



Failure Modes, Effects and Diagnostic Analysis

Project:

4225 Universal f/l f/f converter series

Customer:

PR electronics A/S

Rønde

Denmark

Contract No.: 21/09-052

Report No.: PR 21/09-052 R031

Version V1, Revision R0; June, 2023

Jürgen Hochhaus

Management summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 4225 Universal f/l f/f converter series with hardware version PR4225-1-03 and software version XX256021P (Output CPU) and XX256313P (Input CPU). Table 1 gives an overview of the considered product variants. Table 2 shows the considered output variants.

A Failure Modes, Effects, and Diagnostic Analysis 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 a subsystem. The FMEDA that is described in this report concerns only the hardware of the 4225 Frequency Converter. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Overview of the considered Product variants

	Description	Suffix	Outputs
[P1]	4225	A	Analog, 0/4...20 mA, voltage and relay
[P2]	4225	B	Relays
[P3]	4225	C	Analog, 0/4...20 mA, voltage and frequency

Table 2: Overview of the considered output variants

	Output	Description
[V1]	Current output	Analog current output, active or passive, with read back of the current (S4-20, S20-4)
[V2]	Relay	Relay output, Normally Open contacts
[V3]	Frequency Output	The input signal is transmitted into a frequency
[V4]	Frequency Output in Relay	Binary electronic output, using the same hardware as the frequency output. Only the "PNP" and "NPN" configuration are covered by this variant

Notes: The safety function of the device is to convert different input functions to a referring output (either analog or binary). For the failure rate determination, the worst case of the different inputs was determined. This worst-case input part failure rate is combined with the failure rates of the outputs listed in Table 2 to determine the overall failure rate. The outputs might be slightly different in the different product versions also. In these cases again the worst-case was chosen and included in the failure rate determination.

The **voltage output** is not part of the safety functionality and **cannot be used for safety applications**.

The 4225C **Frequency Output** used as a relay ("binary") output **in push-pull mode** was not considered in the FMEDA. This output usage is not part of the safety functionality and **cannot be used for safety applications**.

For safety applications only the described variants, as well as the described outputs of the 4225 Universal f/l f/f converter series have been considered. All other possible variants and configurations are not covered by this report.

The analysis shows that the 4225 Frequency Converter has a Safe Failure Fraction of over 90% (assuming that the logic solver is programmed to detect over-scale and under-scale outputs) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The 4225 Universal f/l f/f converter series can be considered to be Type B¹ elements with a hardware fault tolerance of 0.

The failure modes used in this analysis are from the exida Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N5]) for a base average temperature of 40°C. This failure rate database is specified in the safety requirements specification from PR electronics A/S for the 4225 Universal f/l f/f converter series.

The FMEDA was carried out considering dedicated safety measures (diagnostics) implemented in software. The results given in this report are therefore only valid if the correct software version including these diagnostics is used and provide the assumed DC. Furthermore, fault insertion tests must be carried out and documented to verify the effectiveness of the diagnostics.

The failure rates are valid for the useful life of the 4225 Universal f/l f/f converter series (see Appendix A) when operating as defined in the considered scenarios.

¹ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

Table of Contents

Management summary	2
1 Purpose and Scope.....	5
2 Project management.....	5
2.1 <i>exida</i>	5
2.2 Roles of the parties involved.....	5
2.3 Standards / Literature used.....	6
2.4 <i>exida</i> tools used.....	7
2.5 Reference documents.....	8
2.5.1 Documentation provided by the customer	8
2.5.2 Documentation generated by the customer and reviewed by <i>exida</i>	8
3 Product Description.....	9
4 Failure Modes, Effects, and Diagnostic Analysis.....	11
4.1 Failure categories description	11
4.2 Methodology – FMEDA, Failure rates	13
4.2.1 FMEDA	13
4.2.2 Failure rates	13
4.3 Assumptions	14
4.4 Restrictions.....	15
4.5 Results	16
4.5.1 4225 Frequency Converter with current output - [V1]	17
4.5.2 4225 Frequency Converter with relay output - [V2].....	18
4.5.3 4225 Frequency Converter with frequency output - [V3].....	19
4.5.4 4225 Frequency Converter with Frequency Output in relay mode - [V4].....	20
4.6 Architectural Constraints.....	21
5 Using the FMEDA results.....	21
5.1 PFD _{avg} calculation 4225 Frequency Converter	21
5.2 Example PFD _{AVG} / PFH calculation	22
6 Terms and Definitions	24
7 Status of the document	25
7.1 Liability	25
7.2 Releases.....	25
7.3 Release Signatures	25
Appendix A Lifetime of Critical Components	26
Appendix B Proof Tests to Reveal Dangerous Undetected Faults	27
Suggested Proof Test	27
Appendix C Determining Safety Integrity Level	28

