



FMEDA and Proven-in-use Assessment

Project:

Temperature Converters D1072S and D1073S
Analog Signal Converter D1053S

Customer:

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

Contract No.: GM 04/10-27

Report No.: GM 04/10-27 R003

Version V2, Revision R0, July 2007

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the temperature converters D1072S and D1073S and the analog signal converter D1053S with software versions PRG024C and PRG005B.

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.

Failure rates used in this analysis are basic failure rates from the Siemens standard SN 29500.

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

The temperature converters D1072S and D1073S and the analog signal converter D1053S are considered to be Type B¹ subsystems with a hardware fault tolerance of 0.

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

As the temperature converters D1072S and D1073S and the analog signal converter D1053S are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the devices and their software was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of $60\% - < 90\%$.

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

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 the device is suitable to be used, as a single device, for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

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

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

The failure rates are valid for the useful life of the temperature converters D1072S and D1073S and the analog signal converter D1053S (see Appendix 3).

¹ Type B subsystem: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 1: Summary – Failure rates

Failure category	Failure rates (in FIT) for variants				
	D1072S with analog output	D1073S with analog output	D1073S with 2 relay outputs in series	D1053S with analog output	D1053S with 2 relay outputs in series
Fail Dangerous Detected	267	267	25	267	25
Fail detected (internal diagnostics or indirectly ²)	65	65	25	65	25
Fail High (detectable by the logic solver)	82	82		82	
Fail low (detectable by the logic solver)	120	120		120	
Fail Dangerous Undetected	95	95	102	95	94
No Effect	134	134	116	134	114
Annunciation Undetected	1	1	28	1	28
Not part	51	51	157	51	160
MTBF = MTTF + MTTR	208 years	208 years	163 years	208 years	164 years

Table 2: Summary – IEC 61508 failure rates

Variant	λ_{SD}	λ_{SU} ³	λ_{DD}	λ_{DU}	SFF	DC _S ⁴	DC _D ⁴
D1072S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1073S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1073S relay output	0 FIT	169 FIT	0 FIT	102 FIT	81%	0%	0%
D1053S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1053S relay output	0 FIT	167 FIT	0 FIT	94 FIT	82%	0%	0%

² “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

³ Note that the SU category includes failures that do not cause a spurious trip

⁴ DC means the diagnostic coverage (safe or dangerous) for the devices by the safety logic solver.

Table 3: Summary – PFD_{AVG} values

Variant	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
D1072S analog output	PFD _{AVG} = 4,16E-04	PFD _{AVG} = 2,08E-03	PFD _{AVG} = 4,15E-03
D1073S analog output	PFD _{AVG} = 4,16E-04	PFD _{AVG} = 2,08E-03	PFD _{AVG} = 4,15E-03
D1073S relay output	PFD _{AVG} = 4,47E-04	PFD _{AVG} = 2,23E-03	PFD _{AVG} = 4,46E-03
D1053S analog output	PFD _{AVG} = 4,16E-04	PFD _{AVG} = 2,08E-03	PFD _{AVG} = 4,15E-03
D1053S relay output	PFD _{AVG} = 4,11E-04	PFD _{AVG} = 2,05E-03	PFD _{AVG} = 4,10E-03

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

The functional assessment has shown that the temperature converters D1072S and D1073S and the analog signal converter D1053S have a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of more than 80%. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to "prior-use" of IEC 61511-1 they can be used as a single device for SIL 2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the temperature converters D1072S and D1073S and the analog signal converter D1053S can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 along with all assumptions.

Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards / Literature used.....	7
2.4 Reference documents.....	8
2.4.1 Documentation provided by the customer.....	8
2.4.2 Documentation generated by <i>exida</i>	9
3 Description of the analyzed modules	10
4 Failure Modes, Effects, and Diagnostics Analysis	12
4.1 Description of the failure categories.....	12
4.2 Methodology – FMEDA, Failure rates.....	13
4.2.1 FMEDA.....	13
4.2.2 Failure rates	13
4.2.3 Assumptions.....	13
5 Results of the assessment.....	15
5.1 D1072S, D1073S, D1053S	17
6 Proven-in-use Assessment	20
6.1 Definition of the term “Proven-in-use” according to IEC 61508	20
6.2 “Prior-use” requirements according to IEC 61511-1	20
7 Terms and Definitions	23
8 Status of the document.....	24
8.1 Liability	24
8.2 Releases	24
8.3 Release Signatures.....	24
Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	25
Appendix 1.1 Section 11.5.3 of IEC 61511-1 First Edition 2003-01	25
Appendix 1.2 Section 11.5.4 of IEC 61511-1 First Edition 2003-01	25
Appendix 1.3 Section 11.5.2 of IEC 61511-1 First Edition 2003-01	25
Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test ..	27
Appendix 2: Possible proof tests to detect dangerous undetected faults.....	29
Appendix 3: Impact of lifetime of critical components on the failure rate	30

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* according to the relevant functional safety standard(s) like 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}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per 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* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like 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 provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 2.

This document shall describe the results of the FMEDAs carried out on the temperature converters D1072S and D1073S and the analog signal converter D1053S with software versions PRG024C and PRG005B.

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

2 Project management

2.1 *exida*

exida is one of the world's leading 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 like TUV and manufacturers, *exida* is a partnership with offices around the world. *exida* 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* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

G.M. International s.r.l Manufacturer of the temperature converters D1072S and D1073S and the analog signal converter D1053S.

exida Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

G.M. International s.r.l contracted *exida* in November 2004 and in September 2006 with the FMEDA and PFD_{AVG} calculation 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 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	IEC 61511-1 First Edition 2003-01	Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
N3	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N4	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N5	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
N6	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	SCD016_p1_r4.sch	Circuit diagram "D1050-D1052-D1053, D1070-D1072-D1073, Converter DIN Rail" revision 4
[D2]	PRL057.PDF	Part List D1072S revision 9
[D3]	TRP033_r0.doc and TRP033.pdf	FMEDA report and fault insertion tests including hardware revision history
[D4]	PRG024A(A-H).asm	Software source code
[D5]	PRG005B.asm	Software source code
[D6]	D1072_E.pdf	Data sheet for D1072*
[D7]	Quality_Manual2000rev3.doc	Quality manual Rev 3 2003.10.01
[D8]	Folder "Quality_Manual_Procedure"	Quality procedures
[D9]	MQ_Annex_D.doc	Modification procedure as part of the quality manual
[D10]	SPP024A_r0.pdf and SPP005B_r0.pdf	Revision history SW
[D11]	INC002_r0.pdf	Statistics of field-feed-back tracking; sold and returned devices
[D12]	INC002.pdf	Updated statistics of field-feed-back tracking; sold and returned devices also considering the relay output versions of D1053S and D1073S
[D13]	Reparation_Report_Sample.pdf	Example of database repair entry
[D14]	SPP024A_r0.pdf	Software project plan SPP024A
[D15]	SPP005B_r0.pdf	Software project plan SPP005B
[D16]	LIST OF APPLICATIONS DOR D104.doc Reference List GM.xls	List of application examples
[D17]	Fw D1072S - D1053S - D1073S.msg of 21.05.07	Email with description of software changes and link to impact analysis and test documents
[D18]	PRL055.PDF	Part list D1053S, revision 12
[D19]	PRL060.PDF	Part list D1073S, revision 11
[D20]	DTS0025.pdf	D1072S datasheet
[D21]	DTS0043.pdf	D1073S datasheet
[D22]	DTS0041.pdf	D1053S datasheet
[D23]	FMEDA_D1053_04_20_2007_06_18.xls	
[D24]	FMEDA_D1053_04_20_2RLY_2007_06_21.xls	
[D25]	FMEDA_D1053_04_20_HYP1_2007_06_25.xls	

[D26]	FMEDA_D1073_TC_RTD_2007_06_18.xls
[D27]	FMEDA_D1073_TC_RTD_HYP1_2007_06_25.xls




2.4.2 Documentation generated by *exida*

[R1]	FMEDA V6 D1072 RTD V1 R1.0.xls of 22.04.05
[R2]	FMEDA V6 D1072 Thermocouple V1 R1.1.xls of 07.10.05
[R3]	FMEDA_D1053_04_20_Review_SA2.xls of 22.06.07
[R4]	FMEDA_D1073_TC_RTD_Review_SA2.xls of 22.06.07
[R5]	Minutes of Meeting PIU.doc of 22.04.05
[R6]	Field data evaluation.xls of 22.04.05 (Field data evaluation of operating hours, sold devices and returned devices)
[R7]	Field data evaluation 2007.xls of 10.07.07 (Field data evaluation of operating hours, sold devices and returned devices)

3 Description of the analyzed modules

The DIN-Rail converters D1072S, D1073S and D1053S convert input signals from Hazardous Area into output signals to drive a Safe Area load.

