Failure Modes, Effects and Diagnostic Analysis

Project:
IMC-series interface modules

Analogue signal transmitter IMC-AI-*
Isolating transducers IMC-AIA-*
Analogue signal transmitters IMC-AO-*
Isolating switching amplifiers IMC-DI-*
Valve control modules IMC-DO-*

Customer:

Hans Turck GmbH & Co. KG
Mühlheim
Germany

Contract No.: TURCK Q10/03-093
Report No.: TURCK Q10/03-093 R016
Version V1, Revision R0; August 2013

Albert Gegg

Management summary

This report summarizes the results of the hardware assessment carried out on the following IMC-series interface modules listed in Table 1 in the versions listed in the drawings referenced in section 2.5.1.

Table 1: Overview of considered IMC-series interface modules [1]

Function	Description
AI - Analogue signal transmitters	IMC-AI-11Ex-i/L
AIA - Isolating transducers	IMC-AIA-11Ex-i/24VDC, IMC-AIA-11Ex-i/24VDC/K62
AO - Analogue signal transmitters	IMC-AO-11Ex-i/L
DI - Isolating switching amplifiers	IMC-DI-22Ex-PNO/24VDC, IMC-DI-22Ex-PNC/24VDC, IMC-DI-22Ex-PNO/24VDC/K62
DO - Valve control modules	IMC-DO-11Ex/L, IMC-DO-11Ex/L/K62

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) can be calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

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

The IMC-series interface modules can be considered to be Type A[2] elements with a hardware fault tolerance of 0.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1 [3]. The analysis has been carried out with the basic failure rates from the Siemens standard SN 29500. However as the comparison between these two databases has shown that the differences are within an acceptable tolerance the failure rates of the *exida* database are listed.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.

[1] The two channels on the redundant boards shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

[2] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

[3] For details see Appendix 3

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the analogue signal transmitter IMC-AI-11Ex-i/L with 4..20 mA current output communicates detected faults by an alarm output current ≤ 3.6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled.

Table 2: Summary for IMC-AI-* – IEC 61508:2010 failure rates

Failure category	**Failure rates (in FIT) for *exida* Profile 1** [4]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**105**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	1
Fail Low (λ_{L})	104
Fail Dangerous Undetected (λ_{DU})	**22**

No effect	48
No part	27

Total failure rate (safety function)	**127**

SFF [5]	**82%**
DC_D	**82%**

SIL AC [6]	**SIL2**

[4] For details see Appendix 3.

[5] The number listed represents the SFF of the considered element without the connectable sensor or actuator. The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 3: Summary for IMC-AIA-* – IEC 61508:2010 failure rates

Failure category	Failure rates (in FIT) for *exida* Profile 1 [7]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**226**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	3
Fail Low (λ_{L})	223
Fail Dangerous Undetected (λ_{DU})	**51**

No effect	104
No part	6

Total failure rate (safety function)	**277**

SFF [8]	**81%**
DC_D	**81%**

SIL AC [9]	**SIL 2**

[7] For details see Appendix 3.

[8] The number listed represents the SFF of the considered element without the connectable sensor or actuator. The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 4: Summary for IMC-AO-* – IEC 61508:2010 failure rates

Failure category	Failure rates (in FIT) for *exida* Profile 1 [10]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**102**
Fail Safe Undetected (λ_{su})	0
Fail Low (λ_{L})	102
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Undetected (λ_{DU})	**23**
Fail Dangerous Undetected (λ_{du})	22
Fail High (λ_{H})	1
No effect	50
No part	27
Total failure rate (safety function)	**125**
SFF [11]	**81%**
DC_D	**0%**
SIL AC [12]	**SIL 2**

[10] For details see Appendix 3.

[11] The number listed represents the SFF of the considered element without the connectable sensor or actuator. The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[12] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 5: Summary for IMC-DI-* – IEC 61508:2010 failure rates

Failure category	Failure rates (in FIT) for *exida* Profile 1 [13]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**224**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	0
Fail Low (λ_{L})	0
Fail Dangerous Undetected (λ_{DU})	**84**

No effect	79
No part	0

Total failure rate (safety function)	**308**

SFF [14]	**72%**
DC_D	**0%**

SIL AC [15]	**SIL 2**

[13] For details see Appendix 3.