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components	<i>exida</i> LLC, Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components ISBN 978-1-934977-09-5
[N3]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 2 – Mechanical Components	
[N4]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 3 – Sensor Components	
[N5]	SN 29500-1:01.2004 SN 29500-1 H1:11.2016 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 29500-11:04.2015 SN 29500-12:02.2008 SN 29500-15:11.2016 SN 29500-16:08.2010	Siemens standard with failure rates for components
[N6]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N7]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N10]	Random versus Systematic – Issues and Solutions, September 2016	Goble, W.M., Bukowski, J.V., and Stewart, L.L., Random versus Systematic – Issues and Solutions, <i>exida</i> White Paper, PA: Sellersville,

		www.exida.com/resources/whitepapers, September 2016.
[N11]	Assessing Safety Culture via the Site Safety Index™, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston, April 2016.
[N12]	Quantifying the Impacts of Human Factors on Functional Safety, April 2016	Bukowski, J.V. and Stewart, L.L., Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York, April 2016.
[N13]	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, November 1999	Goble, W.M. and Brombacher, A.C., Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
[N14]	FMEDA – Accurate Product Failure Metrics, June 2015	Grebe, J. and Goble W.M., FMEDA – Accurate Product Failure Metrics, www.exida.com , June 2015.

2.4 *exida* tools used

[T1]	SILcal V8.0.14	FMEDA Tool
[T2]	exSILentia Ultimate V3.3.0.908	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	4225 FMEDA appendix V1R0, 2017-02-03	FMEDA activity description including assumptions and μ C failure rate distribution
[D2]	4225 HW Design Description.docx, V1R0	Hardware design description
[D3]	System Architecture.pdf with reference to schematic V3R0	Block Diagram with allocation of blocks to detailed design (schematic)
[D4]	BOM-4225A.xlsx	Bill of Material 4225 Variant A
[D5]	BOM-4225B.xlsx	Bill of Material 4225 Variant B
[D6]	BOM-4225C.xlsx	Bill of Material 4225 Variant C
[D7]	4225-1-03-PDF.pdf V3R0, 2021-05-28	Schematic Diagram PR 4225
[D8]	4225V100_IN_20210226.pdf	Product manual 4225 Universal f/l-f/f converter
[D9]	4225 Hardware Fault Insertion Test Report V1.0; 2023-05-23	Hardware Fault Insertion Test on brown out detection

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 the customer and reviewed by *exida*

[R1]	FMEDA – 4225C - XVOLT-TTL Input - 4-20mA Passive Output.xls, V2R0, 09.05.2023	Failure Modes, Effects, and Diagnostic Analysis – 4225 Frequency Converter
[R2]	FMEDA – 4225A - XVOLT-TTL Input - Relay.xls, V2R1, 22.05.2023	Failure Modes, Effects, and Diagnostic Analysis – 4225 Frequency Converter
[R3]	FMEDA - 4225C - XVOLT-TTL Input - PNP as Relay.xls, V2R1, 23.05.2023	Failure Modes, Effects, and Diagnostic Analysis – 4225 Frequency Converter
[R4]	FMEDA - 4225C - XVOLT-TTL Input - Frequency PNP Output.xls, V1R0, 23.05.2023	Failure Modes, Effects, and Diagnostic Analysis – 4225 Frequency Converter

3 Product Description

The 4225 Universal f/I f/f converter series transmitters PR-4225A, 4225B and 4225C are isolated and DIN rail mountable devices used in many different industries for both frequency signal conversion, monitoring, control and safety applications.



Figure 1: PR 4225 (A/B/C) Universal Frequency Transmitters

Figure 2 gives an overview on the functional blocks of the converter. Figure 3 shows the possible input and output signals. The voltage outputs were not analyzed in the FMEDA and are not allowed for usage in safety applications.

