Failure Modes, Effects and Diagnostic Analysis

Project:
Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L

Customer:

Hans Turck GmbH & Co. KG
Mühlheim
Germany

Contract No.: TURCK 04/10-20
Report No.: TURCK 04/10-20 R003
Version V1, Revision R1.0, May 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 carried out on the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L. Table 1 describes the two 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 description

Type	Description
IM72-11Ex/L	Only components of one channel mounted
IM72-22Ex/L	Components of both channels mounted

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 $\geq 10^{-4}$ to < 10^{-3} for SIL 3 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-04.

The Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L are considered to be Type A[1] components with a hardware fault tolerance of 0.

For Type A components the SFF has to be 90% to < 99% according to table 2 of IEC 61508-2 for SIL 3 (sub-) systems with a hardware fault tolerance of 0.

Because the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L 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 following table shows how the above stated requirements are fulfilled.

λ_{safe}	$\lambda_{dangerous}$	SFF	PFD_{AVG}
222 FIT	0 FIT[2]	100%	0,00E+00

This means that the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L can be used for all safety applications.

The calculations are based on the assumption that the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L are mounted in an environment that is IP 54 compliant (e.g. housing, control cabinet or control room).

[1] Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

[2] In order to deal with the excluded faults in the quantitative analysis it might be reasonable to consider a dangerous failure rate of 0.1 FIT, leading to a SFF of 99,97% and a PFD_{AVG} of 4,38E-06 for a proof time of 10 years.

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 1.

This document shall describe the results of the hardware assessment carried out on the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L.

It shall be assessed whether the devices meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 3 sub-systems according to IEC 61508. 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 100 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

Werner Turck GmbH & Co. KG	Manufacturer of the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L.
exida.com	Performed the hardware assessment according to option 1 (see section 1).

Werner Turck GmbH & Co. KG contracted *exida.com* in October 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]	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

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	12353000 of 11.01.05	Circuit diagram „IM72-22Ex0“
[D2]	Lackwerke Peter_s1_0100000e_004.pdf	Information about the insulation material used
[D3]	1000x_FR4 Datenblatt.pdf	Information about the base material used
[D4]	07261302.02_.tif	Data sheet for PCBs
[D5]	im72neuex (2).doc	General description of the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V6 IM72-22Ex0 V0 R1.0.xls.xls of 10.03.05

3 Description of the analyzed module

3.1 Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L

The Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L are one or two channel loop powered devices and are used for intrinsically safe applications for solenoid valves or LED warning lamps.

