8 mA), for D1021S;
  - ● 3 % of full span (> ± 0.6 mA), for D1053S.

- **Fail Dangerous for: PSD1001(C), D1040, D1042, D1043, (in loop/bus powered mode) ; D1053S,(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, this failure leads to a measurement error of more than 3 % (of full span for D1053S or 5 % 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 High for: D1021S ; D1053S, (using analog output)**
  Failure mode that causes the output signal to go above the maximum output current (i.e. > 20 mA, which has been choosen in the functional safety analysis as programmed value for D1053S).
- **Fail High for D1034**
  Failure mode that causes the output signal to go above 7 mA (short circuit).
- **Fail Low for: D1021S ; D1053S, (using analog output)**
  Failure mode that causes the output signal to go below the minimum output current (i.e. < 4 mA, which has been choosen in the functional safety analysis as programmed value for D1053S.
- **Fail Low for D1034**
  Failure mode that causes the output signal to go below 0.35 mA (lead breakage).
- **Fail "No Effect" for: D1021S ; D1053S (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 (< ± 0.8 mA) for D1021S
  - 3 % of full span (< ± 0.6 mA) for D1053S.

  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 = λsd / (λsd + λsu).
- ❑ **DCd:** Diagnostic coverage for dangerous failures = λdd / (λdd + λdu).
- ❑ **FIT:** Failure In Time (1x10 E-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 where chosen in a way that is appropriate for safety integrity level verification calculations, and to mach 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.
- ❑ **PFDavg:** 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: λDD: Dangerous Detected failure rate; λDU: Dangerous Undetected failure rate
  λSD: Safe Detected failure rate; λSU: 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 D1021S, D1034, D1040, D1042, D1043, D1053S, 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 and D1053S, (using analog output) modules, only the current output is used for safety applications.
- For D1053S,(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.
- 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-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 3: Failure rates

Failure category	**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd	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 = λdu	36.15
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu = Fail "No Effect"	197.32
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**364.40**
Fail "Not Part" = λnotpart	6.60
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**371.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**308 years**
MTTF$_S$ = 1/(λsd + λsu)	579 years
MTTF$_D$ = 1/λdu	3158 years

Table 4: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**	**DCs**	**DCd**
0.00 FIT	197.32 FIT	130.93 FIT	36.15 FIT	90.08%	0.00%	78.36%

Table 5: 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 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 = 1.58 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

5.2 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 7: Failure rates

Failure category	**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd	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 = λdu	36.03
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu = Fail “No Effect”	197.29
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**364.20**
Fail “Not Part” = λnotpart	6.60
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**370.80**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**308 years**
MTTF_S = 1/(λsd + λsu)	579 years
MTTF_D = 1/λdu	3168 years

Table 8: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**	**DCs**	**DCd**
0.00 FIT	197.29 FIT	130.88 FIT	36.03 FIT	90.11%	0.00%	78.41%

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 = 1.58 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 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 = 1.58 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

5.3 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 11: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λdd	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 = λdu	36.18
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu = Fail “No Effect”	197.32
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**364.40**
Fail “Not Part” = λnotpart	6.60
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**371.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**308 years**
MTTF$_S$ = 1/(λsd + λsu)	579 years
MTTF$_D$ = 1/λdu	3155 years

Table 12: Failure rates according to IEC 61508

λsd	λsu	λdd	λdu	SFF	DCs	DCd
0.00 FIT	197.32 FIT	130.90 FIT	36.18 FIT	90.07%	0.00%	78.35%

Table 13: 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 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 = 1.58 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

5.4 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 15: Failure rates

Failure category	**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd	0.00
Total Fail Dangerous Undetected = λdu	118.30
↳ Fail Dangerous Undetected	85.30
↳ Fail High	33.00
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu	285.00
↳ Fail Low	109.00
↳ Fail "No Effect"	176.00
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**403.30**
Fail "Not Part" = λnotpart	126.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**529.30**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**216 years**
$MTTF_S$ = 1/(λsd + λsu)	400 years
$MTTF_D$ = 1/λdu	965 years

Table 16: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**
0.00 FIT	285.00 FIT	0.00 FIT	118.30 FIT	70.66%

Table 17: 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 18: 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

5.5 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 19: Failure rates

Failure category	**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd	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 = λdu	19.20
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu = Fail "No Effect"	147.17
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**284.20**
Fail "Not Part" = λnotpart	4.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**288.20**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**396 years**
$MTTF_S$ = 1/(λsd + λsu)	776 years
$MTTF_D$ = 1/λdu	5946 years