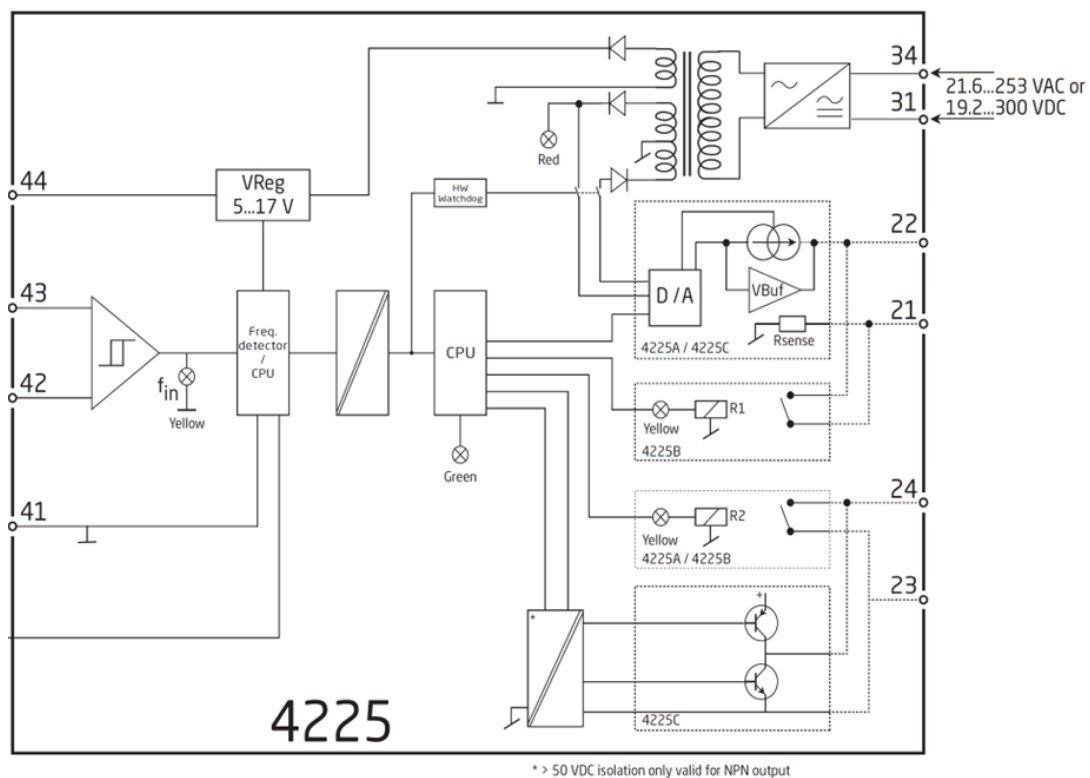
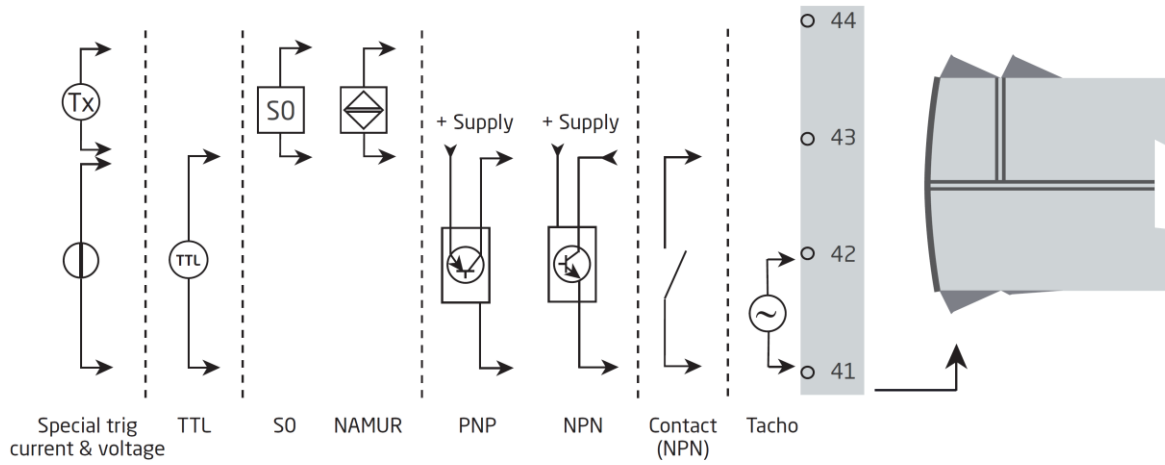


Figure 2: 4225 Frequency Converter, block diagram with parts included in the FMEDA

Input signals:



Output signals:

