TURCK

Industrielle Automation

SAFETY MANUAL

VALVE CONTROL MODULES

IM72-11EX/L
IM72-22EX/L

Sense it! Connect it! Bus it! Solve it!

Hans Turck GmbH & Co. KG • Tel. +49 208/4952-0 • Fax +49 208/4952-264

Contents

Hans Turck GmbH & Co. KG • Tel. +49 208/4952-0 • Fax +49 208/4952-264

1 About this safety manual

This safety manual contains instructions on the use of devices in safety instrumented systems (SIS). The consideration of safety-related values is based on IEC 61508. The safety manual describes the values determined for the SIL assessment and is only applicable in conjunction with the attached EXIDA FMEDA report Turck 04/10-20 R003. Read this document carefully before using the device. This will prevent the risk of personal injury or damage to property or equipment. Keep this manual safe during the service life of the device. If the device is passed on, hand over this safety manual as well.

DANGER

Malfunction caused by operating errors

Danger to life if safety function fails!

➤ Observe the instructions contained in this safety manual without fail if the device is to be used in safety-related applications.

1.1 Target groups

This safety manual is designed for use by suitably qualified or trained personnel. It must be read and understood by anyone entrusted with any of the following tasks:

- Unpacking and mounting
- Commissioning
- Testing and maintenance
- Troubleshooting
- Disassembly and disposal

1.2 Explanation of symbols

The following symbols are used in this safety manual:

DANGER

DANGER indicates an immediate hazardous situation that, if not avoided, will result in death or serious injury.

NOTE

NOTE indicates tips, recommendations and important information. The notes contain information, particular operating steps that facilitate work and possibly help to avoid additional work resulting from incorrect procedures.

MANDATORY ACTION

➤ This symbol denotes actions that the user must carry out.

RESULT OF ACTION

➥ This symbol denotes the relevant results of actions and procedures.

1.3 Abbreviations and terms

Definition of terms, see IEC 61508-4

DC	diagnostic coverage
E/E/PE system	electrical/electronic/programmable electronic system
EUC	equipment under control
	dangerous failure
	no effect failure
	no part failure
	safe failure
	safe state
HFT	hardware fault tolerance

	high demand mode	
	low demand mode	
MooN	M out of N channel architecture	
MTBF	mean time between failures	
MTTR	mean time to restoration	
PFD	probability of dangerous failure on demand	
PFD_{AVG}	probability of dangerous failure on demand	
PFH	probability of a dangerous failure per hour	
SFF	safe failure fraction	
SIF	safety instrumented function	Safety function
SIS	safety instrumented system	
SIL	safety integrity level	
	proof test	
	proof test interval	

1.4 Document history

Rev.	Description	Date
1.0.0	First edition	02.04.2015

The German version shall be considered the definitive document. Every care was taken in the production of the translations of this document. If there is any uncertainty in its interpretation, refer to the German version of the safety manual or contact TURCK directly.

NOTE
In all cases use the latest version of this safety manual. Check whether a newer version is available.

2 Notes on devices

2.1 Device variants

This safety manual applies to the following TURCK valve control modules:

IM72-11Ex/L
IM72-22Ex/L

2.2 Scope of delivery

The device is supplied with the SIL registration card.

Hans Turck GmbH & Co. KG • Tel. +49 208/4952-0 • Fax +49 208/4952-264

2.3 Manufacturer and Service

TURCK supports you in your projects – from the initial analysis right through to the commissioning of your application. The TURCK product database offers you several software tools for programming, configuring or commissioning, as well as data sheets and CAD files in many export formats. You can access the Product Database directly via the following address: www.turck.de/products
For further inquiries in Germany contact the Sales and Service Team on:
Sales: +49 208 4952-380
Technical: +49 208 4952-390
For overseas inquiries contact your national TURCK representative.

Hans Turck GmbH & Co. KG
45466 Mülheim an der Ruhr
Germany

3 For your safety

The device is designed according to the latest state-of-the-art technology. Residual hazards, however, still exist. Observe the following warnings and safety regulations in order to prevent danger to persons and property. TURCK accepts no liability for damage caused by failure to observe regulations.