Table 20: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**	**DCs**	**DCd**
0.00 FIT	147.17 FIT	117.83 FIT	19.20 FIT	93.24%	0.00%	85.99%

Table 21: 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 22: 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

5.6 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 23: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λdd	1.49
Total Fail Dangerous Undetected = λdu	83.20
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu	333.40
↳ Fail Safe Undetected	196.00
↳ Fail "No Effect"	135.00
↳ Fail "Annunciation Undetected"	2.40
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**418.09**
Fail "Not Part" = λnotpart	42.60
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**460.69**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**248 years**
$MTTF_S$ = 1/(λsd + λsu)	342 years
$MTTF_D$ = 1/λdu	1372 years

Table 24: Failure rates according to IEC 61508

λsd	λsu	λdd	λdu	SFF
0.00 FIT	333.40 FIT	1.49 FIT	83.20 FIT	80.12%

Table 25: 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 26: 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

5.7 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 27: Failure rates according to IEC 61508

λsd	λsu	λdd	λdu	SFF	λnotpart	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 λdu = 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 them lifetime (up to 10 years).

5.8 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 28: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λdd	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 = λdu	95.00
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu	135.00
↳ Fail “No Effect”	134.00
↳ Fail “Annunciation Undetected”	1.00
Total Failure Rate (Safety Function) = λsd + λsu + λdd + λdu	**497.00**
Fail “Not Part” = λnotpart	51.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**548.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**208 years**
$MTTF_S$ = 1/(λsd + λsu)	846 years
$MTTF_D$ = 1/λdu	1202 years

Table 29: Failure rates according to IEC 61508

λsd	λsu	λdd	λdu	SFF	DCs	DCd
0.00 FIT	135.00 FIT	267.00 FIT	95.00 FIT	80.89%	0.00%	73.76%

Table 30: 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 31: 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

5.9 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 32: Failure rates

Failure category	**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd	0.00
Total Fail Dangerous Undetected = λdu	94.00
Total Fail Safe Detected = λsd	0.00
Total Fail Safe Undetected = λsu	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) = λsd + λsu + λdd + λdu	**531.00**
Fail “Not Part” = λnotpart	160.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**691.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**164 years**
MTTF_S = 1/(λsd + λsu)	261 years
MTTF_D = 1/λdu	1214 years

Table 33: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**
0.00 FIT	437.00 FIT	0.00 FIT	94.00 FIT	82.30%

Table 34: 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 35: 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

5.10 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 36: Failure rates

Failure category		**Failure rates (FIT)**
Total Fail Dangerous Detected = λdd		0.00
Total Fail Dangerous Undetected = λdu		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 = λsd		0.00
Total Fail Safe Undetected = λsu		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) = λsd + λsu + λdd + λdu		**677.00**
Fail "Not Part" = λnotpart		174.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart		**851.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR		**134 years**
$MTTF_S$ = 1/(λsd + λsu)	210 years	
$MTTF_D$ = 1/λdu	847 years	

Table 37: Failure rates according to IEC 61508

λsd	**λsu**	**λdd**	**λdu**	**SFF**
0.00 FIT	542.20 FIT	0.00 FIT	134.80 FIT	80.09%

Table 38: 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 39: 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

5.11 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 40: Failure rates

Failure category	Failure rates (FIT)
Total Fail Dangerous Detected = λdd	0.00
Total Fail Dangerous Undetected = λdu	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 = λsd	0.00
Total Fail Safe Undetected = λsu	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) = λsd + λsu + λdd + λdu	**677.00**
Fail “Not Part” = λnotpart	174.00
Total Failure Rate (Device) = λsd + λsu + λdd + λdu + λnotpart	**851.00**
MTBF = MTTF + MTTR = 1/(λsd + λsu + λdd + λdu + λnotpart) + MTTR	**134 years**
MTTF_S = 1/(λsd + λsu)	349 years
MTTF_D = 1/λdu	326 years

Table 41: Failure rates according to IEC 61508

λsd	λsu	λdd	λdu	SFF
0.00 FIT	327.20 FIT	0.00 FIT	349.80 FIT	48.33%

Table 42: 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 43: 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

5.12 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.