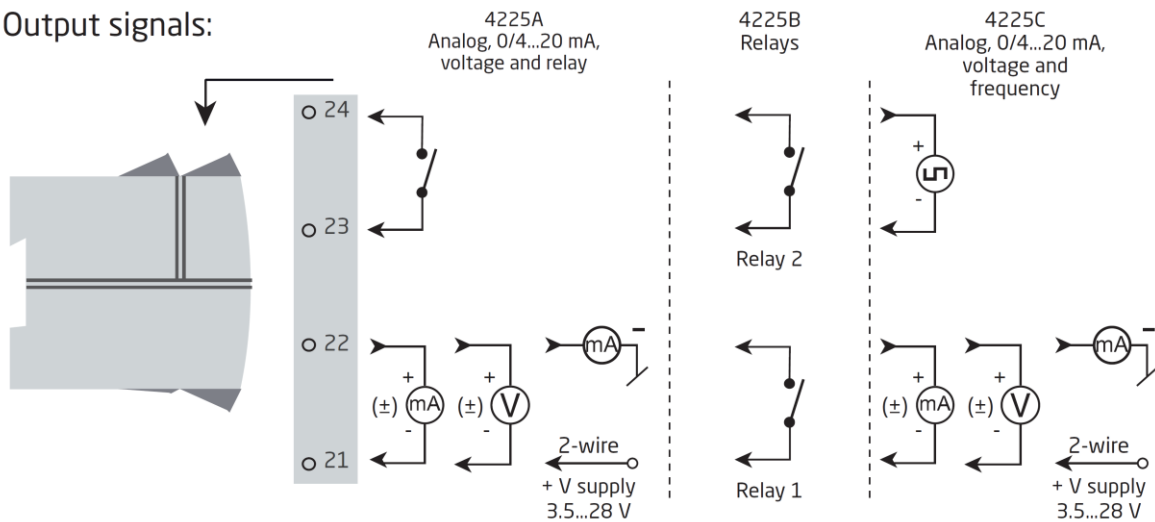


Figure 3 4225 Frequency Converter input and output signals

The 4225 Frequency Converter is classified as a Type B² element according to IEC 61508, having a hardware fault tolerance of 0.

² Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with **PR electronics A/S** and is documented in [R1] to [R4].

4.1 Failure categories description

In order to judge the failure behavior of the 4225 Universal f/I f/f converter series, the following definitions for the failure of the device were considered.

Fail-Safe State

Analog Output	The fail-safe state is defined as output reaching the user defined threshold value.
Relay Output	The fail-safe state is defined as the relay output being de-energized.
Transistor Output	The fail-safe state is defined as the transistor output being blocked. (No current flowing)

Safe A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:

- 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,
- 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.

Dangerous A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:

- 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,
- decreases the probability that the safety function operates correctly when required.

Dangerous Undetected Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).

Dangerous Detected Failure that is dangerous but is detected by internal diagnostics (DD).

Fail High Failure that causes the output signal to go to the over-range or high alarm output current (e.g. > 21 mA).

Fail Low Failure that causes the output signal to go to the under-range or low alarm output current (e.g. < 3.6 mA).

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). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.

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.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress. It combines design FMEA techniques and parts stress analysis with extensions to identify automatic diagnostic techniques, the failure modes relevant to safety instrumented system design, and proof test coverage. It is a technique recommended to generate failure rates for each failure mode category [N13, N14].

4.2.2 Failure rates

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N5]). The rates were chosen in a way that is appropriate for safety integrity level verification calculations and the intended applications. 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.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

Failures caused by external events 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 the failure rate applicability to any particular environment.

Accurate plant specific data may be used to check validity of the failure rate data. 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 4225 Universal f/I f/f converter series.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire 4225 Frequency Converter and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.
- The communication protocols (PR4500 communication interface, Modbus, Bluetooth) are only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The correct parameterization is verified by the user.
- The device is locked against unintended operation/modification.
- The worst-case diagnostic test rate and reaction time is 102s.
- Product is used for measuring static frequencies with change rates slower than 2% of input span divided by response time of the product Hz/s (i.e., (2% of input span)/30ms)).
- The input must always be configured with a low limit corresponding to the worst-case diagnostics test rate or faster i.e. input low limit must be faster than $1/102\text{s} \approx 0,01\text{Hz}$.
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. For higher average temperatures, the failure rates should be multiplied with an experience based factor of e.g. 1.5 for 50°C, 2.5 for 60°C and 5 for 80°C.
- A de-rating analysis is performed to increase reliability of hardware components by operating them well below their maximum stress levels.
- Soft Error Rates (SER) were considered for relative neutron flux of 4.5 corresponding to 1,600 meters above sea.
- Only the described variants are used for safety applications.
- The relay outputs are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.

- The two outputs on the 2-output devices are not used for the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components.
- Only one input and one output are part of the safety function. Signal doubling is not used.

4.4 Restrictions

For safety applications the following limitations apply to the configuration and usage of the product:

- Only one output type can be used for safety per product.
- The following output configurations are valid according to the manufacturer's manual:
 - **4225A**
 - Passive current S4-20, S20-4 (the **S** in **S4-20** is an abbreviation for safe indicating readback is enabled).
 - Active current S4-20, S20-4 (the **S** in **S4-20** is an abbreviation for safe indicating readback is enabled).
 - Relay configured for 'normally open'. De-energized (open) is assumed to indicate error and must be implemented as safe state.
 - **4225B**
 - Relay configured for 'normally open'. De-energized (open) is assumed to indicate error and must be implemented as safe state.
 - **4225C**
 - Only the following output configurations **can** be used for safety applications:
 - Passive current S4-20, S20-4 (the **S** in **S4-20** is an abbreviation for safe indicating readback is enabled) can be used for safety applications.
 - Active current S4-20, S20-4 (the **S** in **S4-20** is an abbreviation for safe indicating readback is enabled).
 - Digital output configured as a relay function using either NPN or PNP as 'normally open'. De-energized (open) is safe state. De-energized (open) is assumed to indicate error and must be implemented as safe state.
 - All frequency output types can be used for safety applications.

