



Failure Modes, Effects and Diagnostic Analysis

Project:

Switching Power Supply Types PSD1206 and PSD1210

Customer:

G.M. International s.r.l

Villasanta

Italy

Contract No.: GMI 06/11-20

Report No.: GMI 06/11-20 R004

Version V1, Revision R0, July 2007

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the switching power supply types PSD1206 and PSD1210. Table 1 gives an overview of the different versions that were considered during the assessment.

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

Table 1: Version overview

	Type	Description
[V1]	PSD1206	24 VDC, 6 A, 150 W
[V2]	PSD1210	24 VDC, 10 A, 250 W

For safety applications only the described versions were considered. All other possible variants or electronics are not covered by this report.

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

The switching power supply types PSD1206 and PSD1210 are considered to be Type A¹ subsystems with a hardware fault tolerance of 0. For Type A subsystems with a hardware fault tolerance of 0 the SFF can be less than 60% according to table 2 of IEC 61508-2 when used in a SIL 1 safety function. Type A subsystems with a hardware fault tolerance of 0 shall have a SFF of greater than 60% according to table 2 of IEC 61508-2 when used in a SIL 2 safety function.

The following tables show how the above stated requirements are fulfilled for the two considered safety functions “normally energized load” and “normally de-energized load”:

SF1: Normally energized load

$$\lambda_{\text{SAFE_NE}} = 542,2 \text{ FIT}$$

$$\lambda_{\text{DANGEROUS_NE}} = 134,8 \text{ FIT}$$

$$\lambda_{\text{total}} = 677 \text{ FIT}$$

$$\text{MTBF} = 134 \text{ years}$$

$$\text{SFF} = 80\%$$

$$\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 5,90\text{E-}04$$

SIL capability: SIL2² for single use

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

² With a hardware fault tolerance of 1 SIL3 capability is possible. Assuming a common cause factor of 5% the $\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 3,03\text{E-}05$.

SF2: Normally de-energized load

$$\lambda_{\text{SAFE_ND}} = 327,2 \text{ FIT}$$

$$\lambda_{\text{DANGEROUS_ND}} = 349,8 \text{ FIT}$$

$$\lambda_{\text{total}} = 677 \text{ FIT}$$

$$\text{MTBF} = 134 \text{ years}$$

$$\text{SFF} = 48\%$$

$$\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 1,53\text{E-}03$$

SIL capability: SIL1³ for single use

The average probability of the system to fail with an over voltage condition, for both safety functions (normally energized and normally de-energized), is, see section 5.2:

$$\text{PFD}_{\text{AVG_OC_Sys}}(\text{Tproof} = 1 \text{ year}) = 9,36\text{E-}14$$

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 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.

A user of the switching power supply types PSD1206 and PSD1210 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 along with all assumptions.

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

³ With a hardware fault tolerance of 1 SIL2 capability is possible. Assuming a common cause factor of 5% the $\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 8,09\text{E-}05$.



Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved.....	6
2.3 Standards / Literature used.....	6
2.4 Reference documents.....	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida</i>	7
3 Description of the analyzed module	8
3.1 System overview.....	8
4 Failure Modes, Effects, and Diagnostics Analysis	9
4.1 Description of the failure categories.....	9
4.2 Methodology – FMEDA, Failure rates.....	10
4.2.1 FMEDA.....	10
4.2.2 Failure rates	10
4.2.3 Assumptions.....	10
5 Results of the assessment.....	12
5.1 Switching power supply types PSD1206 and PSD1210	13
6 Terms and Definitions	15
7 Status of the document.....	16
7.1 Liability.....	16
7.2 Releases	16
Appendix 1: Possible proof tests to detect dangerous undetected faults.....	17
Appendix 2: Impact of lifetime of critical components on the failure rate	17

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

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

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the switching power supply types PSD1206 and PSD1210.

The information in this report can be used to evaluate whether a system, including the switching power supply types PSD1206 and PSD1210 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.



2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

G.M. International s.r.l Manufacturer of the switching power supply types PSD1206 and PSD1210.