[14] The number listed represents the SFF of the considered element without the connectable sensor or actuator. The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[15] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 6: Summary for IMC-DO-* – IEC 61508:2010 failure rates

Failure category	Failure rates (in FIT) for *exida* Profile 1 [16]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**278**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	0
Fail Low (λ_{L})	0
Fail Dangerous Undetected (λ_{DU})	**0**

No effect	72
No part	0

Total failure rate (safety function)	**278**

SFF [17]	**100%**
DC_D	**0%**

SIL AC [18]	**SIL 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%.

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[16] For details see Appendix 3.

[17] The number listed represents the SFF of the considered element without the connectable sensor or actuator. The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[18] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the Failure Modes, Effects and Diagnostics Analysis (FMEDA) carried out on the described IMC-series interface modules configurations with hardware version as shown in the referred circuit diagrams (see section 2.5.1).

The FMEDA builds the basis for an evaluation whether a sensor element or actuator element including the IMC-series interface modules meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

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

2.2 Roles of the parties involved

Werner Turck GmbH & CO. KG	Manufacturer of the IMC-series interface modules.
exida	Performed the hardware assessment.

Werner Turck GmbH & CO. KG contracted *exida* in March 2010 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-1:2010 (2nd edition) IEC 61508-2:2010 (2nd edition) IEC 61508-4:2010 (2nd edition) IEC 61508-6:2010 (2nd edition)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	SN 29500-1:01.2004 SN 29500-1 H1:07.2011 SN 29500-2:09.2010 SN 29500-3:06.2009 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:07.2011 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Siemens standard with failure rates for components
[N3]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* L.L.C, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N4]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* L.L.C, Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7

2.4 *exida* tools used

[T1]	SILcal V8	FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

	Type	Description[19]	Parts List / Circuit Diagram
[D1]	IMC-AI-11Ex-i/L	AI - Analogue signal transmitters	edb_7560004_gbr_en.pdf edb_7560004_ger_de.pdf job6504_Stueckliste_GER_1.pdf job32016_Stueckliste_GER_1.pdf 12385900_B_02.pdf 12385900_B_03.pdf DPS_IMC_AI.doc ÜPS_IMC_AI.doc
[D2]	IMC-AIA-11Ex-i/24VDC, IMC-AIA-11Ex-i/24VDC/K62	AIA - Isolating transducers	edb_7560009_gbr_en.pdf edb_7560009_ger_de.pdf job32042_Stueckliste_GER_1.pdf job32043_Stueckliste_GER_1.pdf DOK-07281305-BP-000.pdf DOK-07281305-SP-000.pdf DPS_IMC_AIA.doc ÜPS_IMC_AIA.doc
[D3]	IMC-AO-11Ex-i/L	AO - Analogue signal transmitters	edb_7560006_gbr_en.pdf edb_7560006_ger_de.pdf job32017_Stueckliste_GER_1.pdf job6507_Stueckliste_GER_1.pdf 12366500_C_01.pdf 12366500_C_03.pdf DPS_IMC_AO.doc ÜPS_IMC_AO.doc

[19] The two channels on the redundant boards shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

[D4]	IMC-DI-22Ex-PNO/24VDC, IMC-DI-22Ex-PNC/24VDC, IMC-DI-22Ex-PNO/24VDC/K62	DI - Isolating switching amplifiers	edb_7560003_gbr_en.pdf edb_7560003_ger_de.pdf edb_7560010_gbr_en.pdf edb_7560010_ger_de.pdf job6513_Stueckliste_GER_1.pdf job32027_Stueckliste_GER_1.pdf job32030_Stueckliste_GER_1.pdf DOK-07295902-BP-000.pdf DOK-07336500-SP-000.pdf DOK-07336500-BP-000.pdf DPS_IMC_DI.doc ÜPS_IMC_DI.doc
[D5]	IMC-DO-11Ex/L, IMC-DO-11Ex/L/K62	DO - Valve control modules	edb_7560008_gbr_en.pdf edb_7560008_ger_de.pdf job32019_Stueckliste_GER_1.pdf job32020_Stueckliste_GER_1.pdf 12412800_A_01_BP.pdf 12412800_A_02_BP.pdf 12412800_A_05_SP.pdf DPS_IMC_DO.doc ÜPS_IMC_DO.doc
[D6]	Lackwerke Peter_s1_0100000e_004.pdf	Information about the insulation material used	
[D7]	1000x_FR4 Datenblatt.pdf	Information about the base material used	
[D8]	07261302.02_.tif	Data sheet for PCBs	

