Failure Modes, Effects and Diagnostic Analysis

Project:
Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*

Customer:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: Stahl Q18-07-006
Report No.: Stahl Q18-07-006 R035
Version V1, Revision R0; October 2018

Jürgen Hochhaus

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of the hardware assessment carried out on the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*with hardware version as listed in the drawings referenced in section 2.5.1. Table 1 gives an overview of the considered device versions. For each version, the different devices have the same circuit diagram.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) can be calculated for a subsystem. For full assessment purposes, all requirements of IEC 61508 must be considered.

Table 1: Overview of the considered device versions

Var. Id	Variant	Output values
[V1]	9276/10-21-25-00s/ 9276/10-21-25-00k	21 V / 25 mA
[V2][1]	9276/10-21-40-00s/ 9276/10-21-40-00k	21 V / 40 mA
	9276/10-24-48-00s/ 9276/10-24-48-00k	24 V / 48 mA
	9276/10-21-60-00s/ 9276/10-21-60-00k	21 V / 58 mA

For safety applications only the described versions of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00* have been considered. All other possible variants and configurations are not covered by this report.

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 [N3]). This failure rate database is specified in the safety requirements specification from R. STAHL Schaltgeräte GmbH for the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*.

According to table 2 of IEC 61508-1:2010 the average PFD for systems operating in low demand mode has to be $\geq 10^{-4}$ to $< 10^{-3}$ for SIL 3 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to 1,00E-04.

The Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00* can be considered to be Type A[2] elements with a hardware fault tolerance of 0.

The Digital Outputs Loop Powered 9276/10-21-25-00* and 9276/10-21-**-00* / 9276/10-24-**-00* are operated in passive mode and can therefore be regarded as loop powered modules. Because loop powered modules are directly driven from the digital output of a safety PLC there is no additional power supply which can keep the output energized in case of an internal fault. Thus, all internal faults have either no effect on the safety function or lead to a safe state.

[1] The variants listed have the same circuitry and only component values are different.

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

The following tables show how the above stated requirements are fulfilled for the considered Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*.

Table 2: [V1] 9276/10-21-25-00* – failure rates per IEC 61508:2010

Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**50**
Dangerous Detected (λ_{DD})	**0**
Dangerous Undetected (λ_{DU})	**0**
No effect	70
Total failure rate (safety function)	**50**
SFF [3]	**100%**
DC	**0%**
SIL AC [4]	**SIL 3**

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

[4] 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.

Table 3: [V2] 9276/10-21--00* and 9276/10-24-**-00*– failure rates per IEC 61508:2010**

Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**50**
Dangerous Detected (λ_{DD})	**0**
Dangerous Undetected (λ_{DU})	**0**
No effect	73
Total failure rate (safety function)	**50**
SFF [5]	**100%**
DC	**0%**
SIL AC [6]	**SIL 3**

The failure rates are valid for the useful life of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*(see Appendix A) when operating as defined in the considered scenarios.

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

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL 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.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*with hardware version as listed in the drawings referenced in section 2.5.1.
The FMEDA builds the basis for an evaluation whether an element including the described Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world’s leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world’s top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

R. STAHL Schaltgeräte GmbH	Supplier of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*.
exida	Performed the hardware assessment.

R. STAHL Schaltgeräte GmbH contracted *exida* in July 2018 with the creation of this report.

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]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	SN 29500-1:01.2004 SN 29500-1 H1:07.2013 SN 29500-2:09.2010 SN 29500-3:06.2009 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:07.2013 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Siemens standard with failure rates for components
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	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
[N6]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 *exida* tools used

[T1]	SILcal V6.5.1	FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	Kurzumschreibung von FMEDA-Berichten.msg	Mail from Sabine Reistle, dated 19.6.2018. showing the device variant names.
[D2]	Einverständniserklärung_SD_SIL.PDF	Agreement with the supplier, including statement of production responsibility by the supplier, dated 2017-03-16

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 manufacturer

[R1]	FMEDA files as listed in 16/04-017 R025.

3 Product Description

3.1 9276/10-21-**-00* and 9276/10-24-**-00*

The Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*are devices used for intrinsically safe applications for solenoid valves and are used without additional power supply. Input and output are galvanically isolated. The Digital Outputs Loop Powered are operated in passive mode and are therefore loop powered modules. Because a loop powered module is directly driven from the digital output of a safety PLC there is no additional power supply which can keep the output energized in case of an internal fault. Thus, all internal faults have either no effect on the safety function or lead to a safe state.