The temperature converters D1072S and D1073S and the analog signal converter D1053S are considered to be Type B subsystems with a hardware fault tolerance of 0.

	D1072S	D1073S	D1053S
Name	1 Channel, Universal Temperature Signal Converter	1 Channel, Universal Temperature Converter and Trip Amplifier	1 Channel, Analog Signal Converter and Trip Amplifier
Type	Temperature Converter	Temperature Converter	Signal Converter and Trip Amplifier
Supply	12-24 VDC	24 VDC	24 VDC
Field device			
Channels	1	1	1
Safety Function	The D1072S converts a mV, RTD, TC input from temperature sensors or from transmitting potentiometer located in Hazardous Location into a corresponding 4..20 mA current signal to drive a Safe Area load.	The D1073S converts a mV, RTD, TC input from temperature sensors, or from transmitting potentiometer located in Hazardous Location into a corresponding 4..20 mA current signal to drive a Safe Area load or de-energizes the output relays upon reaching a pre-defined trip point.	The D1053S converts a voltage or current input from separately powered source located in Hazardous Location into a corresponding 4..20 mA current signal to drive a Safe Area load or de-energizes the output relays upon reaching a pre-defined trip point.

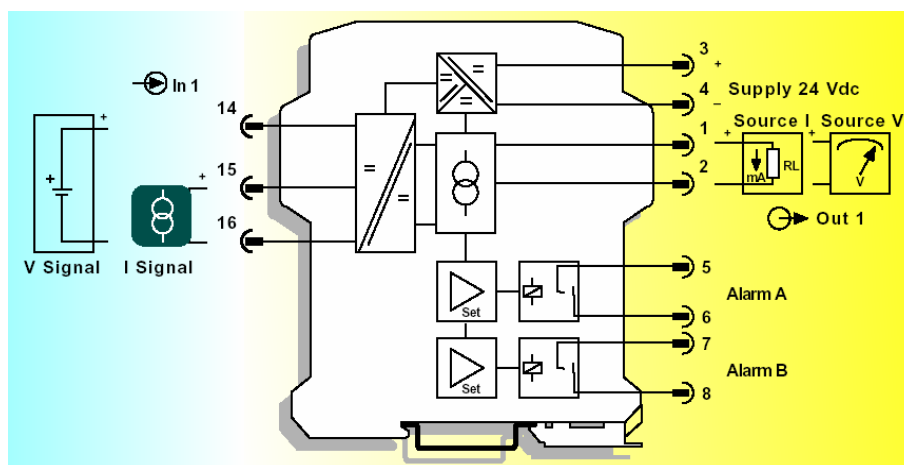


Figure 1: Block diagram of D1053S (with relay output ⁵)

⁵ For safety applications the two relays have to be connected in series.

