FMEDA and Proven-in-use Assessment

Project:
Digital Output Modules D104* and PSD1001(C)

Customer:

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

Contract No.: GM 04/10-26
Report No.: GM 04/10-26 R002
Version V1, Revision R1.0, October 2005
Stephan Aschenbrenner

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

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Digital Output Modules D104* and PSD1001(C) with software versions PRG007A and PRG008A. Table 1 gives an overview of the different versions that belong to the considered devices.

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[1]	Mode of operation
D1040	22 mA at 13.2 V (per channel)	“bus power” / “loop power”
D1042	22 mA at 14.5 V (per channel)	“bus power” / “loop power”
D1043	22 mA at 10.6 V (per channel)	“bus power” / “loop power”
PSD1001	20 mA at 15 V (per channel)	“loop power”
PSD1001C	100 mA at 13.5 V / 150 mA at 10 V	“loop power”

Failure rates used in this analysis are 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 modules 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 Digital Output Modules D104* and PSD1001(C) are considered to be Type B[2] components with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the Digital Output Modules D104* and PSD1001(C) are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% - < 90%.

The proven-in-use investigation was based on field return data collected and analyzed by G.M. International s.r.l.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.2 the devices are suitable to be used, as a single device, for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

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

[1] Multiple channels on a redundant board shall not be used to increase the hardware fault tolerance needed for a higher SIL as they contain common components.

[2] Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 2: Summary – Failure rates, bus powered mode

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	**SFF**
0 FIT	334 FIT	1 FIT	83 FIT	80%

Table 3: Summary – PFD$_{AVG}$ values, bus powered mode

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD$_{AVG}$ = 3,64E-04	**PFD$_{AVG}$ = 1,82E-03**	**PFD$_{AVG}$ = 3,63E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

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

The functional assessment has shown that the Digital Output Modules D104* and PSD1001(C) have a PFD$_{AVG}$ within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of more than 80%. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to “prior-use” of IEC 61511-1 they can be used as a single device for SIL 2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the Digital Output Modules D104* and PSD1001(C) 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.

The failure rates are valid for the useful life of the Digital Output Modules D104* and PSD1001(C), which is estimated to be between 8 and 12 years (see Appendix 3).

The Digital Output Modules D104* and PSD1001(C), when configured in loop powered mode can be used for SIL 3 safety applications. The following tables show how the above stated requirements are fulfilled.

Table 4: Summary – Failure rates, loop powered mode[3]

λ_{safe}	$\lambda_{dangerous}$	**SFF**	**PFD$_{AVG}$**
418 FIT	0 FIT	100%	0,00E+00

[3] This requires the connection as indicated in Figure 2 or Figure 3 and Figure 4.

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}).

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

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

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of 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.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, 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 is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 2.

This document shall describe the results of the FMEDAs carried out on the Digital Output Modules D104* and PSD1001(C) with software versions PRG007A and PRG008A.

It shall be assessed whether these devices meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* 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 Digital Output Modules D104* and PSD1001(C).
exida.com	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