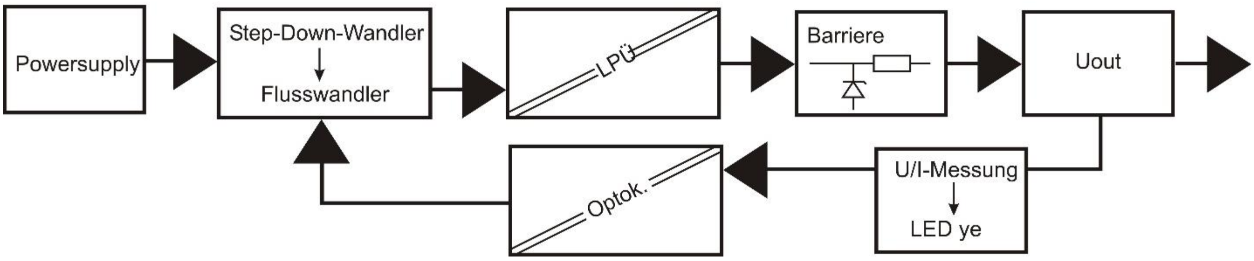


Figure 1: Digital Outputs Loop Powered 9276/10-21--00* and 9276/10-24-**-00* block diagram**

The Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*can be considered to be Type A[7] elements with a hardware fault tolerance of 0.

The description above is valid for all devices of the considered Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*described in Table 1.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with R. STAHL Schaltgeräte GmbH and is documented in [D1] and [D2].

4.1 Description of the failure categories

In order to judge the failure behavior of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*, the following definitions for the failure of the products were considered.

Fail-Safe State
The fail-safe state is defined as the output being de-energized.

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

a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

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

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,

b) decreases the probability that the safety function operates correctly when required.

Dangerous 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).

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.

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 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 [N3]). 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.

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 their applicability to any particular environment. 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.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat^{TM} that indicates higher failure rates, the higher numbers shall be used.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*are installed per the supplier's instructions.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment with temperature limits within the supplier'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.
- Only the described device versions are used for safety applications.

4.2.4 Critical Point of Failure: Short circuit on printed circuit board

The analysis has shown that no components of the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*can be found where potentially dangerous failures exist. All component failures have either no effect on the safety function or can only lead to the defined fail-safe state or are detected and mitigated to the safe state.

The only possible faults that could have an impact on the safety function is a short-circuit on the printed circuit board of the Digital Output Loop Powered.

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

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

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category III for a nominal voltage of 24 VDC are given in Table 4.

Table 4: Clearances and creepage distances according to IEC 60661-1

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

According to R. Stahl Schaltgeräte GmbH the base material used is FR4 according to NEMA- LI 1-1989 which is identical to IEC 60249, maximum temperature > 130°C (according to UL 796A), comparative tracking index CTI > 175 according to IEC112 with UL approval. The minimum distance between the two channels on one board is 1 mm. This is sufficient according to Table 4.

The insulation material is based on modified acryl resin and the comparative tracking index CTI > 600. The dielectric strength is given with 65kV/mm.

4.3 Results

DC = λ_{DD} / (λ_{DD} + λ_{DU})

λ_{total} = λ_{SD} + λ_{SU} + λ_{DD} + λ_{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 = ($\Sigma\lambda_S$ avg + $\Sigma\lambda_{DD}$ avg) / ($\Sigma\lambda_S$ avg + $\Sigma\lambda_{DD}$ avg + $\Sigma\lambda_{DU}$ avg)
When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

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

Where:

$\lambda_{S\,=}$ Fail Safe

$\lambda_{DD\,=}$ Fail Dangerous Detected

$\lambda_{DU\,=}$ Fail Dangerous Undetected

As the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*are only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 [V1] 9276/10-21-25-00*

The FMEDA carried out on the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00*[V1] under the assumptions described in section 4.2.3 and the definitions given in section 4.1 leads to the following failure rates:

Table 5: [V1] 9276/10-21-25-00*– failure rates per IEC 61508:2010

Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**50**
Dangerous Detected (λ_{DD})	**0**
Dangerous Undetected (λ_{DU})	**0**
No effect	70
Total failure rate (safety function)	**50**
SFF [8]	**100%**
DC	**0%**
SIL AC [9]	**SIL 3**

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

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL 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.

4.3.2 [V2] 9276/10-21-**-00* and 9276/10-24-**-00*

The FMEDA carried out on the Digital Outputs Loop Powered 9276/10-21-**-00* and 9276/10-24-**-00* [V2] under the assumptions described in section 4.2.3 and the definitions given in section 4.1 leads to the following failure rates:

Table 6: [V2] 9276/10-21--00* and 9276/10-24-**-00*– failure rates per IEC 61508:2010**

Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**50**
Dangerous Detected (λ_{DD})	**0**
Dangerous Undetected (λ_{DU})	**0**
No effect	73
Total failure rate (safety function)	**50**
SFF [10]	**100%**
DC	**0%**
SIL AC [11]	**SIL 3**

[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.

5 Terms and Definitions

DC	Diagnostic Coverage of dangerous failures (DC = λ_{DD} / (λ_{DD} + λ_{DU}))
FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance 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.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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.
Type A element	"Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2
T[Proof]	Proof Test Interval

6 Status of the document

6.1 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.