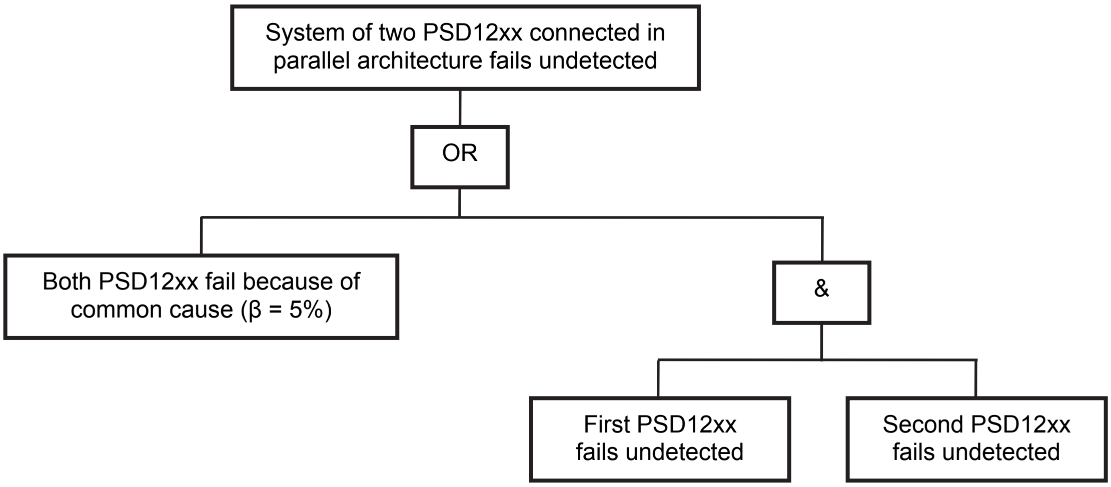
System of two PSD12xx connected in parallel architecture fails undetected
OR
Both PSD12xx fail because of common cause (β = 5%)
&
First PSD12xx fails undetected
Second PSD12xx fails undetected

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:

$$PFD_{AVG\_\mathrm{System}}(TI = x\ years) = \beta \cdot PFD_{AVG\_\mathrm{PSD12xx}}(TI = x\ years) + \left(\left(1-\beta\right) \cdot PFD_{AVG\_\mathrm{PSD12xx}}(TI = x\ years)\right)^2 =$$

$$= \beta \cdot \lambda_{DU} \cdot \frac{TI}{2} + \left(\left(1-\beta\right) \cdot \lambda_{DU} \cdot \frac{TI}{2}\right)^2$$

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

5.12.1 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 $PFD_{AVG\_\mathrm{System}}(TI = x\ years)$ equation and replacing $PFD_{AVG\_\mathrm{PSD12xx}}(TI = x\ years)$ with values in Table 38 and Table 39 (for 10% and 20% contribution to total SIF) or replacing λ_{DU} with value in Table 37.

Table 44: $PFD_{AVG\_\mathrm{System}}(TI = x\ years)$, 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 45: $PFD_{AVG\_\mathrm{System}}(TI = x\ years)$, 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

5.12.2 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 $PFD_{AVG\_\text{System}}(TI = x\ years)$ equation and replacing $PFD_{AVG\_\text{PSD12xx}}(TI = x\ years)$ with values in Table 42 and Table 43 (for 10% and 20% contribution to total SIF) or replacing λ_{DU} with value in Table 41.

Table 46: $PFD_{AVG\_\text{System}}(TI = x\ years)$, 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 47: $PFD_{AVG\_\text{System}}(TI = x\ years)$, 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

5.13 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:

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

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

5.13.1 NE loads

Use previous $PFD_{AVG\_\text{System}}(TI = x\ years)$ equation and replace λ_{DU} with value in Table 37.

Table 48: $PFD_{AVG\_\text{System}}(TI = x\ years)$, 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

5.13.2 ND loads

Use previous $PFD_{AVG\_\text{System}}(TI = x\ years)$ equation and replace λ_{DU} with value in Table 41.

Table 49: $PFD_{AVG\_\text{System}}(TI = x\ years)$, 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

5.14 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.