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

G.M. International s.r.l contracted *exida* in January 2007 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components
[N7]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment; operating conditions

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	DTS0192.pdf	Datasheet
[D2]	DTS0193.pdf	Datasheet
[D3]	SCD073.pdf	Circuit diagram "PSD1206 – PSD1210 Switching Power Supply" SCD073 Rev. 3
[D4]	SCD074.pdf	Circuit diagram "PSD1206 – PSD1210 A309 Module for Switching Power Supply" SCD074 Rev. 0
[D5]	PRL152.pdf	Parts list "PSD1206 Switching Power Supply – Connection Board" PRL152 Rev. 2
[D6]	PRL153.pdf	Parts list "PSD1206 Switching Power Supply – Output Board" PRL153 Rev. 3
[D7]	PRL154.pdf	Parts list "PSD1210 Switching Power Supply – Connection Board" PRL154 Rev. 2
[D8]	PRL155.pdf	Parts list "PSD1210 Switching Power Supply – Output Board" PRL155 Rev. 3
[D9]	CRR053.pdf	Document "SIL Analysis CRR053 – Power Supply PSD1206 and PSD1210" CRR053 Rev. 0
[D10]	FMEDA PSD1210_Diagnostic.xls of 01.06.07	
[D11]	FMEDA PSD1210_Overvoltage.xls of 01.06.07	
[D12]	FMEDA PSD1210_Supply.xls of 01.06.07	
[D13]	FMEDA_PSD1210_Crowbar.xls of 12.06.07	

2.4.2 Documentation generated by exida

[R1]	FMEDA PSD1210_Supply_Review_SA.xls of 20.06.07
[R2]	FMEDA PSD1210_Overvoltage_Review_SA.xls of 20.06.07
[R3]	FMEDA_PSD1210_Crowbar_Review_SA.xls of 22.06.07
[R4]	FMEDA PSD1210_Diagnostic_Review_SA.xls of 20.06.07
[R5]	Summary IEC 61508 values V4.xls of 20.07.07

3 Description of the analyzed module

3.1 System overview

The Switching Power Supply Types PSD1206 and PSD1210 are DIN-Rail power supplies to supply process control in Zone 2 Hazardous Area equipments; they provide isolation between input - output - ground (2000 V). Figure 1 gives an overview of the Switching Power Supply Types PSD1206 and PSD1210.