3.1 Intended use

Valve control modules provide an intrinsically safe output signal with a limited voltage and current. This allows connected loads to be operated in the hazardous gas and dust areas. Typical applications include the actuation of Ex i pilot valves, as well as the supply of indicators and transmitters. The devices are actuated by applying the operating voltage. The output values of the two connections U1 and U2 per channel have different no load voltages and are designed to meet the requirements of different valve manufacturers.
These devices also enable the creation of safety-related systems up to and including SIL3 according to IEC 61508 (hardware fault tolerance HFT = 0). The devices must only be used in safety-related systems if all requirements stated in this safety manual and the EXIDA report are strictly observed. The information in the EXIDA report applies when IEC 61508 is used for applications with a low demand mode (device type A for low demand mode). When used in safety systems, the probability of dangerous failure (PFD) for the entire circuit must be determined and given due consideration.

3.2 Obvious misuse

When using dual-channel devices in safety circuits, the second channel must not be used to increase the hardware fault tolerance and thus achieve a higher SIL level.

3.3 SIL registration card

NOTE
With safety-related applications, the SIL registration card enclosed with the device must be filled in completely by the user and returned to TURCK without fail.

3.4 General safety regulations

- It is the responsibility of the user to ensure that the device is used in compliance with the applicable regulations, standards and laws.
- The suitability for specific applications must be assessed by considering the particular overall safety-related system with regard to the requirements of IEC 61508.
- The device must only be carried out by trained and qualified personnel.
- The device must only be commissioned and operated by trained and qualified personnel.
- A function test must be completed prior to initial operation, after repair and replacement, as well as at the stipulated interval T[Proof]
- When the device is in operation, ensure that the power supply is within the specified voltage range.
- Ensure that the plug connections and cables are always in good condition.
- Special application-specific factors such as chemical and physical stresses may cause the premature wear of the devices and must be taken into consideration when planning systems; take special measures to compensate for a lack of experience based values, e.g. through the implementation of shorter test intervals.
- If faults occur in the device that cause a switch to the defined safe state, measures must be taken to maintain the safe state during the further operation of the overall control system.
- TURCK must be notified of dangerous failures immediately.
- A faulty device must be replaced immediately and must not be repaired.
- The device must be replaced immediately if the terminals are faulty or the device has any visible faults.
- Interventions and conversions on the device are not permissible. Repairs must only be carried out by TURCK. Return the device to TURCK for this (see section "Repair").
- Before using the product in safety-related applications, the suitability of the specifications stated in this safety manual for the particular application (e.g. particular branch-specific requirements and practices) must always be checked. In cases of doubt please contact the stated manufacturer's address.

4 Device specific information on safety applications

4.1 Safety function

The output of a channel is switched off if the input voltage is lower than the switch threshold (< 5 V).

4.2 Safe state

The safe state is defined as the state when the output is LOW. In the safe state the output voltage is less than the voltage of the connected valves.

4.3 Functions and operating modes

4.3.1 Output behavior

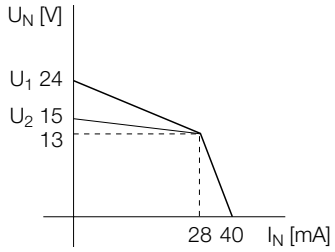

Fig. 1: Output behavior of IM72-11Ex/L and IM72-22Ex/L

4.3.2 Signal change

A signal change at the input causes a signal change at the corresponding output.

- Depending on the input signal, the output is HIGH if the output signal is 19…30 VDC.
- Depending on the input signal, the output is LOW if the output signal is 0…5 VDC.

4.3.3 Fault acknowledgement

Faults do not have to be acknowledged. If the fault is rectified, the device automatically resumes operation.

4.4 Types of faults and failures

Failures must be classified in conjunction with the application into safe (non-hazardous) and unsafe (hazardous) failures. You as the operator are responsible for this.

NOTE

TURCK must be notified immediately of all damage that was caused by a dangerous undetected failure.

4.5 Safety characteristic values

4.5.1 FMEDA assumptions

The safety-related characteristic values were determined based on an FMEDA in accordance with IEC 61508. The FMEDA is based on the following assumptions:

- The failure rates are constant.
- The mechanical wear is not considered.
- The propagation of failures is not relevant.
- The MTTR repair time after a safe failure is 8 hours (replacement of the device).
- The device is operated in low demand mode.
- The failure rates of an external power supply are not considered.
- The failure rates used are the Siemens standards SN 29500 at 40 °C .
- The second channel of a device cannot be used to increase the HFT hardware fault tolerance.
- The ambient conditions correspond to an average industrial environment, as defined in MIL-HNBK-217-F or IEC 60654-1, Class C (sheltered location).
  - The ambient temperature is normally 40 °C.
  - A safety factor of 2.5 must be applied for ambient temperatures of 60 °C and frequent temperature fluctuations.