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.5.2 Documentation generated by *exida* together with the customer

[R1]	FMEDA_V7_IMC-AIL_V0R1.efm of 14.05.13
[R2]	FMEDA_V7_IMC-AIA_L_V0R1.efm of 14.05.13
[R3]	FMEDA_V7_IMC-AOL_V0R1.efm of 14.05.13
[R4]	FMEDA_V7_IMC-DI-T_V0R1.efm of 14.05.13
[R5]	FMEDA_V7_IMC-DO_V0R1.efm of 14.05.13

3 Description of the analyzed elements

The IMC-series interface modules can be considered to be Type A[20] elements with a hardware fault tolerance of 0.

The only exception that should be taken into account are IMC-DI-* modules that are designed with a semi-custom ASIC 724 from ZETEX. In fact there is low complexity, the full analyzability of the used ASIC and that the ASIC does not contain hidden state information such as internal digital registers. It only consists of 103 transistors, 908 resistors and 7 junction capacitors, which can individually be connected. For these reasons it may still be considered as a type A element.

exida did a detailed analysis of the ASIC based on the individual failure modes of the internal transistors, resistors and capacitors. Possible dependencies were taken into account with a common cause factor of 25%. The failure rate from the Siemens standard SN 29500 for a bipolar ECL ASIC with 50 to 5000 transistors was multiplied with a safety factor of 2. The resulting 100 FIT were used in the overall analysis for the Isolating switching amplifiers.

3.1 AI - Analogue signal transmitter

Figure 1: Block diagram - IMC-AI-*

Main features:

- Active current signals are galvanically isolated and transmitted via the 1-port analogue data transmitter IMC-AI-11EX-i/L from the Ex area to the safe area.
- The device features one input circuit 0/4…20 mA and one short-circuit proof output circuit 0/4…20mA.
- Safe galvanic isolation of input and output circuit.
- The input signals are transmitted 1: 1 to the outputs in the safe area without attenuation.
- The devices are loop-powered.

[20] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

3.2 AIA - Isolating transducers

Figure 2: Block diagram – IMC-AIA-*

Main features:

- The 1-channel isolating transducers IMC-AIA-11EX-i/24VDC and IMC-AIA-11EX-i/24VDC/K62 are used to energize intrinsically safe 2-wire transducers in the Ex area and to transmit the measuring signal to the safe area.
- The device features one input and one short-circuit proof output circuit, with 0/4…20 mA each.
- Safe galvanic isolation of input and output circuit. The input signal is transmitted 1:1 without attenuation to the output in the safe area. Due to the 1:1 transmission characteristic, wire-break or short-circuit of the measuring transducer circuit are indicated as currents of 0 mA or > 22.5 mA.
- The IMC-AIA-11EX-i/24VDC and IMC-AIA-11EX-i/24VDC/K62 are external powered and provide galvanic isolation of the supply voltage.