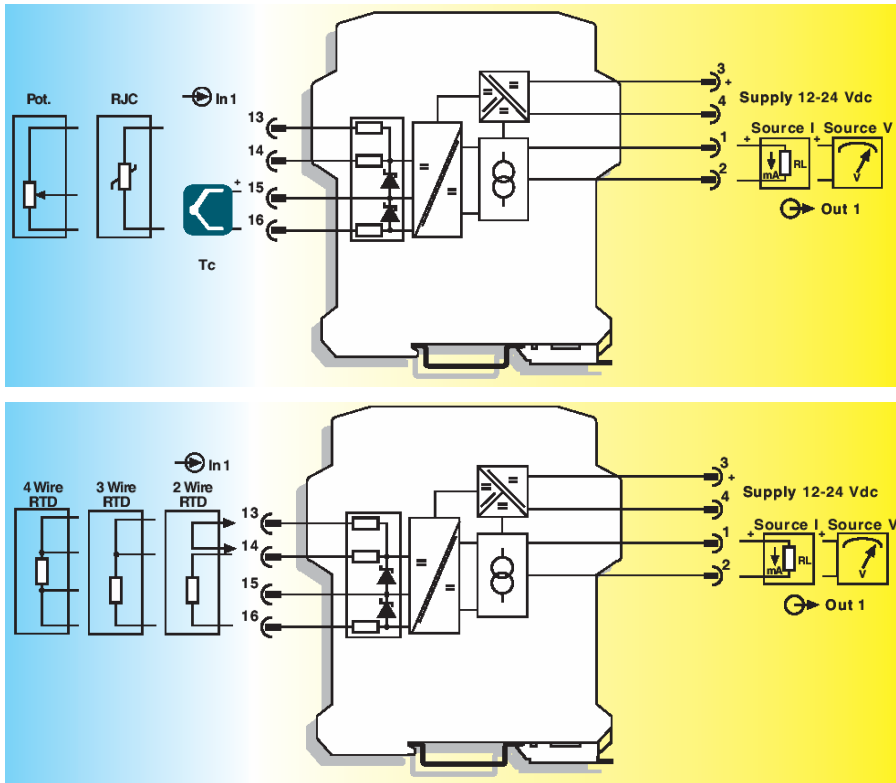


Figure 2: Block diagram of D1072S (with 4-20 mA current output), in two connection options

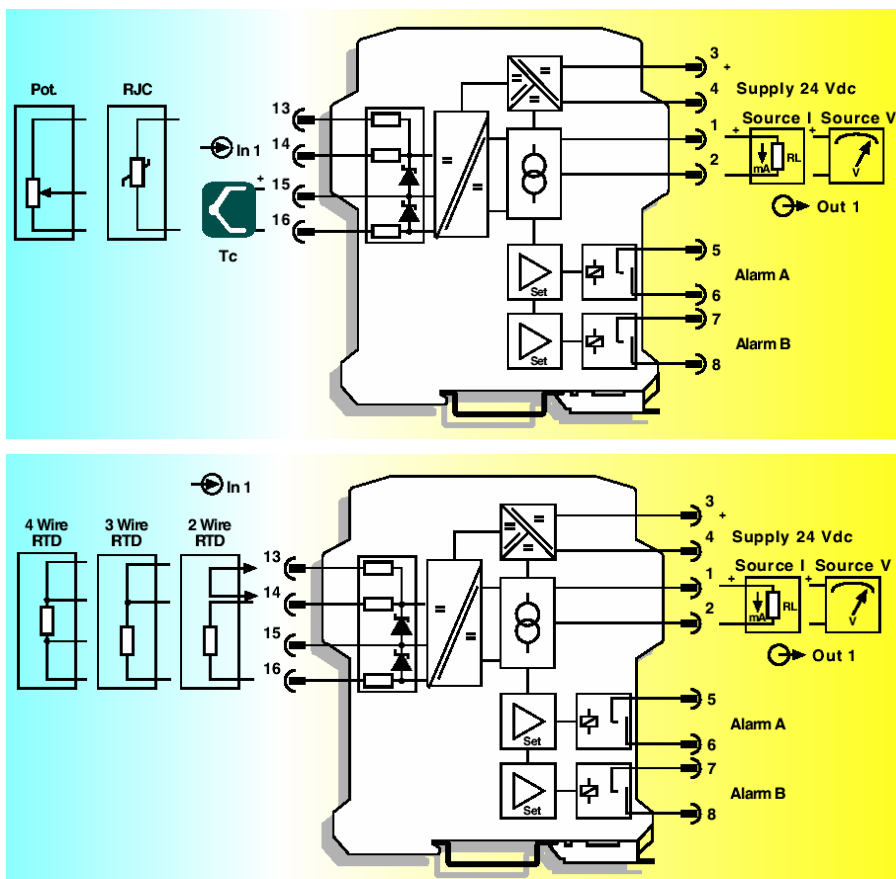


Figure 3: Block diagram of D1073S (with relay output ⁵), in two connection options

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by G.M. International s.r.l and reviewed by *exida*. The results are documented in [D3] and [D23] to [D27] as well as in [R1] to [R4]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see [D3]). This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the temperature converters D1072S and D1073S and the analog signal converter D1053S, the following definitions for the failure of the product were considered. Note that the definitions depend on the converter type.