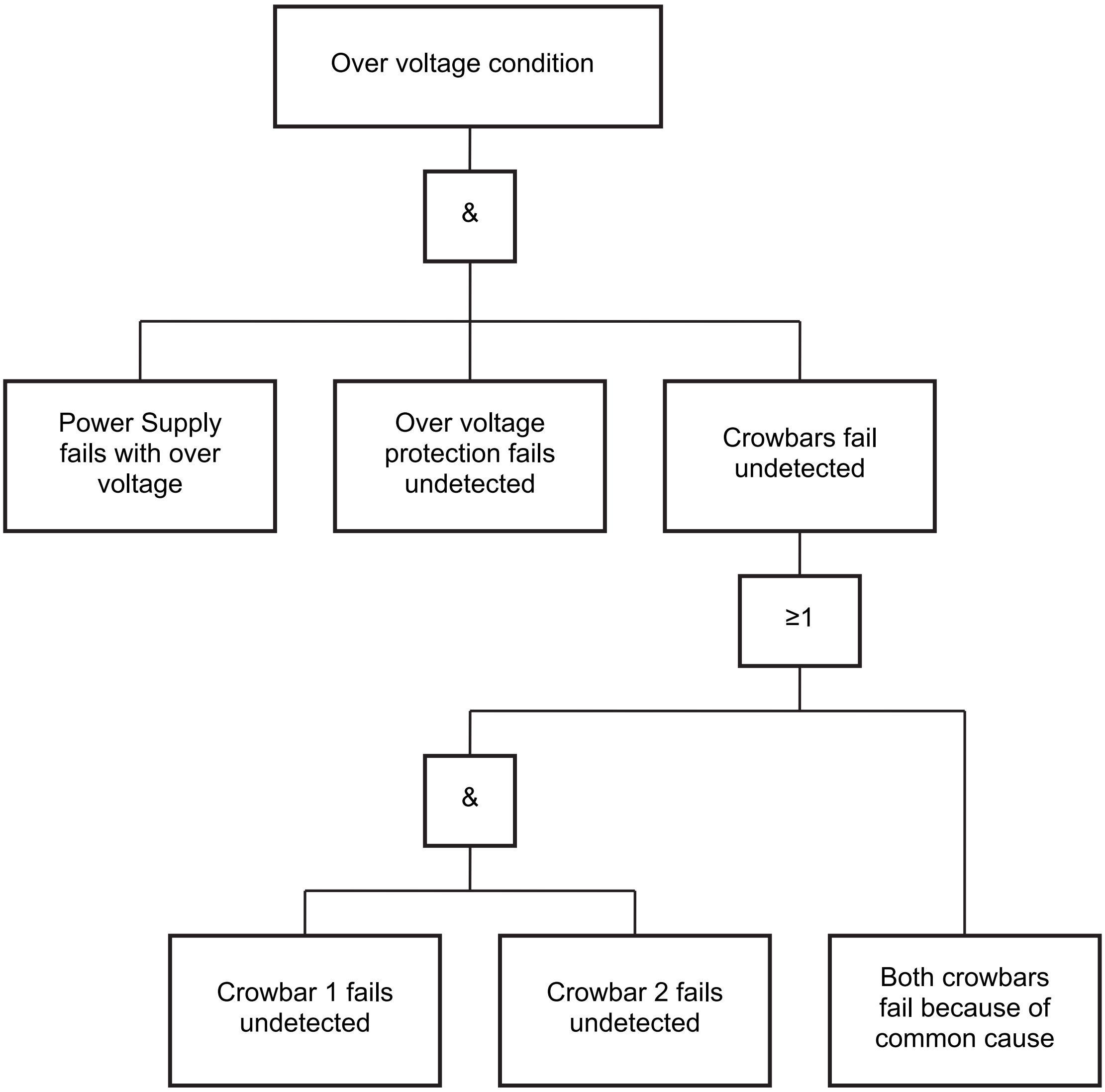
Over voltage condition
&
Power Supply fails with over voltage
Over voltage protection fails undetected
Crowbars fail undetected
≥1
&
Crowbar 1 fails undetected
Crowbar 2 fails undetected
Both crowbars fail because of common cause

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 (Tproof = 1 year) = 1.84 E-04
PFD_OP (Tproof = 1 year) = 9.64 E-05
PFD_CB1 (Tproof = 1 year) = PFD_CB2 (Tproof = 1 year) = 2.10 E-04
PFD_CB12 (Tproof = 1 year) = 2.11 E-04
β * PFD_CB12 (Tproof = 1 year) = 0.05 * 2.11 E-04 = 1.05 E-05
PFD_CB (Tproof = 1 year) = 1.06 E-05

$PFD_{AVG}\_OC\_Sys$ (Tproof = 1 year) = 9.36 E-14

6 Notes

- **Note 1:**
  Considering a SIL 3 application, the total PFDavg value of the SIF must be < 1.00 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 ≤ 1.00 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 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 ≤ 1.00 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 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 ≤ 1.00 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 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 ≤ 1.00 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 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 ≤ 1.00 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 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 ≤ 2.00 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 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 ≤ 2.00 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 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 ≤ 2.00 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 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 ≤ 2.00 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 FMEDA, 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 D1010S-054, D1010S-056, D1010S-057

Table 50: 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 51: 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 50).
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.