G.M. International s.r.l contracted *exida.com* in November 2004 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	IEC 61511-1 First Edition 2003-01	Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
N3	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N4	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N5	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
N6	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	SCD017_R3.sch	Circuit diagram “D1040, D1042, D1043, PSD1001 Digital Out DIN Rail” revision 3
[D2]	PRL061.PDF	Part List D1040Q revision 4
[D3]	PRL064.PDF	Part List PSD1001 revision 4
[D4]	PRL066.PDF	Part List D1042Q revision 3
[D5]	PRL067.PDF	Part List D1043Q revision 3
[D6]	PRL133.PDF	Part List PSD1001C revision 0
[D7]	TRP032_r0.doc, TRP032 for EXIDA.pdf and TRP032.pdf	FMEDA report and fault insertion tests including hardware revision history
[D8]	PRG007A.asm	Software source code
[D9]	PRG008A.asm	Software source code
[D10]	D1040_E.pdf	Data sheet for D104*
[D11]	PSD1001_E.pdf	Data sheet for PSD1001
[D12]	PSD1001C_E.pdf	Data sheet for PSD1001C
[D13]	Quality_Manual2000rev3.doc	Quality manual Rev 3 2003.10.01
[D14]	Folder “Quality_Manual_Procedure”	Quality procedures
[D15]	MQ_Annex_D.doc	Modification procedure as part of the quality manual
[D16]	Email dated 18.10.05 and SPP007A_r0.pdf and SPP008A_r0.pdf	Revision history SW
[D17]	INC002_r0.pdf	Statistics of field-feed-back tracking; sold and returned devices
[D18]	Reparation_Report_Sample.pdf	Example of database repair entry
[D19]	SPP007A_r0.pdf	Software project plan SPP007A
[D20]	SPP008A_r0.pdf	Software project plan SPP008A
[D21]	LIST OF APPLICATIONS DOR D104.doc Reference List GM.xls	List of application examples

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V6 D104x Bus powered V1 R1.2.xls of 29.04.05
[R2]	Minutes of Meeting PIU.doc of 22.04.05
[R3]	Field data evaluation.xls of 22.04.05 (Field data evaluation of operating hours, sold devices and returned devices)

3 Description of the analyzed modules

The D104* series are a quad channel Din Rail Digital Output Modules enabling a Safe Area contact or logic level or drive signal to control a device in Hazardous Area; it provides 3 port isolation (input/output/supply). Typical applications include driving signaling LEDs, providing visual or audible alarms to alert a plant operator or driving a solenoid valve or other process control devices. The device can also be used as a controllable supply to power measuring or process control equipments in Hazardous Area. Output channels can be paralleled if more power is required: 2 channels in parallel are still suitable for Gas Group II C. Four basic models meet a large number of applications: it is possible to obtain 16 different combinations of Safety Parameters and Driving Currents.

The PSD1001 is a quad channel Din Rail Power Supply to drive measuring, process control equipments in Hazardous Area; it provides isolation between input and output (1.5 KV). Typical application is to drive 4-20 mA 2 wire transmitter with local indication (no repetition of current in Safe Area). Output channels can be paralleled if more power is required.

The PSD1001C is a single channel Din Rail Power Supply to drive measuring, process control equipments in IIB Group Hazardous Area; it provides isolation between input and output (1.5 KV). Typical application is to drive high power devices, transmitter or other equipment with 13 V, 100 mA supply capability.

The Digital Output Modules D104* and PSD1001(C) are considered to be Type B components with a hardware fault tolerance of 0.