4.5.2 Hardware architecture

The device is considered as a Type A component (non complex). The hardware fault tolerance HFT is 0.

4.5.3 Characteristic values for IM72-11Ex/L and IM72-22Ex/L valve control modules

The device can be used for applications up to SIL 3.

The IM72-11Ex/L and IM72-22Ex/L valve control modules are fed directly with voltage via the digital output of the safety controller. This means that there is no additional energy source, so that the outputs of the devices may not be able to switch to the safe state in the event of an internal fault. All internal faults must therefore be considered as failures without any effect on the safety function or as safe failures which cause the device to switch to the safe state

Rate of safe and dangerous failures

λ_{safe}	$\lambda_{dangerous}$	SFF	PFD_{AVG}
222 FIT	0 FIT	100 %	0×10^0

4.6 Useful life

The calculated failure rates of the device are valid for a useful lifetime of 8 years.

4.7 Special regulations and restrictions

NOTE

Each application has its particular conditions of use and ambient requirements. For this reason, the safety-related assessment of a system must always take the actual process into account – in addition to the general statements concerning probability of failure, tolerances and failure rates of the components. Special application-specific factors such as chemical and physical stresses may thus cause the premature wear of the devices and must therefore be taken into consideration when planning systems. Take special measures to compensate for a lack of experience based values, e.g. through the implementation of shorter test intervals. The estimation of the diagnostic coverage (DC) can vary from application to application. The estimation of the hardware fault tolerance (HFT) can only take place if the use of the compliant object is restricted.

5 Installation and commissioning

DANGER

Failure caused by commissioning and operating errors

Danger to life if safety function fails!

➤ Ensure that the product is only fitted, installed, operated and maintained by trained and qualified personnel.

5.1 Mounting

Observe the mounting instructions in the user manual.

5.2 Connection

Observe the mounting instructions in the user manual.