7.2 D1021S

Table 52: 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 53: 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 52).
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.

.

7.3 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, 1KΩ resistor in series and 10KΩ resistor in parallel to the contacts.

Table 54: 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.

7.4 D1040, D1042, D1043, PSD1001, PSD1001C

Table 55: 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.

7.5 D1053S (using analog output)

Table 56: 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 signals converter to go to the full scale current output and verify that the analog current reaches that value.
3	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.
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 57: 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 56).
3	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.
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.

7.6 D1053S (using 2 relay outputs in series)

Table 58: 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 59: 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 58).
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 60: 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.

7.7 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.

7.7.1 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 KΩ trimmer.

7.7.2 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 61: 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 62: 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 KΩ 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 63: 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 64: 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.

7.7.3 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 65: 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 66: 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 67: 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

	For NE load:
	a) SIL 2 with T-proof = 1 year;
	b) SIL 2 with T-proof = 3 years.
	For ND load:
	c) SIL 1 with T-proof = 5 years;
	d) SIL 1 with T-proof = 10 years.
	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.
		For NE load:
		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.
		For ND load:
		c) SIL 2 with T-proof = 9 years or SIL 1 with T-proof = 10 years;
		d) SIL 2 with T-proof = 10 years.
		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.
			For NE load:
			a) SIL 3 with T-proof = 3 years;
			b) SIL 3 with T-proof = 6 years.
			For ND load:
			c) SIL 2 with T-proof = 9 years;
			d) SIL 2 with T-proof = 10 years.
			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.

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.

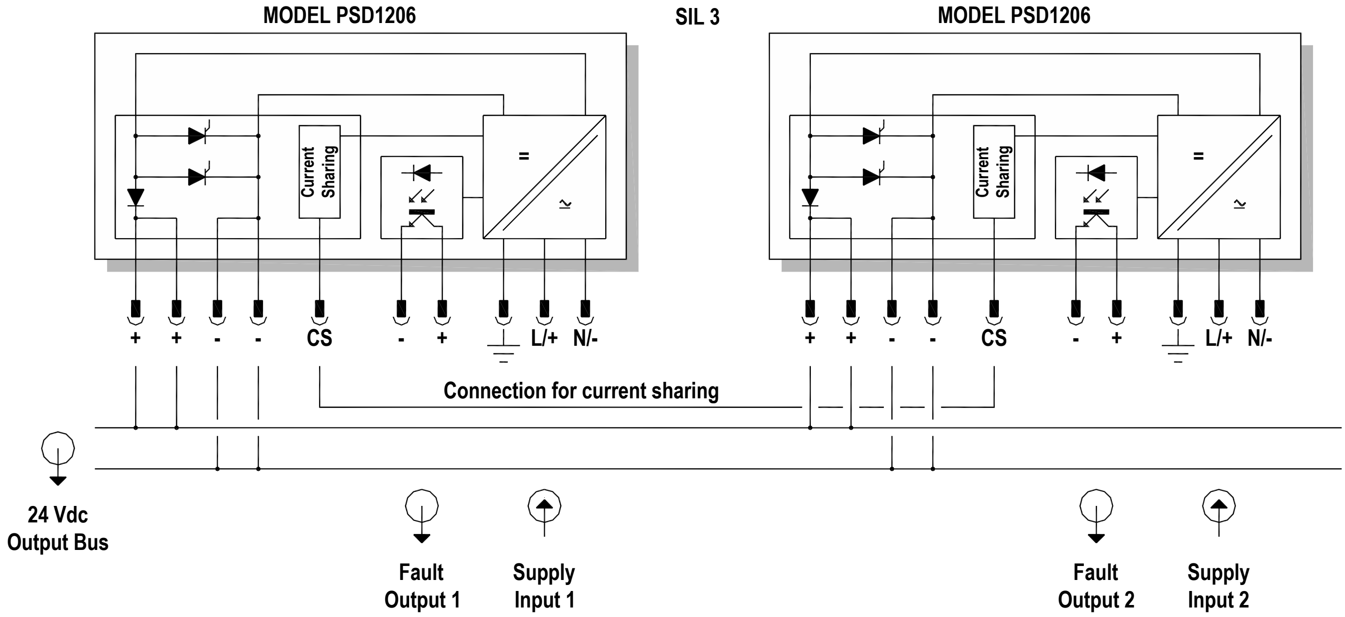

Figure 3: Draft about connection of 2 units PSD1206 in parallel mode.