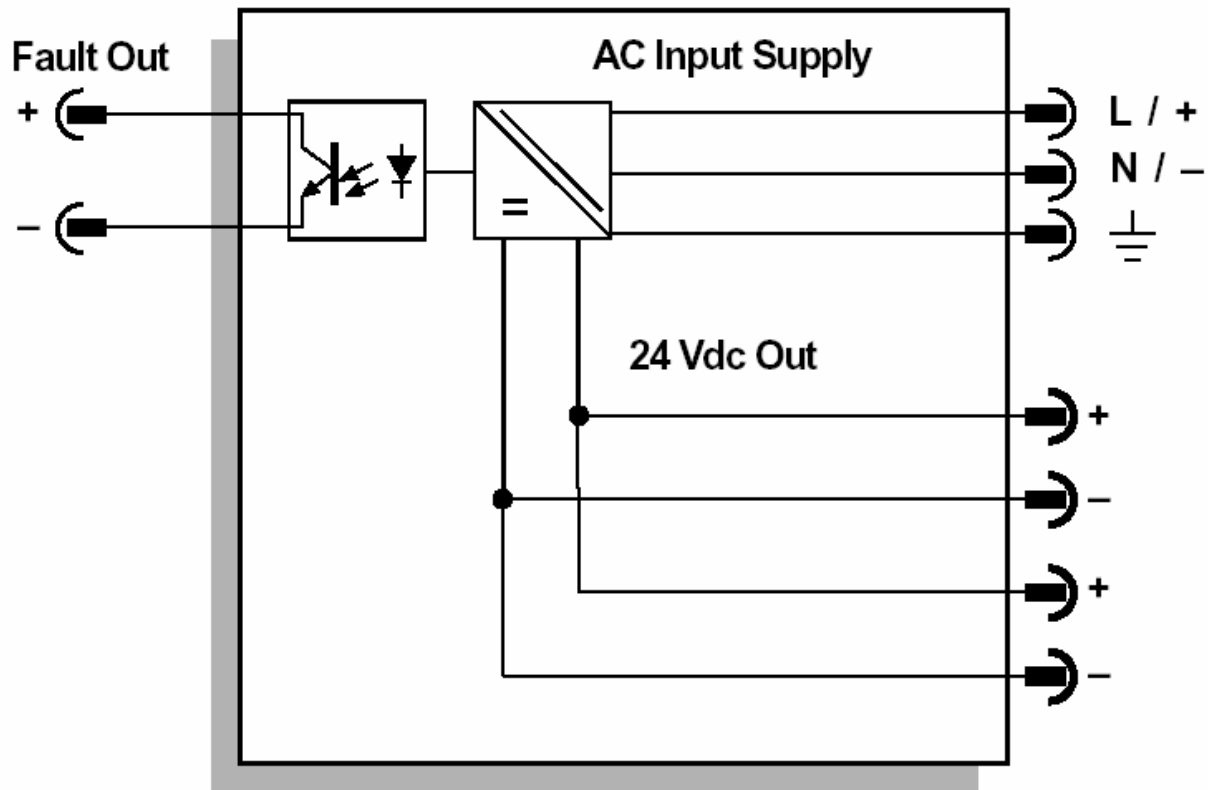


Figure 1: Overview

The Switching Power Supply Types PSD1206 and PSD1210 are considered to be Type A subsystems with a hardware fault tolerance of 0.

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by G.M. International s.r.l and reviewed by *exida*. The results are documented in [D10]to [D13] and [R4] to [R5].

4.1 Description of the failure categories

In order to judge the failure behavior of the Switching Power Supply Types PSD1206 and PSD1210, the following definitions for the failure of the product were considered.

General

Fail high	A fail high failure (H) is defined as a failure that leads to an over voltage condition ($> 30V$).
Fail low	A fail low failure (L) is defined as a failure that leads to an under voltage condition ($< 2V$).
No Effect	A no effect failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.
Annunciation	An annunciation failure (A) is defined as a failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). For the calculation of the 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.
No part	"no part" (-) means that this component is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

Normally energized loads

Fail-Safe State	The fail-safe state is defined as the output being between 20 V and 30 V (load current up to 80% of rated) or lower than 2 V.
Fail Safe	A safe failure (S) is defined as a failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	A dangerous failure (D) is defined as a failure that leads to an output higher than 30V or between 2V and 20V.

Normally de-energized loads

Fail-Safe State	The fail-safe state is defined as the output being between 20 V and 30 V (load current up to 80% of rated).
Fail Safe	A safe failure (S) is defined as a failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	A dangerous failure (D) is defined as a failure that leads to an output higher than 30V or lower than 20V.

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

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are from the Siemens SN 29500 electronic component database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 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 tests 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 the design analyzed.
- The device is operated in the low demand mode of operation.
- The time to restoration after a safe failure is 8 hours.
- 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 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 Results of the assessment

exida and G.M. International s.r.l performed the FMEDA. For the calculation of the Safe Failure Fraction (SFF) the following must be noted:

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

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

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

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

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

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

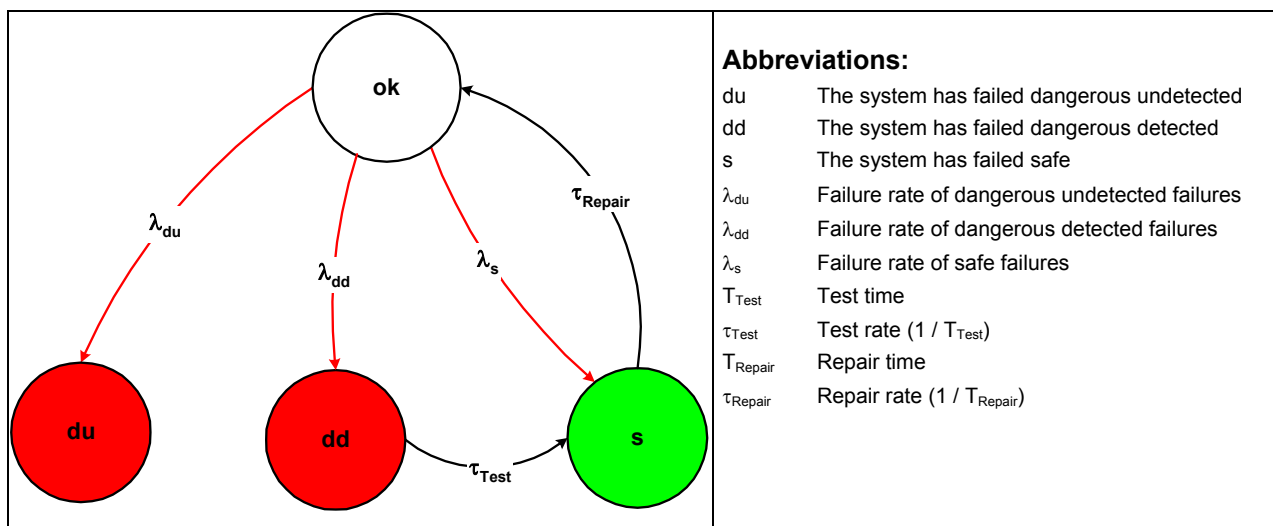


Figure 2: Markov model for a 1oo1D structure

5.1 Switching power supply types PSD1206 and PSD1210

The FMEDA carried out on the Switching Power Supply Types PSD1206 and PSD1210 leads under the assumptions described in section 4.2.3 to the following failure rates:

	λ_{safe}^4	$\lambda_{\text{dangerous}}$	λ_{high}	λ_{low}	$\lambda_{\text{no effect}}$	$\lambda_{\text{annunciation}}$	$\lambda_{\text{not part}}$
Power supply	33 FIT	132 FIT	21 FIT	175 FIT	177 FIT	0 FIT	41 FIT
Crowbar 1	0 FIT	0 FIT	0 FIT	18 FIT	16 FIT	24 FIT	0 FIT
Crowbar 2	0 FIT	0 FIT	0 FIT	18 FIT	16 FIT	24 FIT	0 FIT
Over voltage protection	0 FIT	2 FIT	0 FIT	4 FIT	5 FIT	11 FIT	0 FIT
Fault output	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	133 FIT

These failure rates lead to the following overall failure rates for the two considered safety functions “normally energized load” and “normally de-energized load”:

SF1: Normally energized load

$$\lambda_{\text{SAFE_NE}} = \lambda_{\text{safe_PS}} + \lambda_{\text{low_PS}} + \lambda_{\text{safe_CB1}} + \lambda_{\text{safe_CB2}} + \lambda_{\text{low_CB1}} + \lambda_{\text{low_CB2}} + \lambda_{\text{safe_OP}} + \lambda_{\text{low_OP}} + 99\% * (\lambda_{\text{high_PS}} + \lambda_{\text{annunciation_CB1}} + \lambda_{\text{annunciation_CB2}} + \lambda_{\text{annunciation_OP}})$$

$$\lambda_{\text{DANGEROUS_NE}} = \lambda_{\text{dangerous_PS}} + \lambda_{\text{dangerous_OP}} + 1\% * (\lambda_{\text{high_PS}} + \lambda_{\text{annunciation_CB1}} + \lambda_{\text{annunciation_CB2}} + \lambda_{\text{annunciation_OP}})$$

$$\lambda_{\text{SAFE_NE}} = 542,2 \text{ FIT}$$

$$\lambda_{\text{DANGEROUS_NE}} = 134,8 \text{ FIT}$$

$$\lambda_{\text{total}} = 677 \text{ FIT}$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = 1 / (\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 134 \text{ years}$$

$$\text{SFF} = 80,09\%$$

$$\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 5,90\text{E-}04$$

SF2: Normally de-energized load

$$\lambda_{\text{SAFE_NE}} = \lambda_{\text{safe_PS}} + \lambda_{\text{safe_CB1}} + \lambda_{\text{safe_CB2}} + \lambda_{\text{safe_OP}} + 99\% * (\lambda_{\text{high_PS}} + \lambda_{\text{annunciation_CB1}} + \lambda_{\text{annunciation_CB2}} + \lambda_{\text{annunciation_OP}})$$

$$\lambda_{\text{DANGEROUS_NE}} = \lambda_{\text{dangerous_PS}} + \lambda_{\text{low_PS}} + \lambda_{\text{low_CB1}} + \lambda_{\text{low_CB2}} + \lambda_{\text{dangerous_OP}} + \lambda_{\text{low_OP}} + 1\% * (\lambda_{\text{high_PS}} + \lambda_{\text{annunciation_CB1}} + \lambda_{\text{annunciation_CB2}} + \lambda_{\text{annunciation_OP}})$$