3.3 AO - Analogue signal transmitters

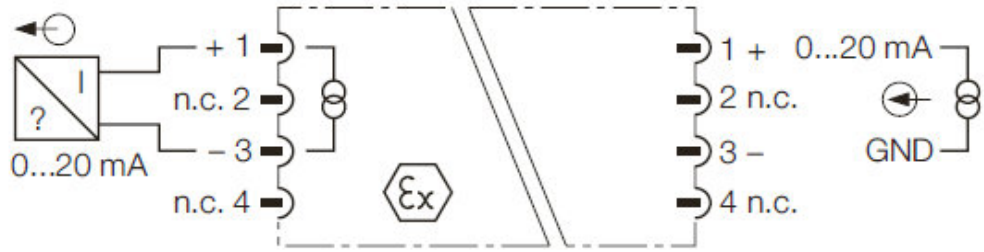

Figure 3: Block diagram - IMC-AO-*

Main features:

- The analogue signal transmitter IMC-AO-11Ex-i/L features 1 channel and the output circuit is intrinsically safe.
- The standard current signal is galvanically isolated and transmitted from the safe to the Ex-area without attenuation (1:1).
- The output circuit is equipped with a short circuit protected power source. Intrinsically analogue actuators like I/P converters (e.g. at control valves) or displays can be applied in the Ex area.
- The device is loop-powered.

3.4 DI – Isolating switching amplifier

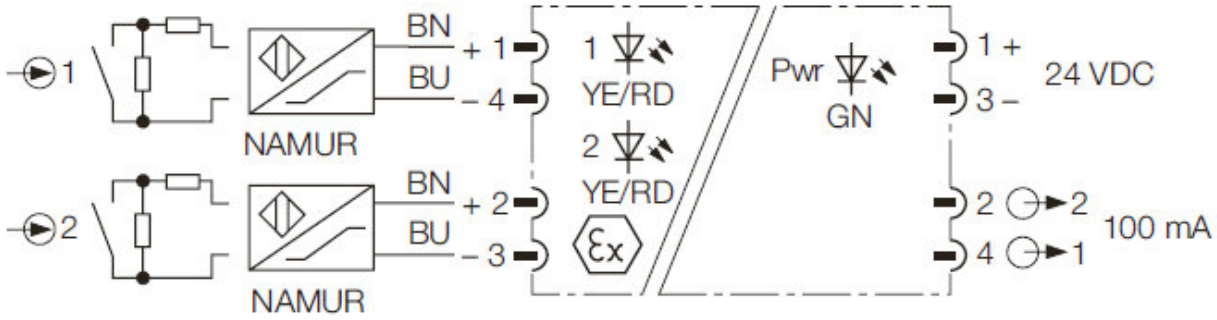

Figure 4: Block diagram - IMC-DI-*

Main features:

- The 2-channel isolating switching amplifiers IMC-DI-22Ex-PNO/24VDC, IMC-DI-22Ex-PNC/24VDC and IMC-DI-22Ex-PNO/24VDC/K62 are equipped with an intrinsically safe input circuit. Sensors according to EN 60947-5-6 (NAMUR) can be connected to the device or potential free contactors.
- When using mechanical contacts, resistors must be wired to the contacts for wire break and short-circuit monitoring (see circuit diagram).
- The switching status of the corresponding output is indicated yellow by the two-color LED. In the event of input circuit errors the dual color LED changes to red, provided the input circuit monitoring function is activated. Thereupon the correspondent output is driven.
- The output circuits of the IMC-DI-22Ex-PNO/24VDC and IMC-DI-22Ex-PNO/24VDC/K62 feature two transistors for the output mode NO (normally open) and the output circuits of the IMC-DI-22Ex-PNC/24VDC feature two potential free transistors for the output mode NC (normally closed).

3.5 DO – Valve control modules

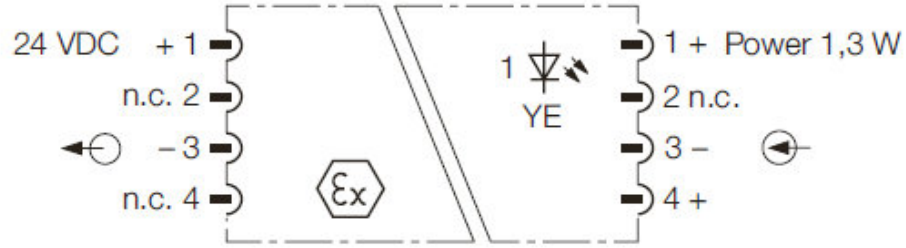

Figure 5: Block diagram - IMC-DO-11Ex/L

Main features:

- The single channel valve drivers of series IMC-DO-11Ex/L feature an intrinsically safe output with limited current and voltage. Thus making direct connection to loads in the Ex-area possible.
- Within the area of applicability of the European directive 94/9/EC (ATEX) it is permitted to operate connected loads in potentially explosive atmospheres caused by dust or gas, provided they comply with the applicable regulations. Typical applications are the control of EEx i pilot valves as well as the supply of displays and transmitters.
- Safe galvanic isolation of input and output circuit.
- The device is loop-powered.
- The output voltage differs with respect to the load. They are adapted to the valves of different manufacturers.

Figure 6: Block diagram - IMC-DO-11Ex/L/K62

Main features:

- The single channel valve drivers of series IMC-DO-11Ex/L/K62 feature an intrinsically safe input with limited current and voltage. Thus making direct connection to control of valves or supply of consumers in explosion hazardous areas possible.
- Within the area of applicability of the European directive 94/9/EC (ATEX) it is permitted to operate connected loads in potentially explosive atmospheres caused by dust or gas, provided they comply with the applicable regulations. Typical applications are the control of EEx i pilot valves as well as the supply of displays and transmitters.
- The device provides safe galvanic isolation of input and output circuit and is loop powered.
- The power output has a rated current of 80mA.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by Werner Turck GmbH & CO. KG. and reviewed by *exida*. The results are documented in [R1] to [R5].

4.1 Description of the failure categories

In order to judge the failure behavior of the IMC-series interface modules, the following definitions for the failure of the products were considered.

Fail-Safe State	For AI and AIA: The fail-safe state is defined as the output reaching the user defined threshold value. For AO: The fail-safe state is defined as the output going to fail low (< 3.6mA). For DI: The fail-safe state is defined as the output being de-energized. This corresponds to an input signal of less than 1.4mA (NAMUR signal). For DO: The fail-safe state is defined as the output being de-energized.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) deviates the output measurement value by more than 2% of full scale or prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (DD).
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics (DU).
Fail High	A fail high failure (H) is defined as a failure that causes the output signal to go to a current above 21mA.
Fail Low	A fail low failure (L) is defined as a failure that causes the output signal to go to a current below 3.6mA.
No Effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No Part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected) 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 rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. 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. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

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 such as *exida* SILStat™ 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 IMC-series interface modules.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- Complete practical fault insertion tests can demonstrate that the fault behavior corresponds to the assumed one in the FMEDAs.
- The device is installed per manufacturer's instructions.
- 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.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- Inputs and outputs are connected to SIL2 / SIL3 compliant subsystems.
- Only one input and one output are part of the considered safety function.
- Only the described versions are used for safety applications.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

4.2.4 Critical Points of Failure

The analysis has shown that no components of the Valve Control Modules IMC-DO-* (IMC-DO-11Ex/L and IMC-DO-11Ex/L/K62) 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 IEC 60947-5-3 (1999) A.1.2 if:

- The Valve Control Modules IMC-DO-* (IMC-DO-11Ex/L and IMC-DO-11Ex/L/K62) 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 (2007) with pollution degree 2 / installation category III, and
- The printed side(s) are coated with an insulation material in accordance with IEC 60664-3 (2003)

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 7.

Table 7: 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 7.

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

4.3 Results

$DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

$\lambda_{total} = + \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{AU})) + 24\ h$

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-2.

This assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg) / (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg + \Sigma\lambda_{DU}\ avg)$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the IMC-series interface modules are only one part of an element, the architectural constraints should be determined for the entire subsystem.

4.3.1 IMC-AI-*

The FMEDA carried out on the IMC-AI-11Ex-i/L interface modules leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	Failure rates (in FIT) for *exida* Profile 1 [21]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**105**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	1
Fail Low (λ_{L})	104
Fail Dangerous Undetected (λ_{DU})	**22**

No effect	48
No part	27

Total failure rate of the safety function (λ_{Total})	**127**
Safe failure fraction (SFF) [22]	**82%**
DC_D	**82%**
MTBF	**565 years**

SIL AC [23]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[21] For details see Appendix 3.