5.2.1 Wiring diagrams

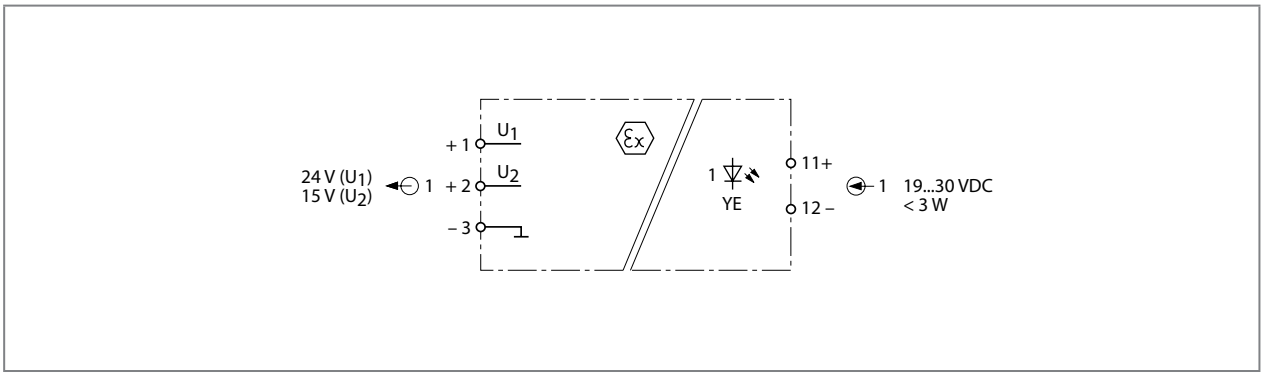

Fig. 2: Block diagram of the IM72-11Ex/L

Hans Turck GmbH & Co. KG • Tel. +49 208/4952-0 • Fax +49 208/4952-264

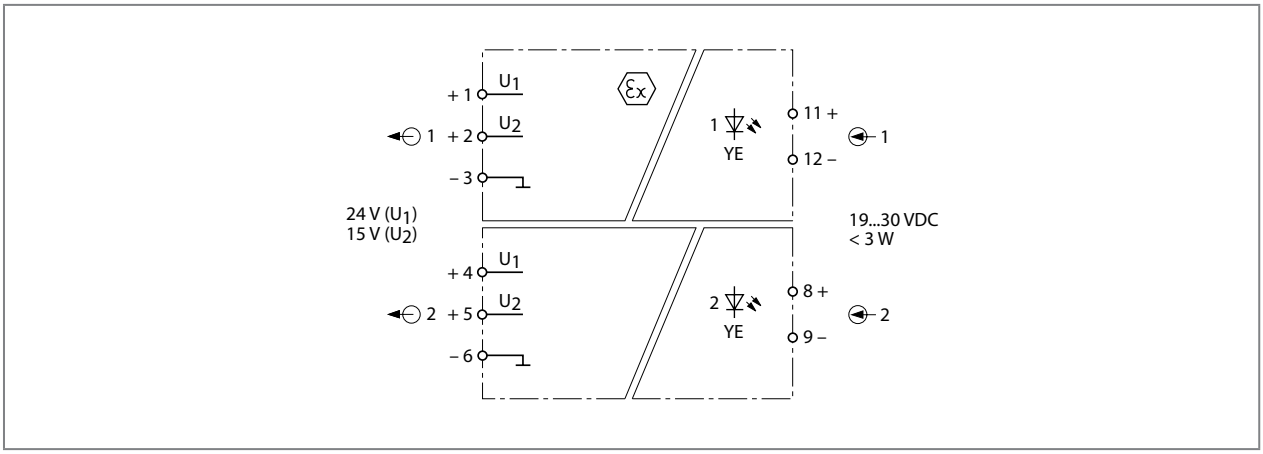

Fig. 3: Block diagram of the IM72-22Ex/L

5.3 Commissioning

When the device is in operation, ensure that the power supply is within the specified voltage range. Commissioning is described in the operating instructions for the particular device.

5.3.1 Selecting valves

If valves are used in safety circuits, they must be certified according to IEC 61508.
Ensure that the devices and the housing materials are suitable for the application.
For this refer also to the applicable data sheets of the TURCK devices at www.turck.com.

6 Operation, maintenance and repair

The information is valid for the operating stress conditions in an industrial environment as per IEC 606541-1 Class C (sheltered location) with an ambient temperature of 40 °C over a long period of time.

6.1 Troubleshooting

The rectification of faults is described in the operating instructions for the particular device.

NOTE
The user must notify TURCK immediately of any faults on the device which occur when it is used in safety instrumented applications.

6.2 Maintenance

Ensure that the plug connections and cables are always in good condition.
The devices are maintenance-free, clean dry if required.

DANGER
Malfunction caused by conductive media or static charge
Danger to life if safety function fails!
➤ When cleaning do not use any liquid media or statically charging cleaning agent.

DANGER
Accidental changing of parameters
Danger to life if safety function fails!
➤ Perform a function test after each cleaning.

6.3 Repair

DANGER
The device must not be repaired.
Danger to life due to malfunction!
➤ Send the device to TURCK for repair. Observe here the specific warranty conditions agreed with the shipment.

6.3.1 Returning devices

If a device has to be returned, bear in mind that only devices with a decontamination declaration will be accepted. This is available for download at
http://www.turck.de/static/media/downloads/Declaration_of_Decontamination_en.pdf
and must be completely filled in, and affixed securely and weather-proof to the outside of the packaging.

7 Decommissioning and withdrawal from service

7.1 Decommissioning

Decommissioning is described in the operating instructions for the particular device.

7.2 Withdrawing from service

After the useful lifetime of eight years has expired, the devices must be taken out of service. The devices are designed for installation in large-scale industrial installations and equipment. The relevant laws and regulations must be observed for the disposal of these installations and tools. They must not be included in normal household garbage.

8 Appendix – EXIDA FMEDA report Turck 04/10-20 R003

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

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.