These restrictions shall be included in the safety manual for the 4225 Frequency Converter.

4.5 Results

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

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

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:

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

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 4225 Universal f/l f/f converter series is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.5.1 4225 Frequency Converter with current output - [V1]

The FMEDA carried out on the 4225 Universal f/I f/f converter series [V1] under the assumptions described in section 4.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

Table 3: [V1] analog output – failure rates per IEC 61508:2010

Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	0
Dangerous Detected (λ_{DD})	630
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly ³	491
Fail High (λ_H); detected by the logic solver	13
Fail Low (λ_L); detected by the logic solver	110
Annunciation Detected (λ_{AD})	16
Dangerous Undetected (λ_{DU})	34
Annunciation Undetected (λ_{AU})	12
No effect ($\lambda_{\#}$)	311
No part (λ_{-})	331
Total failure rate (safety function)	664
SFF ⁴	94%
DC	94%
SIL AC ⁵	SIL 2

These failure rates are valid for the useful lifetime of the product, see Appendix A.

³ “indirectly” means that these failures are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

⁴ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

4.5.2 4225 Frequency Converter with relay output - [V2]

The FMEDA carried out on the 4225 Universal f/I f/f converter series [V2] under the assumptions described in section 4.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

Table 4: [V2] relay output – failure rates per IEC 61508:2010

Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	130
Dangerous Detected (λ_{DD})	434
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly ⁶	423
Fail High (λ_H); detected by the logic solver	0
Fail Low (λ_L); detected by the logic solver	0
Annunciation Detected (λ_{AD})	11
Dangerous Undetected (λ_{DU})	34
Annunciation Undetected (λ_{AU})	7
No effect ($\lambda_{\#}$)	200
No part (λ_{-})	551
Total failure rate (safety function)	598
SFF ⁷	94%
DC	92%
SIL AC ⁸	SIL 2

These failure rates are valid for the useful lifetime of the product, see Appendix A.

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

⁷ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁸ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

4.5.3 4225 Frequency Converter with frequency output - [V3]

The FMEDA carried out on the 4225 Universal f/I f/f converter series [V3] under the assumptions described in section 4.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

Table 5: [V3] frequency output – failure rates per IEC 61508:2010

Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	0
Dangerous Detected (λ_{DD})	633
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly ⁹	431
Fail High (λ_H); detected by the logic solver	0
Fail Low (λ_L); detected by the logic solver	186
Annunciation Detected (λ_{AD})	16
Dangerous Undetected (λ_{DU})	52
Annunciation Undetected (λ_{AU})	4
No effect ($\lambda_{\#}$)	244
No part (λ_{-})	424
Total failure rate (safety function)	685
SFF ¹⁰	92%
DC	92%
SIL AC ¹¹	SIL 2

These failure rates are valid for the useful lifetime of the product, see Appendix A.

⁹ “indirectly” means that these failures are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

¹⁰ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹¹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

4.5.4 4225 Frequency Converter with Frequency Output in relay mode - [V4]

The FMEDA carried out on the 4225 Universal f/I f/f converter series [V4] under the assumptions described in section 4.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

Table 6: [V3] Frequency Output in relay mode – failure rates per IEC 61508:2010

Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	149
Dangerous Detected (λ_{DD})	444
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly ¹²	432
Fail High (λ_H); detected by the logic solver	0
Fail Low (λ_L); detected by the logic solver	0
Annunciation Detected (λ_{AD})	12
Dangerous Undetected (λ_{DU})	52
Annunciation Undetected (λ_{AU})	4
No effect ($\lambda_{\#}$)	326
No part (λ_{-})	344
Total failure rate (safety function)	645
SFF ¹³	91%
DC	89%
SIL AC ¹⁴	SIL 2

These failure rates are valid for the useful lifetime of the product, see Appendix A.

¹² “indirectly” means that these failures are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

¹³ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁴ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

4.6 Architectural Constraints

According to IEC 61508-2 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.

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.

The analysis shows that the 4225 Frequency Converter has a Safe Failure Fraction of over 90% (assuming that the logic solver is programmed to detect over-scale and under-scale outputs) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The architectural constraint type for the 4225 Frequency Converter is B. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

5 Using the FMEDA results

Using the failure rate data displayed in section 4.5, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{AVG}) calculation can be performed for the entire safety function.