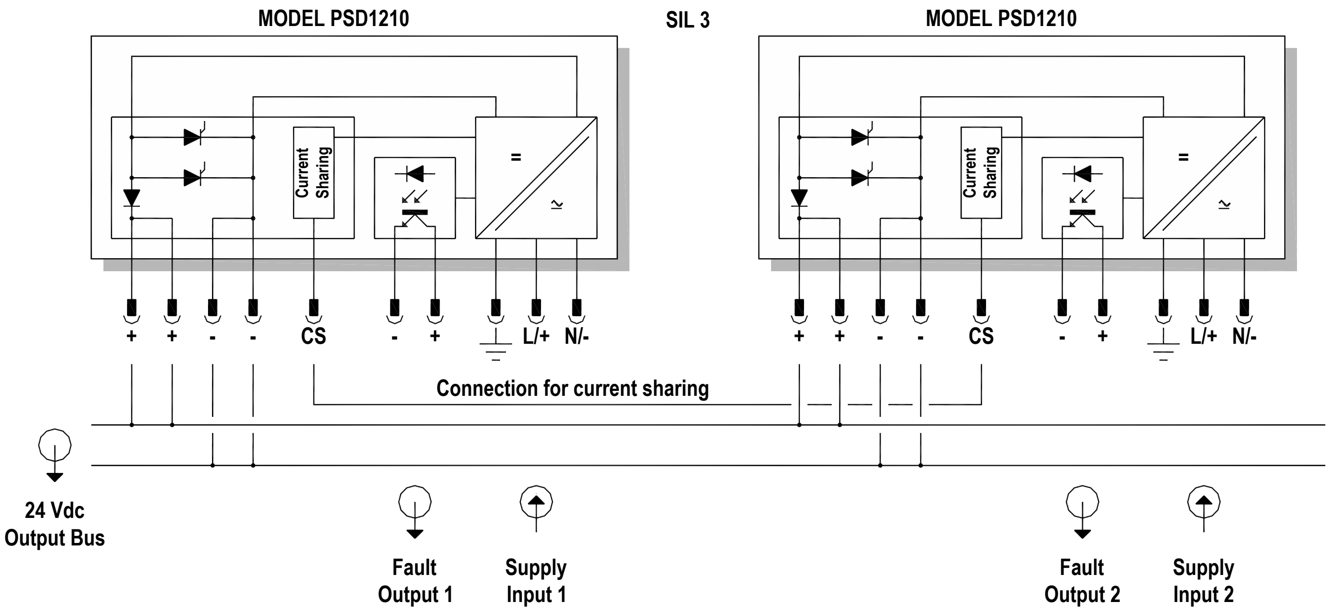

Figure 4: Draft about connection of 2 units PSD1210 in parallel mode.

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 λdu are 99 % known by proof test is:

$$PFDavg = \lambda du \times \frac{TI}{2}$$

When these tests do not detect at least 99 % of λdu the same equation changes to:

$$PFDavg = (Et \times \lambda du \times \frac{TI}{2}) + (1 - Et) \times \lambda du \times \frac{SL}{2}$$

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:

$$PFDavg = \left(Et \times \frac{\lambda du}{2} \right) + \left(1 - Et\right) \times \lambda du \times \frac{SL}{2}$$

Example 1:

λdu = 0.01 / yr ; TI = 1 yr ; SL = 12 yrs ; Et = 90 % = 0.9 ; PFDavg = 0.0002 / yr

At installation: PFDavg = 0.01 / 2 = 0.005 / yr ; RRF = 1 / PFDavg = 1 / 0.005 = 200 (Suitable for SIL 2)

After 1 yr: PFDavg = (0.9 x 0.01/2) + (0.1 x 0.01 x 6) = 0.0105 ; RRF = 95 (Suitable for SIL 1)

Example 2:

λdu = 0.01 / yr ; TI = 1 yr ; SL = 12 yrs ; Et = 99 % = 0.99 ; PFDavg = 0.0002 / yr

At installation: PFDavg = 0.01 / 2 = 0.005 / yr ; RRF = 1 / PFDavg = 1 / 0.005 = 200 (Suitable for SIL 2)

After 1 yr: PFDavg = (0.99 x 0.01/2) + (0.01 x 0.01 x 6) = 0.0056 ; RRF = 178 (Suitable for SIL 2)