<p>Definitions common to all variants (D1072S, D1073S, D1053S)</p>	<p>Fail Safe: Failure that causes the output to go to the defined fail-safe state without a demand from the process.</p> <p>Fail Dangerous Undetected: Failure that is dangerous and that is not being diagnosed by internal diagnostics.</p> <p>Fail Dangerous Detected: Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).</p> <p>Annunciation: Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). For the calculation of the SFF it is treated like a safe undetected failure.</p> <p>Fail No Effect: Failure of a component that is part of the safety function but has no effect on the safety function or does not lead to a measurement error of more than 3% (+/- 0.6mA) of the correct value. For the calculation of the SFF it is treated like a safe undetected failure.</p> <p>Not part: Failure of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.</p>
<p>Specific definitions for: 1/ D1072S 2/ D1073S analog output 3/ D1053S analog output</p>	<p>Fail-safe State: The fail-safe state is defined as the output reaching the user defined threshold value.</p> <p>Fail Dangerous: Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 3% (+/- 0.6mA) of the correct value.</p> <p>Fail High: Failure that causes the output signal to go to the maximum output current (> 21 mA).</p> <p>Fail Low: Failure that causes the output signal to go to the minimum output current (< 3,6 mA).</p>

Specific definitions for: 1/ D1073S relay output 2/ D1053S relay output	<p>Fail-safe State: The fail-safe state is defined as the output being de-energized.</p> <p>Fail Dangerous: Failure that that leads to a measurement error of more than 3% (+/- 0.6mA) of the correct value and therefore has the potential to not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or the relay contacts to remain closed.</p>
---	--

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

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.

- Failures during parameterization are not considered.
- 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.
- The repair time after a safe failure is 8 hours.
- The test time is 1 hour.
- The common cause factor for the two relays in series is considered to be 5%.
- The stress levels are average for an industrial environment and 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 40°C. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- All modules are operated in the low demand mode of operation.
- The safety function is carried out via 1 input and 1 output channel.
- In the relay version the two relay outputs are connected in series and are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- External power supply failure rates are not included.
- The application program in the safety logic solver is configured 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.

5 Results of the assessment

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

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

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

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

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

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

The shut-down path for the relay versions of D1053S and D1073S is carried out redundant. Therefore they could be split into two separate subsystems, one representing the input electronics having a hardware fault tolerance of 0, and one representing the shut-down path having a hardware fault tolerance of 1.

For simplicity reasons the analysis, however, was done by considering one of the two relays to be the "diagnostics" for the "primary" relay. A Diagnostic Coverage (DC) of 95% was considered to account for possible common cause failures.

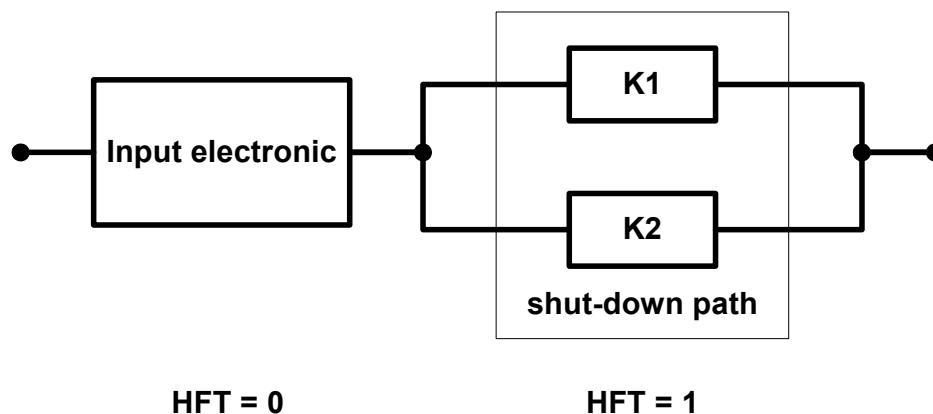


Figure 4: Separation of the relay versions of D1053S and D1073S into two subsystems

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the Microsoft® Excel 2000 based FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.