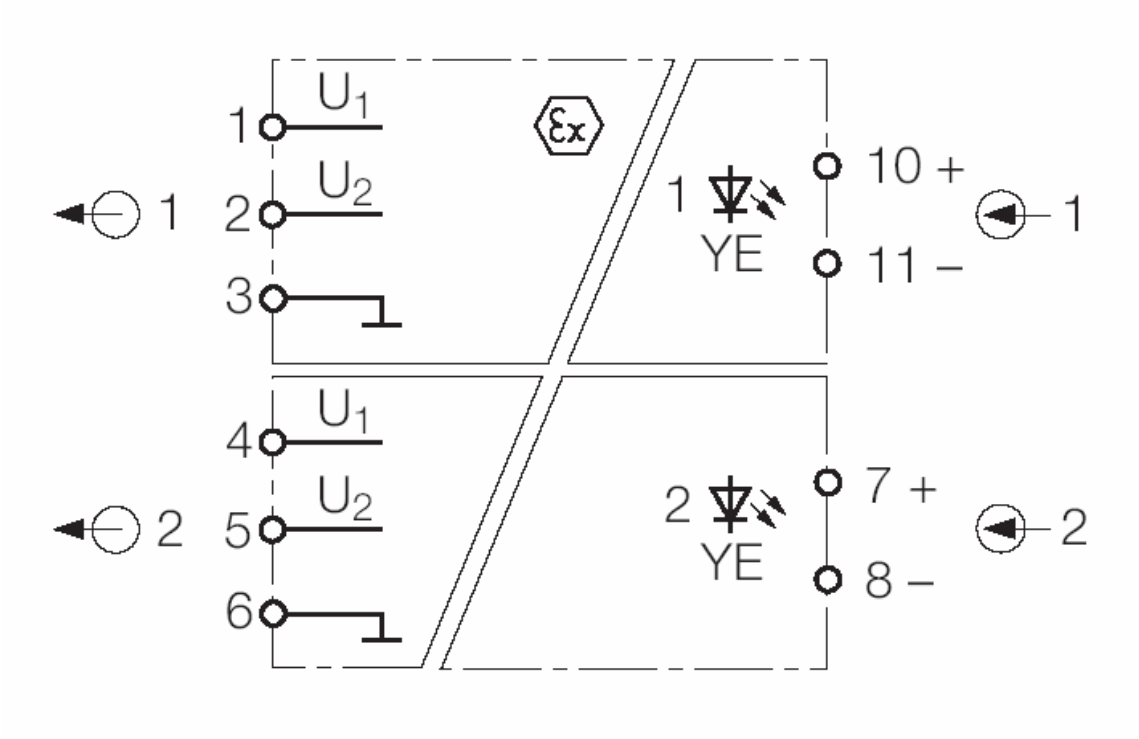

Figure 1: Block diagram of the Solenoid Driver IM72-22Ex/L

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.

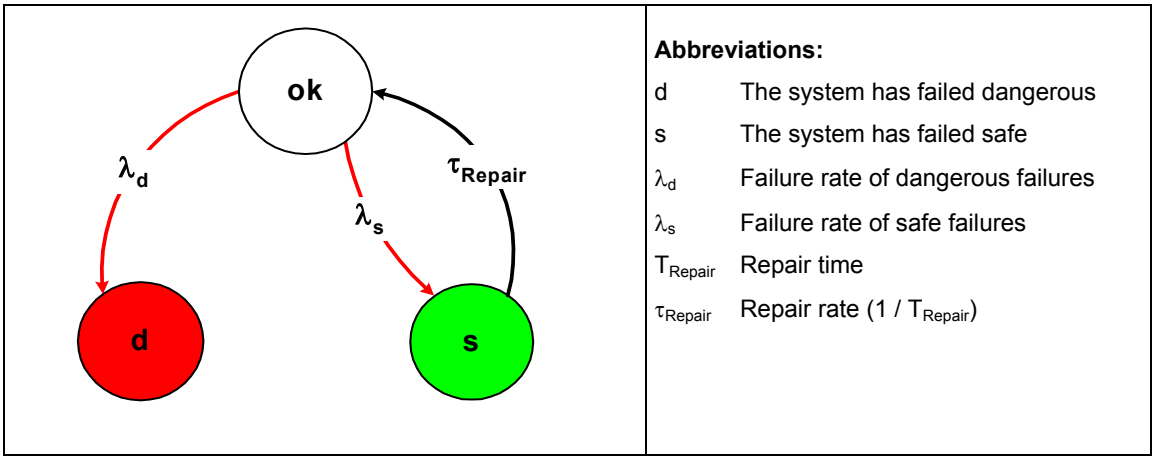

Figure 2: Markov model for a 1oo1 architecture

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

TURCK

Industrielle
Automation

Your Global
Automation Partner!

WORLDWIDE HEADQUARTERS

Hans Turck GmbH & Co. KG
Witzlebenstr. 7
45472 Muelheim an der Ruhr
Germany
Tel. +49 208 4952-0
Fax +49 208 4952-264
Email more@turck.com
Internet www.turck.com

D201460 2015/04