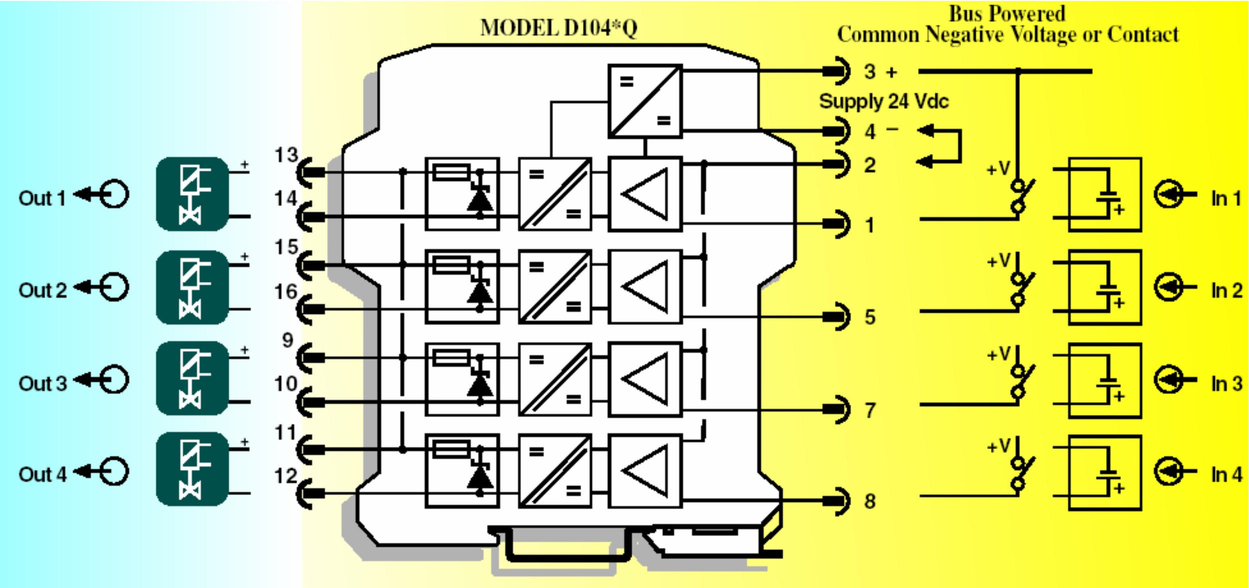


Figure 1: Block diagram of D104* in bus powered configuration

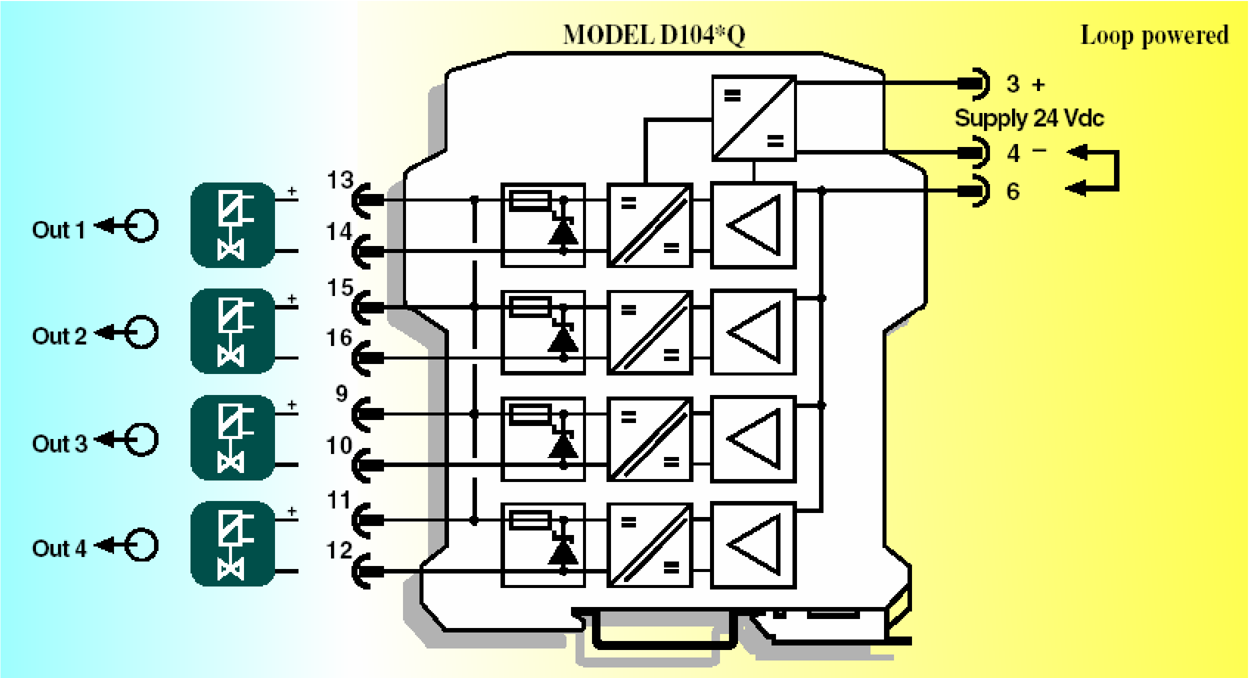


Figure 2: Block diagram of D104* in loop powered configuration

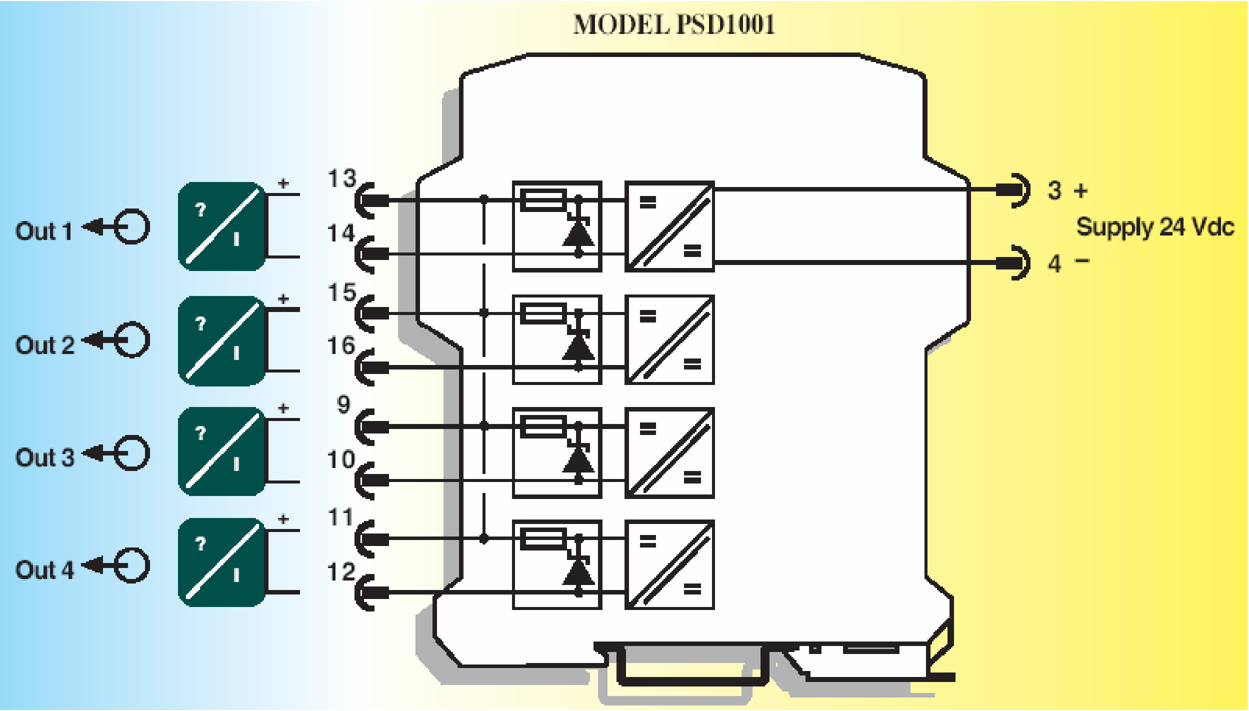


Figure 3: Block diagram of PSD1001 loop powered

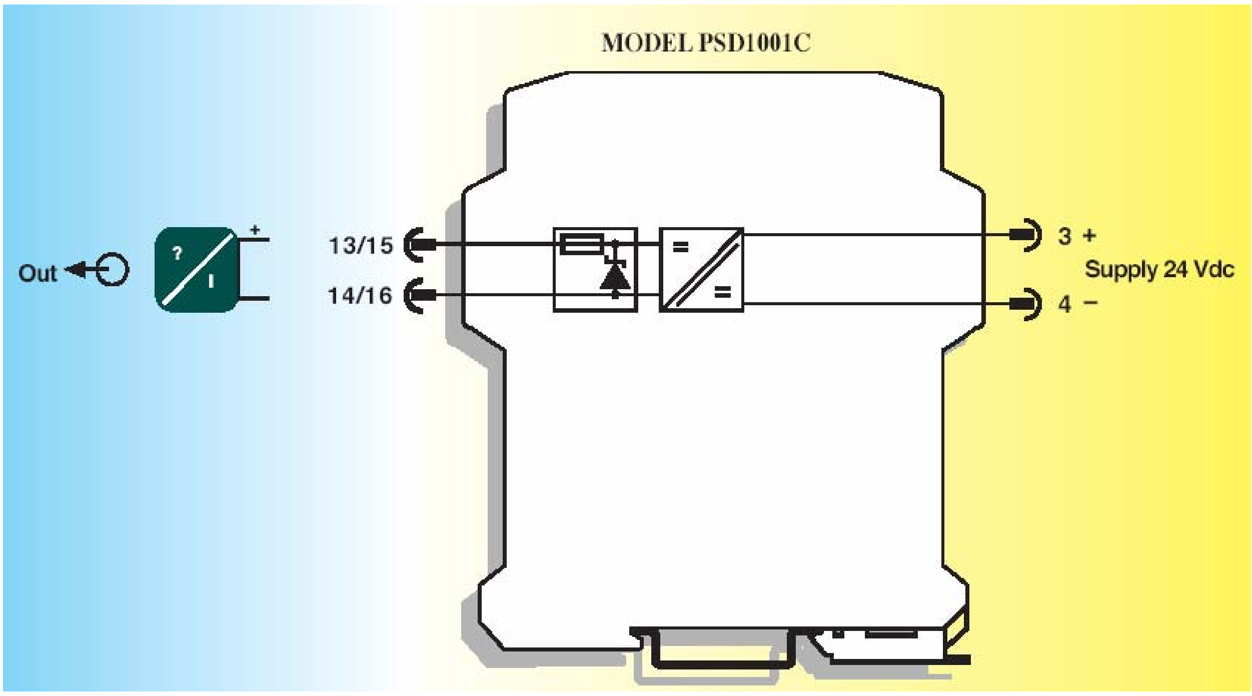


Figure 4: Block diagram of PSD1001C loop powered

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by G.M. International s.r.I and reviewed by *exida.com*. The results are documented in [D7] and [R1]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see [D7]). This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the Digital Output Modules D104* and PSD1001(C), the following definitions for the failure of the product were considered.

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

Fail Safe
Failure that causes the output to go to the defined fail-safe state.

Fail Dangerous
Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output power more than 10% of the actual value.

Annunciation Undetected
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) and that is not detected by internal diagnostics. For the calculation of the SFF it is treated like a safe undetected failure.

Fail No Effect
Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output power not more than 10% of the actual value. For the calculation of the SFF it is treated like a safe undetected failure.

Not part
Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The “no effect” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the “no effect” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension 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.com* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. 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 FMEDA:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The repair time after a safe failure is 8 hours.
- 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 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- All modules are operated in the low demand mode of operation.
- The safety function is carried out via 1 input and 1 output channel.
- External power supply failure rates are not included.
- 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.

4.2.4 Critical Points of Failure

The analysis has shown that no components of the loop powered modules can be found where potentially dangerous failures exist. All component failures have either no effect on the safety function or can only lead to the defined fail-safe state. A possible short-circuit on the printed circuit board between different channels is also not a problem as all channels are connected in parallel anyway when used in loop powered mode.