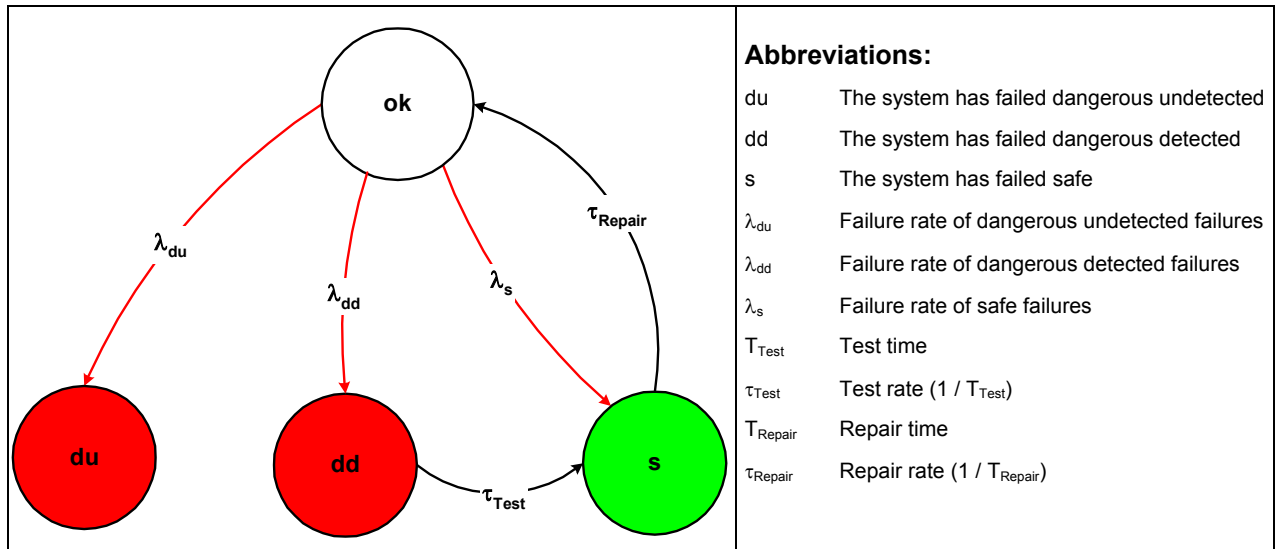


Figure 5: Markov model for a 1oo1D structure

5.1 D1072S, D1073S, D1053S

The FMEDA carried out on the temperature converters D1072S and D1073S and the analog signal converter D1053S leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

Failure category	Failure rates (in FIT) for variants				
	D1072S with analog output	D1073S with analog output	D1073S with 2 relay outputs in series	D1053S with analog output	D1053S with 2 relay outputs in series
Fail Dangerous Detected	267	267	25	267	25
Fail detected (internal diagnostics or indirectly ⁶)	65	65	25	65	25
Fail High (detectable by the logic solver)	82	82		82	
Fail low (detectable by the logic solver)	120	120		120	
Fail Dangerous Undetected	95	95	102	95	94
No Effect	134	134	116	134	114
Annunciation Undetected	1	1	28	1	28
Not part	51	51	157	51	160
MTBF = MTTF + MTTR	208 years	208 years	163 years	208 years	164 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

Table 4: Summary – IEC 61508 failure rates

Variant	λ_{SD}	λ_{SU} ⁷	λ_{DD}	λ_{DU}	SFF	DC _s	DC _D
D1072S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1073S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1073S relay output	0 FIT	169 FIT	0 FIT	102 FIT	81%	0%	0%
D1053S analog output	0 FIT	135 FIT	267 FIT	95 FIT	80%	0%	73%
D1053S relay output	0 FIT	167 FIT	0 FIT	94 FIT	82%	0%	0%