[22] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[23] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

4.3.2 IMC-AIA-*

The FMEDA carried out on the IMC-AIA-11Ex-i/24VDC and IMC-AIA-11Ex-i/24VDC/K62 interface modules leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	Failure rates (in FIT) for *exida* Profile 1 [24]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**226**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	3
Fail Low (λ_{L})	223
Fail Dangerous Undetected (λ_{DU})	**51**

No effect	104
No part	6

Total failure rate of the safety function (λ_{Total})	**277**
Safe failure fraction (SFF) [25]	**81%**
DC_D	**81%**
MTBF	**294 years**

SIL AC [26]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[24] For details see Appendix 3.

[25] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[26] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

4.3.3 IMC-AO-*

The FMEDA carried out on the IMC-AO-11Ex-i/L interface modules leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	Failure rates (in FIT) for *exida* Profile 1 [27]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**102**
Fail Safe Undetected (λ_{su})	0
Fail Low (λ_{L})	102
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Undetected (λ_{DU})	**23**
Fail Dangerous Undetected (λ_{du})	22
Fail High (λ_{H})	1

No effect	50
No part	27

Total failure rate of the safety function (λ_{Total})	**125**
Safe failure fraction (SFF) [28]	**81%**
DC_D	**0%**
MTBF	**566 years**

SIL AC [29]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[27] For details see Appendix 3.

[28] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[29] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

4.3.4 IMC-DI-*

The FMEDA carried out on the IMC-DI-22Ex-PNO/24VDC, IMC-DI-22Ex-PNO/24VDC/K62 and IMC-22Ex-PNC/24VDC interface modules leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	Failure rates (in FIT) for *exida* Profile 1 [30]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**224**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	0
Fail Low (λ_{L})	0
Fail Dangerous Undetected (λ_{DU})	**84**

No effect	79
No part	0

Total failure rate of the safety function (λ_{Total})	**308**
Safe failure fraction (SFF) [31]	**72%**
DC_D	**0%**
MTBF	**295 years**

SIL AC [32]	**SIL 2**

The failure rates are valid for the useful life of the interface module (see Appendix 2).

[30] For details see Appendix 3.

[31] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[32] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

4.3.5 IMC-DO-*

The FMEDA carried out on the IMC-DO-11Ex/L and IMC-DO-11Ex/L/K62 interface modules leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	Failure rates (in FIT) for *exida* Profile 1 [33]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**278**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	0
Fail Low (λ_{L})	0
Fail Dangerous Undetected (λ_{DU})	**0**

No effect	72
No part	0

Total failure rate of the safety function (λ_{Total})	**278**
Safe failure fraction (SFF) [34]	**100%**
DC_D	**0%**
MTBF	**326 years**

SIL AC [35]	**SIL 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.The failure rates are valid for the useful life of the interface module (see Appendix 2).

[33] For details see Appendix 3.

[34] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[35] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. For full assessment purposes all requirements of IEC 61508 must be considered. The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

5 Using the FMEDA results

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following section describes how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} calculation

The following results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).
An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for the IMC-series interface modules considering a proof test coverage of 95% (see Appendix 1.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 4.3. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 8 for the analogue modules and in Table 9 for the digital modules.

For SIL2 applications, the PFD_{AVG} value needs to be < 1.00E-02.
For SIL3 applications, the PFD_{AVG} value needs to be < 1.00E-03.

5.1.1 Analogue modules (AI, AIA, AO)

Table 8: PFD_{AVG} for IMC-series analogue interface modules

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
IMC-AI-11Ex-i/L	PFD_{AVG} = 1,40E-04	PFD_{AVG} = 2,31E-04	PFD_{AVG} = 5,02E-04
IMC-AIA-11Ex-i/24VDC, IMC-AIA-11Ex-i/24VDC/K62	PFD_{AVG} = 3,33E-04	PFD_{AVG} = 5,47E-04	PFD_{AVG} = 1,19E-03
IMC-AO-11Ex-i/L	PFD_{AVG} = 1,40E-04	PFD_{AVG} = 2,31E-04	PFD_{AVG} = 5,01E-04

Figure 7 shows the time-dependent function of PFD_{AVG} for the analogue modules.

