



## **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 V0, Revision R1, June 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 belong to the considered switching power supply types PSD1206 and PSD1210.

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.

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

The switching power supply types PSD1206 and PSD1210 are considered to be Type A<sup>1</sup> 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: SIL2<sup>2</sup>

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

<sup>2</sup> 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

$$\lambda_{\text{SAFE\_NE}} = 327,2 \text{ FIT}$$

$$\lambda_{\text{DANGEROUS\_NE}} = 349,8 \text{ FIT}$$

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

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

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

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

SIL capability: SIL1<sup>3</sup>

The average probability of the system to fail with an over voltage condition is:

$$\text{PFD}_{\text{AVG\_OC\_Sys}}(\text{Tproof} = 1 \text{ year}) = 2,34\text{E-}14$$

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.

---

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