$$\lambda_{\text{SAFE_NE}} = 327,2 \text{ FIT}$$

$$\lambda_{\text{DANGEROUS_NE}} = 349,8 \text{ FIT}$$

$$\lambda_{\text{total}} = 677 \text{ FIT}$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = 1 / (\lambda_{\text{total}} + \lambda_{\text{not part}}) + 8 \text{ h} = 134 \text{ years}$$

$$\text{SFF} = 48,33\%$$

$$\text{PFD}_{\text{AVG}}(\text{Tproof} = 1 \text{ year}) = 1,53\text{E-}03$$

⁴ Note that the safe category includes failures that do not cause a spurious trip.

5.2 Example PFD_{AVG} calculation for over-voltage condition

One way to calculate the probability that the Switching Power Supply Types PSD1206 and PSD1210 fail with an over voltage condition is by using the fault tree as presented in Figure 3. 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.

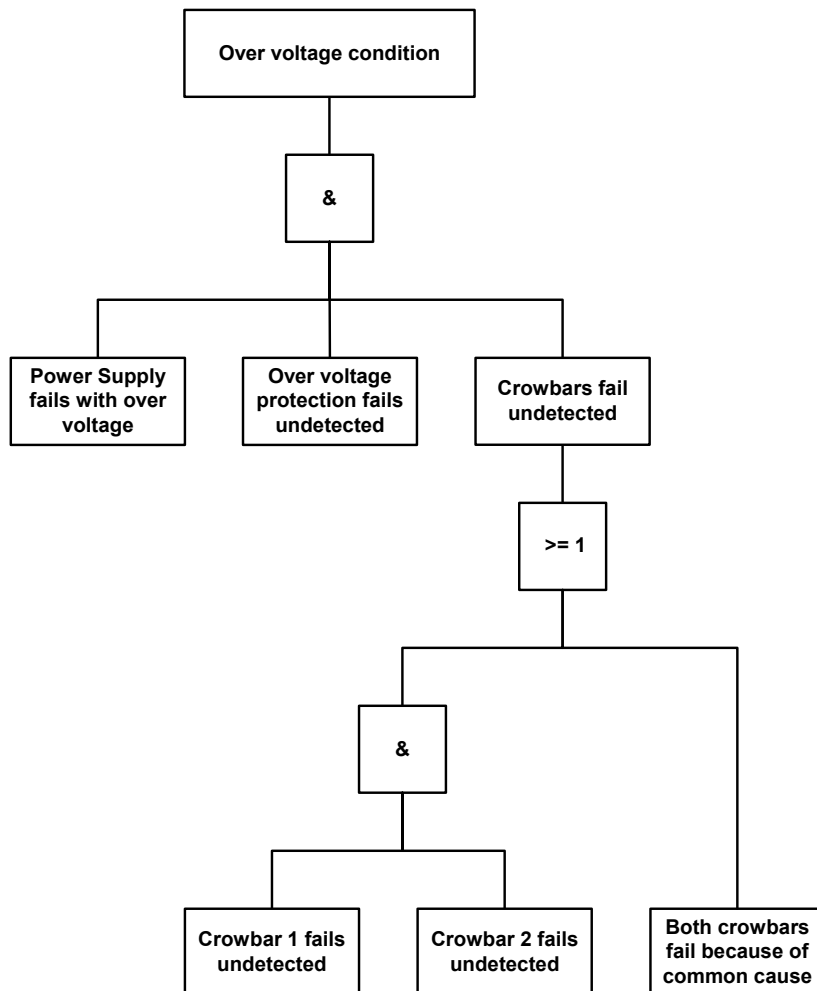


Figure 3: Fault tree for the probability to fail with an over voltage condition

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

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

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

$$PFD_{OC_PS}(T_{proof} = 1 \text{ year}) = 1,84E-04$$

$$PFD_{OP}(T_{proof} = 1 \text{ year}) = 9,64E-05$$

$$PFD_{CB1}(T_{proof} = 1 \text{ year}) = PFD_{CB2}(T_{proof} = 1 \text{ year}) = 2,10E-04$$