Probability of Failure on Demand (PFD_{AVG}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{AVG}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{AVG} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{AVG}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix C for a complete description of how to determine the Safety Integrity Level for an entire safety function. The mission time used for the calculation depends on the PFD_{AVG} target and the useful life of the product. The failure rates for all the devices of the safety function and the corresponding proof test coverages are required to perform the PFD_{AVG} calculation. The proof test coverage of the suggested proof test for the 4225 Universal f/I f/f converter series is listed in Appendix B. This is combined with the dangerous failure rates after proof test for other devices to establish the proof test coverage for the entire safety function.

When performing testing at regular intervals, the 4225 Universal f/I f/f converter series contribute less to the overall PFD_{AVG} of the Safety Instrumented Function.

The following section gives a simplified example on how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation 4225 Frequency Converter

Using the failure rate data displayed in section 4.5, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third-party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix C for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test is listed in Appendix A.

5.2 Example PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 4225 Universal f/l f/f converter series with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.5.1. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 7 lists the results for different proof test intervals considering an average proof test coverage of 90% (see Appendix B).

Table 7: 4225 Universal f/l f/f converter series – PFD_{AVG} / PFH values

	PFH ¹⁵	T[Proof]	
		1 year	4 years
[V1]	PFH = 4.61 E-08 1/h	PFD _{AVG} = 4.35 E-04	PFD _{AVG} = 9.60 E-04

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h. As the 4225 Universal f/l f/f converter series are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget they should be better than or equal to 1.00E-03 or 1.00E-07 1/h, respectively. The calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of the allowed range, i.e. to be better than or equal to 1.00E-03 or 1.00E-07 1/h, respectively.

The resulting PFD_{AVG} graphs generated from the exSILentia tool for a proof test of 1 year are displayed in Figure 4.

¹⁵ The PFH value is based on a worst-case diagnostic test rate and a reaction time of 20ms. The ratio of the diagnostic test rate to the demand rate shall equal or exceed 100.

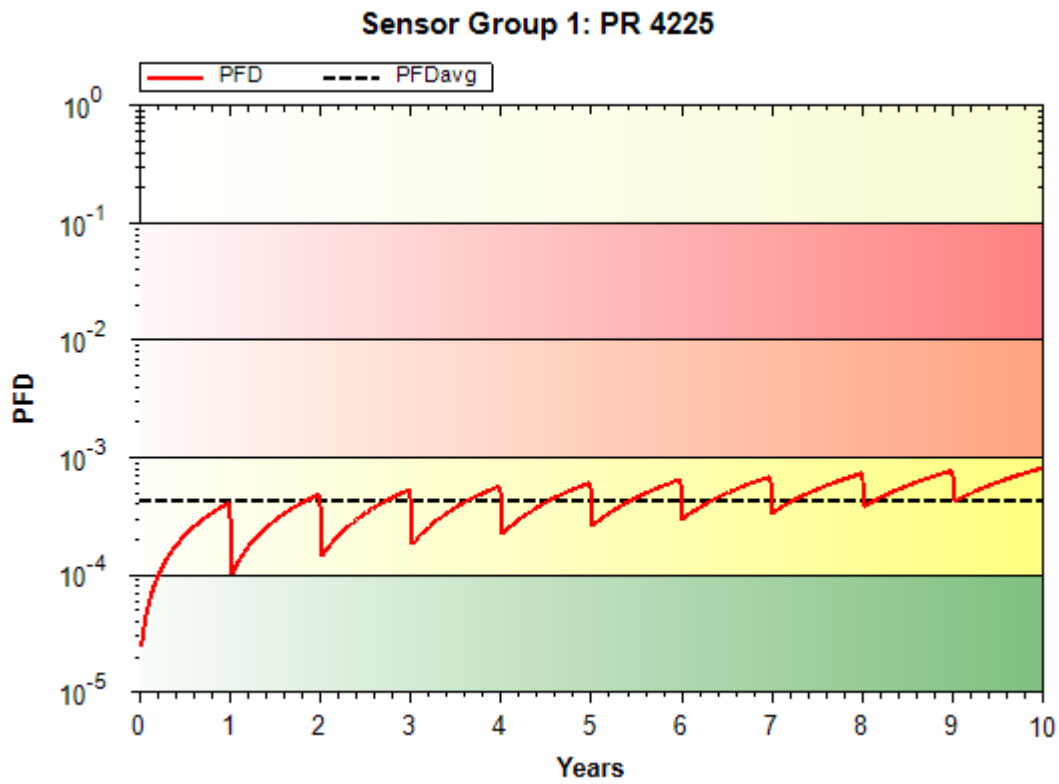


Figure 4: PFD_{AVG}(t)