⁶ “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

⁷ Note that the SU category includes failures that do not cause a spurious trip

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

Variant	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
D1072S analog output	$PFD_{AVG} = 4,16E-04$	$PFD_{AVG} = 2,08E-03$	$PFD_{AVG} = 4,15E-03$
D1073S analog output	$PFD_{AVG} = 4,16E-04$	$PFD_{AVG} = 2,08E-03$	$PFD_{AVG} = 4,15E-03$
D1073S relay output	$PFD_{AVG} = 4,47E-04$	$PFD_{AVG} = 2,23E-03$	$PFD_{AVG} = 4,46E-03$
D1053S analog output	$PFD_{AVG} = 4,16E-04$	$PFD_{AVG} = 2,08E-03$	$PFD_{AVG} = 4,15E-03$
D1053S relay output	$PFD_{AVG} = 4,11E-04$	$PFD_{AVG} = 2,05E-03$	$PFD_{AVG} = 4,10E-03$



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

6 Proven-in-use Assessment

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

Reference: IEC 61508-7; B.5.4

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

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

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

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

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

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

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

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

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

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

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

This means that if the requirements of section 11.4.4 of IEC 61511-1 First Edition 2003-01 are fulfilled a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with a SFF of 60% to < 90%¹⁰.

The assessment of the temperature converters D1072S and D1073S and the analog signal converter D1053S has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

Requirement	Argumentation ¹¹
<p>See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01</p>	<ol style="list-style-type: none"> 1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 4 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail¹² is 0,6%. 2. G.M. International s.r.l is ISO 9001 certified with appropriate quality management and configuration management system. See [D7] to [D13]. The assessed sub-systems are clearly identified and specified. The field feedback tracking database of G.M. International s.r.l together with the explanations given in [D11] to [D16] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience. The software and modifications (see [D17]) were carried out in accordance with a SIL 2 compliant modification process. The following operating experience exist: D1072S: More than 123.500.000 operating hours. D1053S: More than 2.000.000 operating hours. D1073S: More than 9.500.000 operating hours. The operating hours for D1073S and D1053S alone would not be sufficient for a proven-in-use proof. However, as D1073S, D1053S and D1072S are almost identical (identical software, slightly different hardware) also D1073S and D1053S can be considered to be suitable for SIL 2 safety functions. Therefore the operating hours of both devices together are considered to be sufficient taking into account the low complexity of the sub-systems and the use in SIL 2 safety functions only). 3. 11.5.2 is under the responsibility of the user / manufacturer → no argumentation. 11.5.3 see bullet items before. 4. N/A 5. Under the responsibility of the user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D16].

¹⁰ IEC 61511-1 First Edition 2003-01 explicitly says "...provided that the dominant failure mode is to the safe state or dangerous failures are detected...".

¹¹ The numbering is based on the requirements detailed in appendix 1.

¹² The probability of failure is the percentage of all returned devices with relevant repair reasons to all sold devices.

Requirement	Argumentation ¹¹
Adjustment of process-related parameters only	The device allows the adjustment of process-related parameters only.
Adjustment of process-related parameters is protected	The adjustment of the process-related parameters of the device is protected. A PC or a configuration tool has to be connected to D1072S, D1073S and D1053S to have access.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the temperature converters D1072S and D1073S and the analog signal converter D1053S with a SFF of 60% - < 90% and a HFT = 0 can be considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

7 Terms and Definitions

DC _S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC _D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B subsystem	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.
T[Proof]	Proof Test Interval

8 Status of the document

8.1 Liability

exida 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.

8.2 Releases

Version: V2

Revision: R0

Version History: V0, R1.0: Initial version, October 7, 2005

V1, R1.0: Review comments incorporated; October 24, 2005

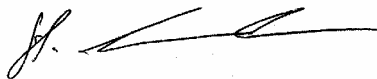
V2, R0: Extended with temperature converter D1073S and analog signal converter D1053S; July 10 2007

Author: Stephan Aschenbrenner

Review: V0, R1.0: Rachel Amkreutz (*exida*); October 17, 2005

Release status: Released to G.M. International s.r.l

8.3 Release Signatures

A handwritten signature in black ink, appearing to read "S. Aschenbrenner".

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

A handwritten signature in black ink, appearing to read "R. Faller".

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

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

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

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

1. An assessment shall provide appropriate evidence that the components and sub-systems are suitable for use in the safety instrumented system.
2. The evidence of suitability shall include the following:
 - consideration of the manufacturer's quality, management and configuration management systems;
 - adequate identification and specification of the components or sub-systems;
 - demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;
 - the volume of the operating experience.