5 Results of the assessment

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

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

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

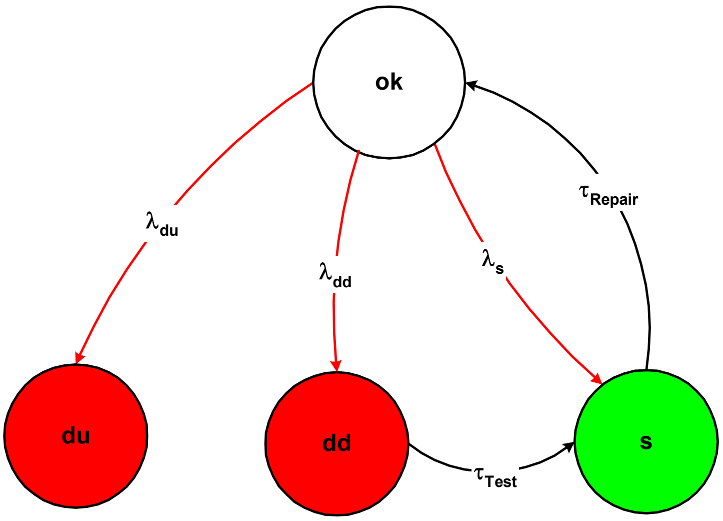
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$

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

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 Microsoft® Excel 2000 based FMEDA tool of *exida.com* as a simulation tool. The results are documented in the following sections.



Abbreviations:

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

Figure 5: Markov model for a 1oo1D structure

5.1 Digital Output Modules D104* and PSD1001(C) – Bus powered mode

The FMEDA carried out on the Digital Output Modules D104* and PSD1001(C) leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,96E-07 1/h

λ_{dd} = 1,49E-09 1/h

λ_{du} = 8,32E-08 1/h

$\lambda_{annunciation}$ = 2,40E-09 1/h

$\lambda_{no\ effect}$ = 1,35E-07 1/h

λ_{total} = 4,18E-07 1/h

$\lambda_{not\ part}$ = 4,26E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 248 years

Under the assumptions described in section 4.2.4 the following tables show the failure rates according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	**SFF**
0 FIT	334 FIT	1 FIT	83 FIT	80,12%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 3,64E-04	**PFD_{AVG} = 1,82E-03**	**PFD_{AVG} = 3,63E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