6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
DC	Diagnostic Coverage of dangerous failures ($DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$)
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
PFD _{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 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: V0R1: Initial draft version for review; May 26, 2023
V1R0: Changes based on review findings – some editorial findings and additional step in the proof test; June 02, 2023

Authors: Jürgen Hochhaus
Review: V0R1: June 01, 2023 by Rasmus Ellerbæk Ørndrup, PR electronics A/S
Stephan Aschenbrenner, *exida*

Release status: Released

7.3 Release Signatures



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



Dipl.-Ing. (FH) Jürgen Hochhaus, Senior Safety Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the exida FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime¹⁶ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the probability 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 8 which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{avg} calculation and what their estimated useful lifetime is.

Table 8 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 90,000 hours
Relay	Approx. 100, 000 switching cycles with resistive load.

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.

For high demand mode applications, the relays can be a limiting factor and have to be considered in the useful lifetime assumption. Loads other than resistive can lower the amount of switching cycles determining the useful lifetime.

Experience has shown that the useful lifetime of mechanical components often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

It is the responsibility of the end user to maintain and operate the 4225 Frequency Converter per manufacturer's instructions.

Experience has shown that the useful lifetime of mechanical components often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

The limiting factors with regard to the useful lifetime of the system are the electrolytic capacitors. Therefore, the useful is lifetime predicted to be 10 years when the device is operated at 40°C.

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

¹⁶ 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 B Proof Tests to Reveal Dangerous Undetected Faults

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 automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

Suggested Proof Test

The suggested proof test described in Table 9 will detect 90% of possible DU failures in the 4225 Frequency Converter.

Table 9 Suggested Proof Test – 4225 Frequency Converter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Disconnect the input signal(s) from the input terminals and connect instead a simulator suited for simulating the actual input setup.
3.	If input sensor/loop supply is used: Measure that the supply voltage is within $\pm 10\%$ of setting.
4.	Apply input value(s) corresponding to 0% and 100% output range for the analog outputs. For the relay (binary) outputs apply input values below and above the considered threshold.
5.	Observe whether the output acts as expected.
6.	Restore the input terminals to normal operation, i.e. re-connect the input signal(s).
7.	Measure the process value at the connected input and observe that the output corresponds to the applied input value(s).
8.	Remove the bypass from the safety PLC or otherwise restore normal operation.

Appendix C Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). **The numbers used in the examples are not for the product described in this report.**

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL), see [N6] and [N8].

These are:

- A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;
- B. Architecture Constraints (minimum redundancy requirements) are met; and
- C. a PFD_{AVG} / PFH calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC 61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N9].

C. Probability of Failure on Demand (PFD_{AVG}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{AVG}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restoration (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{AVG} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC 61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{AVG} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the ones of the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{AVG} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{AVG} contributions are Sensor $PFD_{AVG} = 5.55E-04$, Logic Solver $PFD_{AVG} = 9.55E-06$, and Final Element $PFD_{AVG} = 6.26E-03$ Figure 2: 4225 Frequency Converter, block diagram with parts included in the FMEDA (Figure 5).