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

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

3. The requirements of 11.5.2 and 11.5.3 apply.
4. Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.
5. For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider:
 - characteristics of input and output signals;
 - modes of use;
 - functions and configurations used;
 - previous use in similar applications and physical environments.

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

(General Requirements)

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

7. Components and sub-systems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.
8. The suitability of the selected components and sub-systems shall be demonstrated, through consideration of:
 - manufacturer hardware and embedded software documentation;
 - if applicable, appropriate application language and tool selection (see clause 12.4.4).
9. The components and sub-systems shall be consistent with the SIS safety requirements specifications.

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

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

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

Table 5 to Table 7 show an importance analysis of the ten most critical dangerous undetected faults and indicate how these faults can be detected during proof testing.

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

Table 5: Importance Analysis of “du” failures for D1072S, D1073S, D1053S, analog output

Component	% of total λ_{du}	Detection through
IC4A-2	21,05%	100% functional test with monitoring of the output signal
IC9-2	21,05%	100% functional test with monitoring of the output signal
IC1A-2	15,79%	100% functional test with monitoring of the output signal
IC7A-2	10,53%	100% functional test with monitoring of the output signal
IC5A	2,21%	100% functional test with monitoring of the output signal
TR4A	1,74%	100% functional test with monitoring of the output signal
D4A	1,68%	100% functional test with monitoring of the output signal
IC3A	1,26%	100% functional test with monitoring of the output signal
IC6A	1,11%	100% functional test with monitoring of the output signal
D1A	1,05%	100% functional test with monitoring of the output signal

Table 6: Importance Analysis of “du” failures for D1053S, relay output

Component	% of total λ_{du}	Detection through
IC4A-2	21,29%	100% functional test with monitoring of the output signal
IC9-2	21,29%	100% functional test with monitoring of the output signal
IC1A-2	15,97%	100% functional test with monitoring of the output signal
OT5	9,58%	100% functional test with monitoring of the output signal
D1A, D2A, D3A	3,19%	100% functional test with monitoring of the output signal
D5A, D6A, D7A	3,19%	100% functional test with monitoring of the output signal
TR18, TR19	2,56%	100% functional test with monitoring of the output signal
IC5A	2,24%	100% functional test with monitoring of the output signal
TR4A	1,76%	100% functional test with monitoring of the output signal
TR23	1,76%	100% functional test with monitoring of the output signal

Table 7: Importance Analysis of “du” failures for D1073Srelay output

Component	% of total λ_{du}	Detection through
IC4A-2	19,57%	100% functional test with monitoring of the output signal
IC9-2	19,57%	100% functional test with monitoring of the output signal
IC1A-2	14,68%	100% functional test with monitoring of the output signal
OT5	8,81%	100% functional test with monitoring of the output signal
D1A, D2A, D3A	2,94%	100% functional test with monitoring of the output signal
D5A, D6A, D7A	2,94%	100% functional test with monitoring of the output signal
TR18, TR19	2,35%	100% functional test with monitoring of the output signal
IC5A	2,05%	100% functional test with monitoring of the output signal
TR4A	1,61%	100% functional test with monitoring of the output signal
TR23	1,61%	100% functional test with monitoring of the output signal

Appendix 2: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 8. This test will detect approximately 99% of possible “du” failures in the converters.

Table 8 Steps for suggested proof test of the converters

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a command to the converter to go to the high alarm current output or initiate a high trip alarm and verify that the analog current reaches that value or the relay outputs de-energize. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3	Send a command to the converter to go to the low alarm current output or initiate a low trip alarm and verify that the analog current reaches that value or the relay outputs de-energize. This tests for possible quiescent current related failures
4	Perform a two-point calibration of the transmitter and verify that the outputs switch accordingly
5	Restore the loop to full operation
6	Remove the bypass from the safety PLC or otherwise restore normal operation

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

According to section 7.4.7.4 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 lifetime¹³ 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.

Table 9 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 9: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Relay	RL1A (RL2A)	100.000 switching cycles

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

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

¹³ 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.