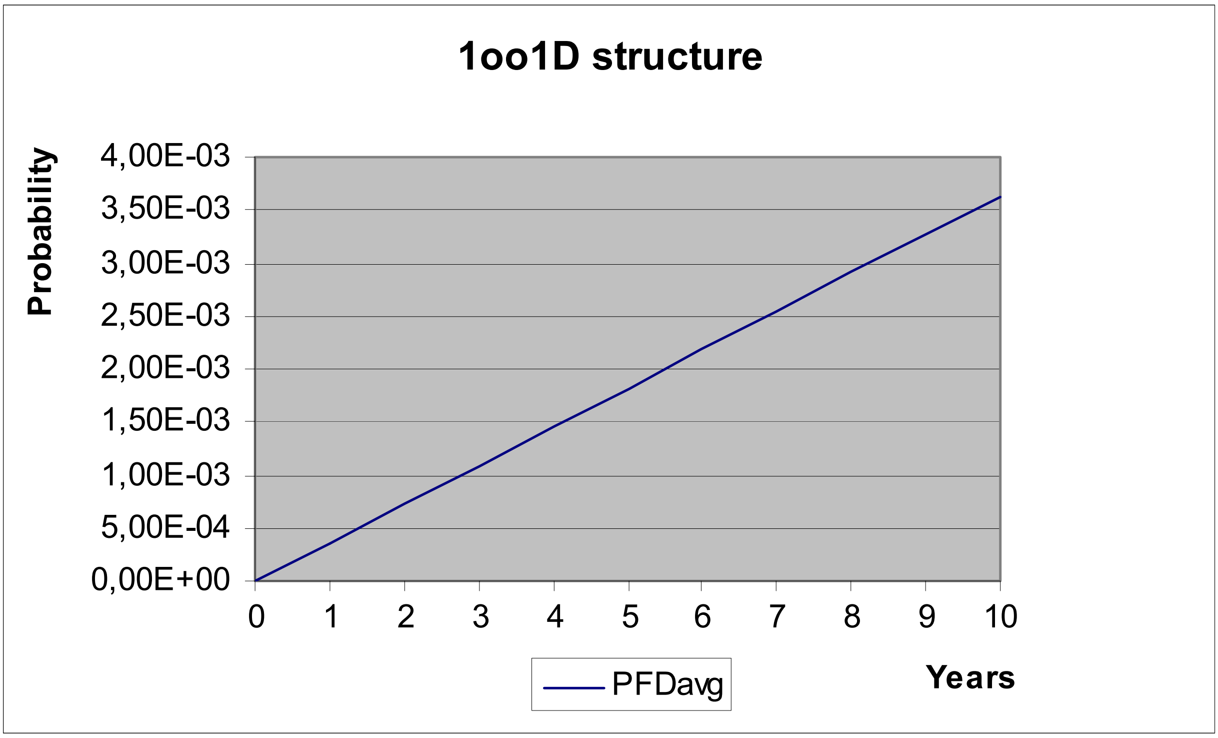


Figure 6: $PFD_{AVG}(t)$

5.2 Loop powered modules

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.

The Digital Output Modules D104* and PSD1001(C), when configured in loop powered mode can be used for SIL 3 safety applications.

λ_{su} = 2,81E-07 1/h

$\lambda_{no\ effect}$ = 1,37E-07 1/h

The following table shows how the above stated requirements are fulfilled.

Table 5: Summary – Loop powered mode[4]

λ_{safe}	$\lambda_{dangerous}$	SFF	PFD_{AVG}
418 FIT	0 FIT	100%	0,00E+00

[4] This requires the connection as indicated in Figure 2 or Figure 3 and Figure 4.

6 Proven-in-use Assessment

6.1 Definition of the term “Proven-in-use” according to IEC 61508

Reference: IEC 61508-7; B.5.4

Aim: To use field experience from different applications to prove that the safety-related system will work according to its specification.

Description: Use of components or subsystems, which have been shown by experience to have no, or only unimportant, faults when used, essentially unchanged, over a sufficient period of time in numerous different applications.

For proven by use to apply, the following requirements must have been fulfilled:

- unchanged specification;
- 10 systems in different applications;
- 10^5 operating hours and at least 1 year of service history.

The proof is given through documentation of the vendor and/or operating company. This documentation must contain at least the:

- exact designation of the system and its component, including version control for hardware;
- users and time of application;
- operating hours;
- procedures for the selection of the systems and applications procured to the proof;
- procedures for fault detection and fault registration as well as fault removal.

6.2 “Prior-use” requirements according to IEC 61511-1

According to IEC 61511-1 First Edition 2003-01 section 11.4.4 for all subsystems (e.g., sensor, final elements and non-PE logic solvers) except PE logic solvers the minimum fault tolerance specified in Table 6 of this standard may be reduced by one if the devices under consideration comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3)
- the device allows adjustment of process-related parameters only, e.g., measuring range, upscale or downscale failure direction, etc.;
- the adjustment of the process-related parameters of the device is protected, e.g., jumper, password;
- the function has a SIL requirement less than 4.

Table 6 of IEC 61511-1 First Edition 2003-01
(Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers):

SIL	Minimum Hardware Fault Tolerance	
	Does not meet 11.4.4 requirements	Meets 11.4.4 requirements
1	0	0
2	1	0
3	2	1
4	Special requirements apply - See IEC 61508	

This means that 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 a SFF of 60% to < 90%[5].

The assessment of the Digital Output Modules D104* and PSD1001(C) has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

Requirement	**Argumentation**[6]
See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 4 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail[7] is very low (no returned devices so far). 2. G.M. International s.r.l is ISO 9001 certified with appropriate quality management and configuration management system. See [D13] to [D18]. The assessed sub-systems are clearly identified and specified. The field feedback tracking database of G.M. International s.r.l together with the explanations given in [D17] to [D21] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience. The following operating experience exist: More than 41.000.000 operating hours This is considered to be sufficient taking into account the low complexity of the sub-systems and the use in SIL 2 safety functions only). 3. 11.5.2 is under the responsibility of the user / manufacturer –> no argumentation. 11.5.3 see bullet items before. 4. N/A 5. Under the responsibility of the user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D21].
Adjustment of process-related parameters only	There are no process-related parameters which can be adjusted.
Adjustment of process-related parameters is protected	N/A
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Digital Output Modules D104* and PSD1001(C) with a SFF of 60% - < 90% and a HFT = 0 can considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

[5] IEC 61511-1 First Edition 2003-01 explicitly says “…provided that the dominant failure mode is to the safe state or dangerous failures are detected…”.