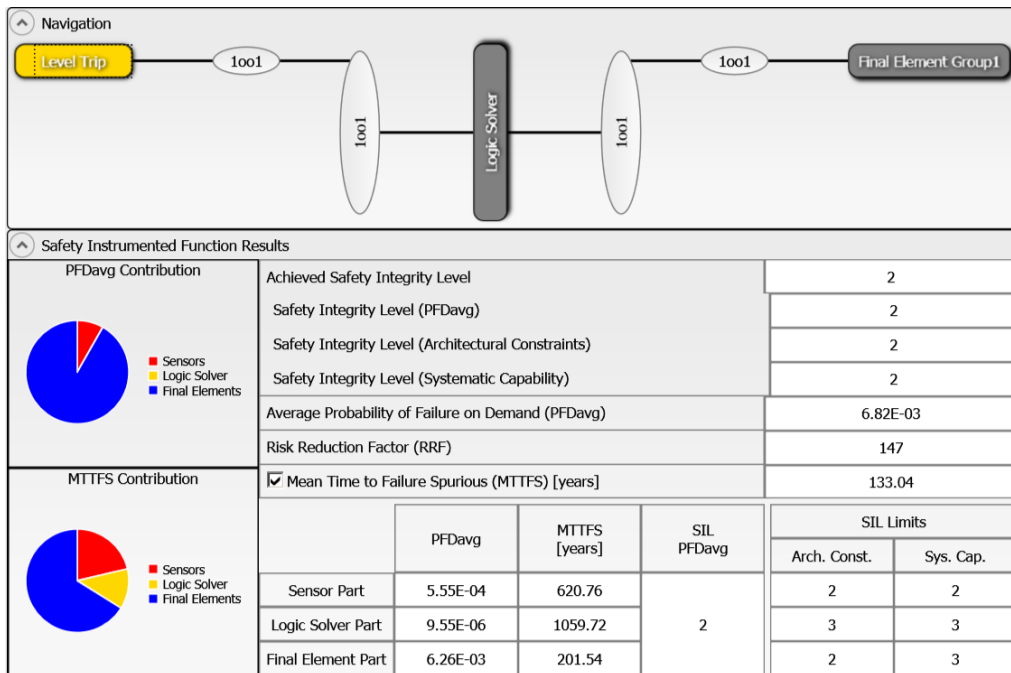


Figure 5: exSILentia results for idealistic variables

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 6

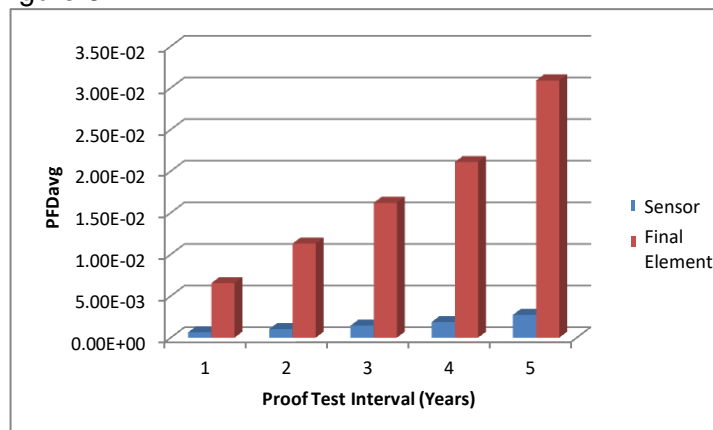


Figure 6: PFD_{AVG} versus Proof Test Interval

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{AVG} for the SIF equals $5.76E-02$ which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD_{AVG} contributions are Sensor $PFD_{AVG} = 2.77E-03$, Logic Solver $PFD_{AVG} = 1.14E-05$, and Final Element $PFD_{AVG} = 5.49E-02$ (Figure 7).

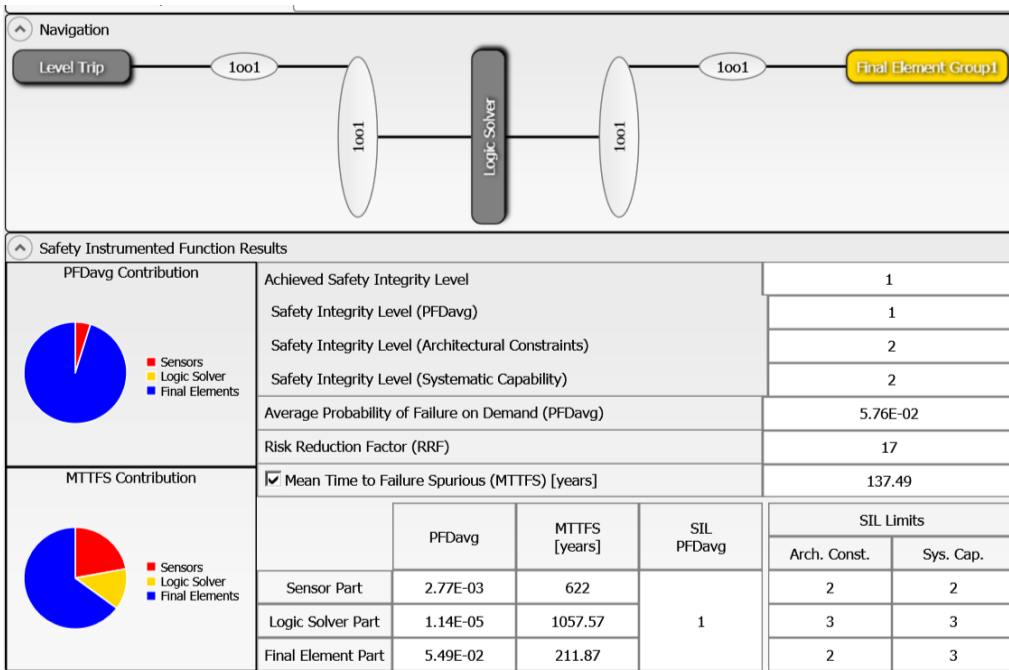


Figure 7: exSILentia results with realistic variables

It is clear that PFD_{AVG} results can change an entire SIL level or more when all critical variables are not used.