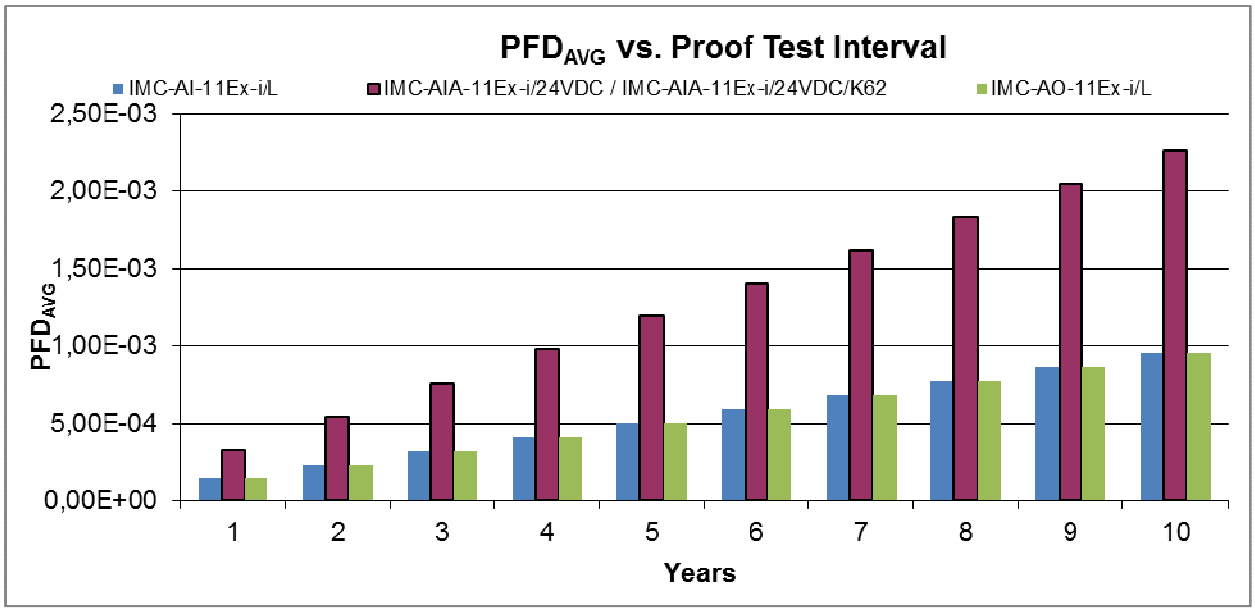

Figure 7: PFD_{AVG} for IMC-series analogue modules (diagram)

5.1.2 Digital modules (DI, DO)

Table 9: PFD_{AVG} for IMC-series digital modules

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
IMC-DI-22Ex-PNO/24VDC, IMC-DI-22Ex-PNC/24VDC, IMC-DI-22Ex-PNO/ 24VDC/K62	PFD_{AVG} = 5,30E-04	PFD_{AVG} = 8,78E-04	PFD_{AVG} = 1,92E-03
IMC-DO-11Ex/L, IMC-DO-11Ex/L/K62	PFD_{AVG} =0,00E+00	PFD_{AVG} = 0,00E+00	PFD_{AVG} =0,00E+00

Figure 8 shows the time-dependent function of PFD_{AVG} for the digital modules.