$$PFD_{CB12}(T_{proof} = 1 \text{ year}) = 1,05E-05$$

$$PFD_{CB}(T_{proof} = 1 \text{ year}) = 1,06E-05$$

$$PFD_{AVG_OC_Sys}(T_{proof} = 1 \text{ year}) = 9,36E-14$$

6 Terms and Definitions

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

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version: V1

Revision: R0

Version History: V0, R1: Initial version; June 27, 2007

V1, R0: Review comments incorporated; July 20, 2007

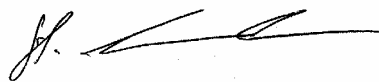
Authors: Stephan Aschenbrenner

Review: V0, R1: Basilio Abbamonte (G.M. International); July 2, 2007

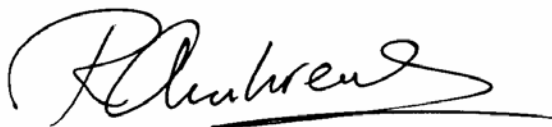
V0, R1: Rachel Amkreutz (*exida*); July 17, 2007

Release status: Released to G.M. International s.r.l

7.3 Release Signatures

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

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

A handwritten signature in black ink, appearing to be "Rachel Amkreutz".

Rachel Amkreutz, Safety Engineer

Appendix 1: Proof tests to detect dangerous undetected faults

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 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
- Out of normal voltage signalling
- Over voltage limiting
- Paralleling diode operation
- Current sharing capability

Test Setup – Required equipment

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 model PSD1210 or 150 W variable power resistor, adjustable between 4 and 25 Ω , with a current capability of 6 A for testing model PSD1206.
- 10 k Ω trimmer.

Test of single Power Supply or individual unit of 1oo2 configuration

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.

1. <u>Current capability</u>
1.1. Set the load resistor to 25 Ω for minimum loading.
1.2. Connect the mains power connections and apply power to the test circuit.
1.3. Adjust load current to 10 A for PSD1210 or 6 A for PSD 1206; wait 30 minutes for warm-up and stabilization.
1.4. Check voltage at output terminals to be within the limits (23.6 to 24.4 VDC) and load current to be as above.
2. <u>Crowbar A</u>
2.1. Connect a jumper between test terminals B1 and B2 to disable over voltage protection.
2.2. Connect a jumper between test terminals S2 to disable crowbar B.
2.3. Turn the trimmer to have the maximum resistance.
2.4. Connect the 10 k Ω trimmer between terminals C1 and C2.

2.5. Monitor output voltage that should be above 24 V nominal at full load, slowly turn the trimmer to decrease its resistance and observe the corresponding output voltage that should increase.
2.6. 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 and 29.0 V.
2.7. Shutdown the power supply to reset the crowbar.
2.8. Turn the trimmer fully to have the maximum resistance.
2.9. Disconnect the jumper from test terminals S2
3. <u>Crowbar B</u>
3.1. Switch on the power supply.
3.2. Connect a jumper between test terminals S1 to disable crowbar A.
3.3. Monitor output voltage that should be above 24 V nominal at full load, slowly turn the trimmer to decrease its resistance and observe the corresponding output voltage that should increase.
3.4. 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 and 29.0V.
3.5. Shutdown the power supply to reset the crowbar.
3.6. Disconnect the trimmer from terminals C1 and C2.
3.7. Disconnect the jumper from test terminals S2.
3.8. Disconnect the jumper between test terminals B1 and B2 to enable the over voltage protection.

Tests required when the unit is used as subsystem of a 1oo2 system

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.

1. <u>Paralleling Diode test</u>
1.1. Shutdown the other Power Supply unit.
1.2. Adjust load current to 10 A for PSD1210 or 6 A for PSD 1206; wait 30 minutes for warm-up and stabilization.
1.3. Connect a voltmeter, scale 0 to 20 VDC across the paralleling diode terminals D2 (+) and D1 (-) and check that voltage drop is within limits (0.5 to 0.7 V).
1.4. Switch on the other power supply.
1.5. Switch off the supply under test.
1.6. Check that the supply unit under test has zero voltage output and also check voltage across paralleling diode to be within limits (-22 V to -26 V).

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime⁵ of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

Table 2 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 2: Useful lifetime of components with reduced useful lifetime contributing to λ_{du}

Type	Name	Useful life at 40°C
Capacitor (electrolytic) - Aluminum electrolytic, non solid electrolyte	C5, C20M	Appr. 90 000 Hours ⁶

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

⁵ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

⁶ The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.