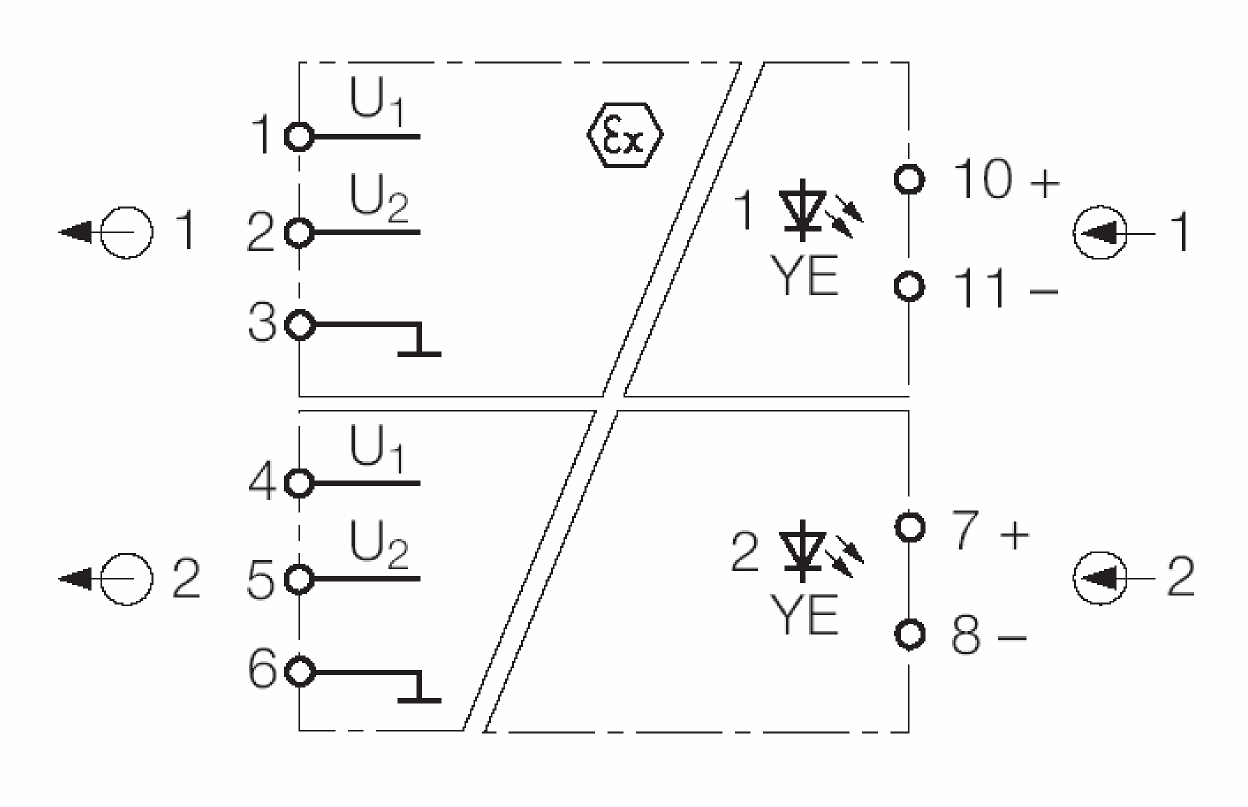


Figure 1: Block diagram of the Solenoid Driver IM72-22Ex/L

The Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L are considered to be Type A components with a hardware fault tolerance of 0.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by *exida.com* and is documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L, 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 module / (sub)system to go to the defined fail-safe state without a demand from the process or has no effect on the safety function.

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).

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.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a 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 are considered to be appropriate for safety integrity level verification calculations. The rates 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 Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- 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 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.

4.2.4 Critical Points of Failure

The analysis has shown that no components of the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L 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. The only possible fault which could have an impact on the safety function is a short-circuit on the printed circuit board.

This possible fault, however, can be excluded according to draft IEC 60947-5-3 A.1.2 if:

- The Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L are mounted in a housing of minimum IP 54
- The base material used is according to IEC 60249, the design and use of the printed board is according to IEC 60326 T3 and the creepage distances and clearances are designed according to IEC 60664-1 (1992) with pollution degree 2 / installation category III, **or**
- The printed side(s) are coated with an insulation material in accordance with IEC 60664-3 (1992)

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category III for a nominal voltage of 24 VDC are given in Table 2.

Table 2: Clearances and creepage distances according to IEC 60661-1

	Clearances (table 2)	Creepage distances (table 4)
Printed wiring material	0,2 mm	0,04 mm

According to Werner Turck GmbH & Co. KG the base material used is FR4 according to NEMA- LI 1-1989 which is identical to IEC 60249, comparative tracking index CTI > 175 according to IEC112 with UL approval. The minimum distance between the two channels on one board is 4,5 mm. This is sufficient according to Table 2.

The insulation material is of the type SL1301N which is based on modified polyurethane resin. SL1301N is UL approved according to UL 94.

5 Results of the assessment

exida.com did the FMEDA.

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:

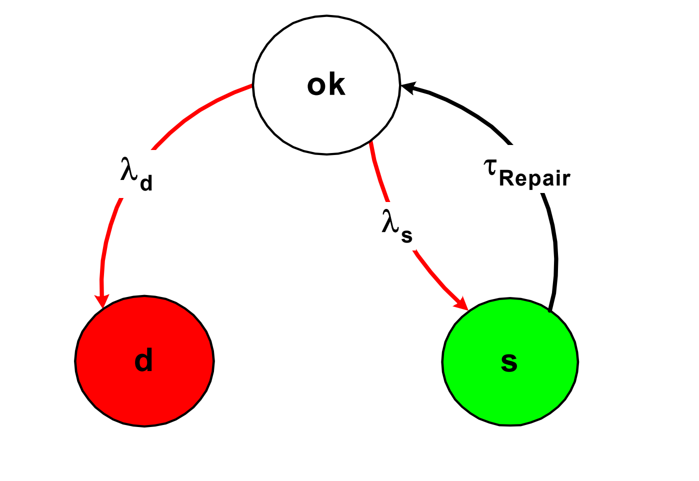
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous}$

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

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 1oo1 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:

d	The system has failed dangerous
s	The system has failed safe
λ_d	Failure rate of dangerous failures
λ_s	Failure rate of safe failures
T_{Repair}	Repair time
τ_{Repair}	Repair rate (1 / T_{Repair})

Figure 2: Markov model for a 1oo1 architecture

5.1 Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L

Because the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L 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 following table shows how the above stated requirements are fulfilled.

λ_{safe}	$\lambda_{dangerous}$	**SFF**	**PFD$_{AVG}$**
222 FIT	0 FIT[3]	100%	0,00E+00

This means that the Solenoid Drivers IM72-11Ex/L and IM72-22Ex/L can be used for all safety applications.

[3] In order to deal with the excluded faults in the quantitative analysis it might be reasonable to consider a dangerous failure rate of 0.1 FIT, leading to a SFF of 99,97% and a PFD$_{AVG}$ of 4,38E-06 for a proof time of 10 years.

6 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, 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 A component	“Non-complex” component (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.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.

7.2 Releases

Version:	V1	
Revision:	R1.0	
Version History:	V0, R1.0:	Initial version; March 10, 2005
	V0, R2.0:	Internal review comments integrated and block diagram added; May 10, 2005
	V1, R1.0:	External review comments integrated; May 20, 2005
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com); March 28, 2005
	V0, R2.0:	Frank Seeler (Werner Turck GmbH & Co. KG); May 19, 2005
Release status:	Released to Werner Turck GmbH & Co. KG	

7.3 Release Signatures

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

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