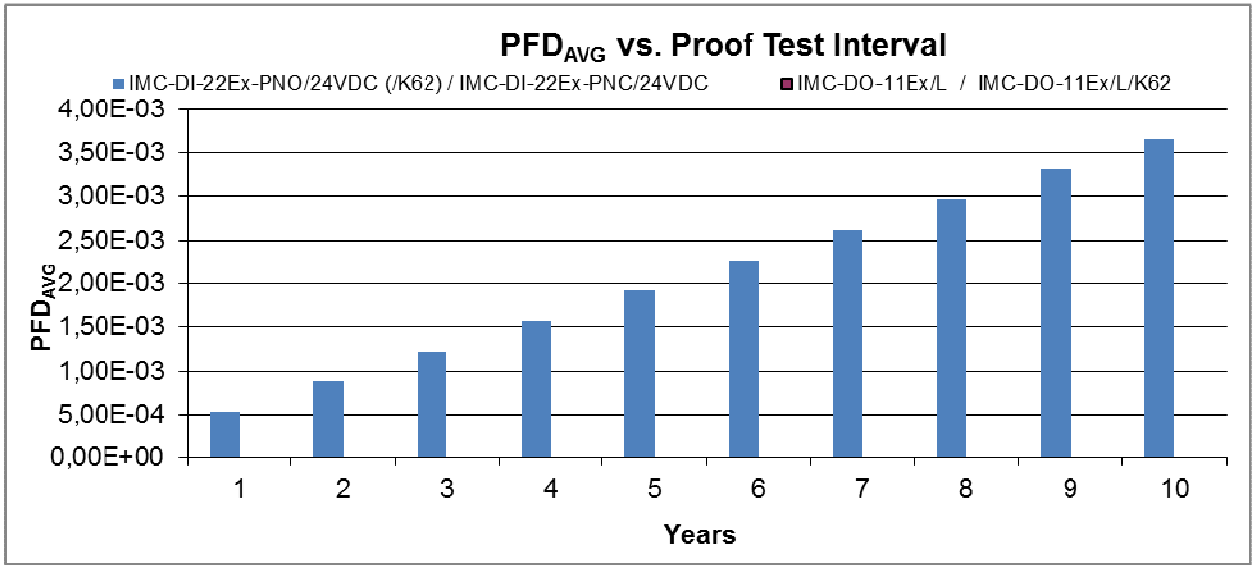

Figure 8: PFD_{AVG} for IMC-series digital modules (diagram)

6 Terms and Definitions

DC_D	Diagnostic Coverage of dangerous failures (DC = λ_{dd} / (λ_{dd} + λ_{du}))
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 safety function is only performed on demand, on order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MRT	Mean Repair Time
MTTR	Mean Time To Restoration
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 element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

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

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

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

7.2 Releases

Version History:	V1R0:	Review comments incorporated; August 06, 2013
	V0R1:	Initial version; July 25, 2013
Author:	Albert Gegg	
Review:	V0R1:	Frank Seeler (Turck); July 25, 2013
		Stephan Aschenbrenner (*exida*); July 25, 2013
Release status:	Released to Werner Turck GmbH & CO. KG. GmbH	

7.3 Release Signatures

Dipl.-Ing. (FH) Albert Gegg, Safety Engineer

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

Appendix 1 Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 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.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1 Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 10.

Table 10: Suggested proof test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Provide appropriate input-/control signals to the interface modules and verify that the function is carried out correctly with regard to the transmitted current/voltage values for the analogue devices and expected signal input/output conditions for the digital interfaces.
3	Provide appropriate input-/control signals to the interface modules and verify that the safety function is carried out correctly.
4	Restore the loop to full operation.
5	Remove the bypass and otherwise restore normal operation

This test will detect more than 95% of possible “du” failures in the IMC-series interface modules.

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

According to section 7.4.9.9 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[36] 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 which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

It is the responsibility of the end user to maintain and operate the actuator per manufacturer's instructions. Regular inspection should show that all components are clean and free from damage.

Based on general field failure data, a useful life period of approximately 10 to 15 years is expected for the IMC-series interface modules.

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

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

Appendix 3 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[1]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[2]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[3]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[4]	G2	G3	G3	G3	G3	Compatible Material
Surge[5]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[6]						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)[7]	6kV	6kV	6kV	6kV	6kV	N/A

[1] Humidity rating per IEC 60068-2-3
[2] Shock rating per IEC 60068-2-6
[3] Vibration rating per IEC 60770-1
[4] Chemical Corrosion rating per ISA 71.04
[5] Surge rating per IEC 61000-4-5
[6] EMI Susceptibility rating per IEC 6100-4-3
[7] ESD (Air) rating per IEC 61000-4-2