[6] The numbering is based on the requirements detailed in appendix 1.

[7] The probability of failure is the percentage of all returned devices with relevant repair reasons to all sold devices.

7 Terms and Definitions

FIT	Failure In Time (1x10^{-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 one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.
T[Proof]	Proof Test Interval

8 Status of the document

8.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* 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.

8.2 Releases

Version:	V1	
Revision:	R1.0	
Version History:	V0, R1.0:	Initial version, May 10, 2005
	V1, R1.0:	Released version after review, October 24, 2005
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com); May 16, 2005
	V0, R1.0:	Glisente Landrini (G.M. International s.r.l); July 28, 2005
Release status:	Released to G.M. International s.r.l	

8.3 Release Signatures

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

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

Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01

Appendix 1.1 Section 11.5.3 of IEC 61511-1 First Edition 2003-01

(Requirements for the selection of components and subsystems based on prior use)

1. An assessment shall provide appropriate evidence that the components and sub-systems are suitable for use in the safety instrumented system.

2. The evidence of suitability shall include the following:

   - consideration of the manufacturer's quality, management and configuration management systems;
   - adequate identification and specification of the components or sub-systems;
   - demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;
   - the volume of the operating experience.

Appendix 1.2 Section 11.5.4 of IEC 61511-1 First Edition 2003-01

(Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use)

3. The requirements of 11.5.2 and 11.5.3 apply.

4. Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.

5. For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider:

   - characteristics of input and output signals;
   - modes of use;
   - functions and configurations used;
   - previous use in similar applications and physical environments.

Appendix 1.3 Section 11.5.2 of IEC 61511-1 First Edition 2003-01

(General Requirements)

6. Components and sub-systems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with sub-clauses 11.4 and 11.5.3 to 11.5.6, as appropriate.

7. Components and sub-systems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.

8. The suitability of the selected components and sub-systems shall be demonstrated, through consideration of:

   - manufacturer hardware and embedded software documentation;

   - if applicable, appropriate application language and tool selection (see clause 12.4.4).

9. The components and sub-systems shall be consistent with the SIS safety requirements specifications.

Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test

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

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

Table 6 shows an importance analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 2 and 3 should be considered when writing the safety manual as they contain important safety related information.

Table 6: Importance Analysis of "du" failures

Component	% of total λ_{du}	Detection through
IC2-2	24,04%	100% functional test with monitoring of the output signal
IC5-2	24,04%	100% functional test with monitoring of the output signal
IC4	6,63%	100% functional test with monitoring of the output signal
OT1A (OT1B, OT1C, OT1D)	5,41%	100% functional test with monitoring of the output signal
XT1	3,61%	100% functional test with monitoring of the output signal
TR1A (TR1B, TR1C, TR1D)	3,00%	100% functional test with monitoring of the output signal
IC1	2,88%	100% functional test with monitoring of the output signal
TR8	1,98%	100% functional test with monitoring of the output signal
TR9	1,98%	100% functional test with monitoring of the output signal
R25	0,17%	100% functional test with monitoring of the output signal

Appendix 2: Possible proof tests to detect dangerous undetected faults

A possible proof test could consist of the following steps, as described in Table 7.

Table 7 Steps for Proof Test

Step	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 "du" failures in the Digital Output Modules D104* and PSD1001(C).

Appendix 3: Impact of lifetime of critical components on the failure rate

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their 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).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

The circuits of the Digital Output Modules D104* and PSD1001(C) do not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

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 IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.