6.2 Releases

Version History:	V1, R0:	Editorial review findings incorporated; October 8, 2018
	V0, R1:	Initial version; September 27, 2018
Authors:	Jürgen Hochhaus	
Review:	V0R1:	Sabine Reistle R. STAHL Schaltgeräte GmbH Stephan Aschenbrenner, *exida*
Release status:	Released	

6.3 Release Signatures

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

J. Hochhaus

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

Appendix A: 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 [N4] and [N5].

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 [N6].

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 supplier. Those supplier 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 supplier is responsible for the first variable. Most suppliers use the *exida* FMEDA technique that 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^{TM} software considers all these variables and provides an effective means to calculate PFD$_{AVG}$ for any given set of variables.

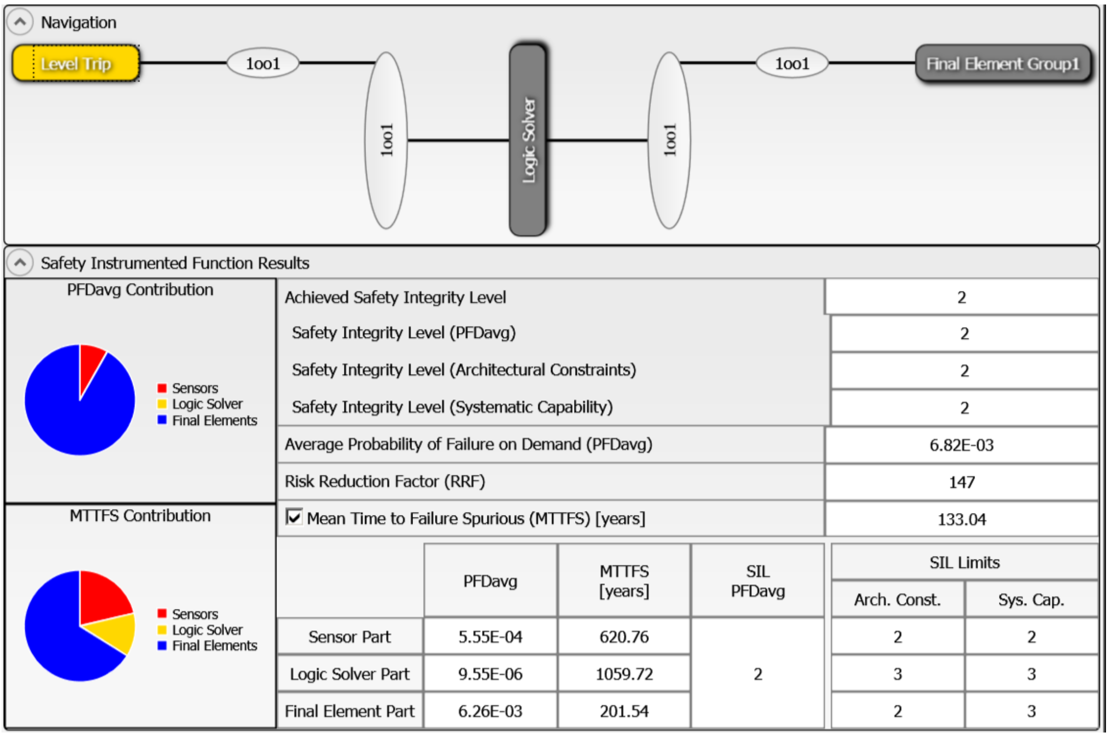
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC 61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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).



Safety Instrumented Function Results

Achieved Safety Integrity Level	2
Safety Integrity Level (PFDavg)	2
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	6.82E-03
Risk Reduction Factor (RRF)	147
☑ Mean Time to Failure Spurious (MTTFS) [years]	133.04

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	5.55E-04	620.76	2	2	2
Logic Solver Part	9.55E-06	1059.72		3	3
Final Element Part	6.26E-03	201.54		2	3

Figure 2: 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 3.

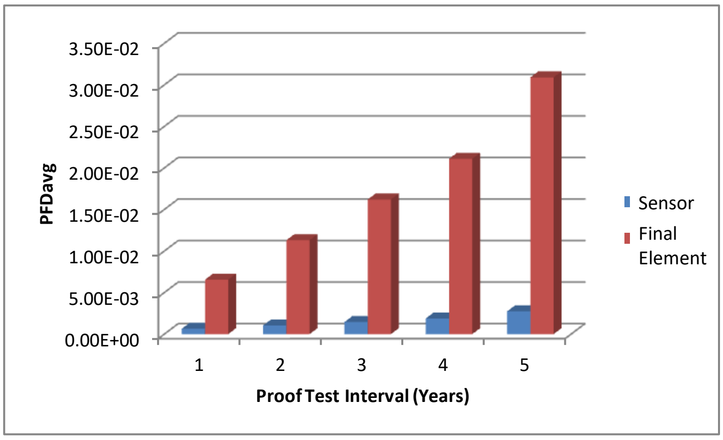
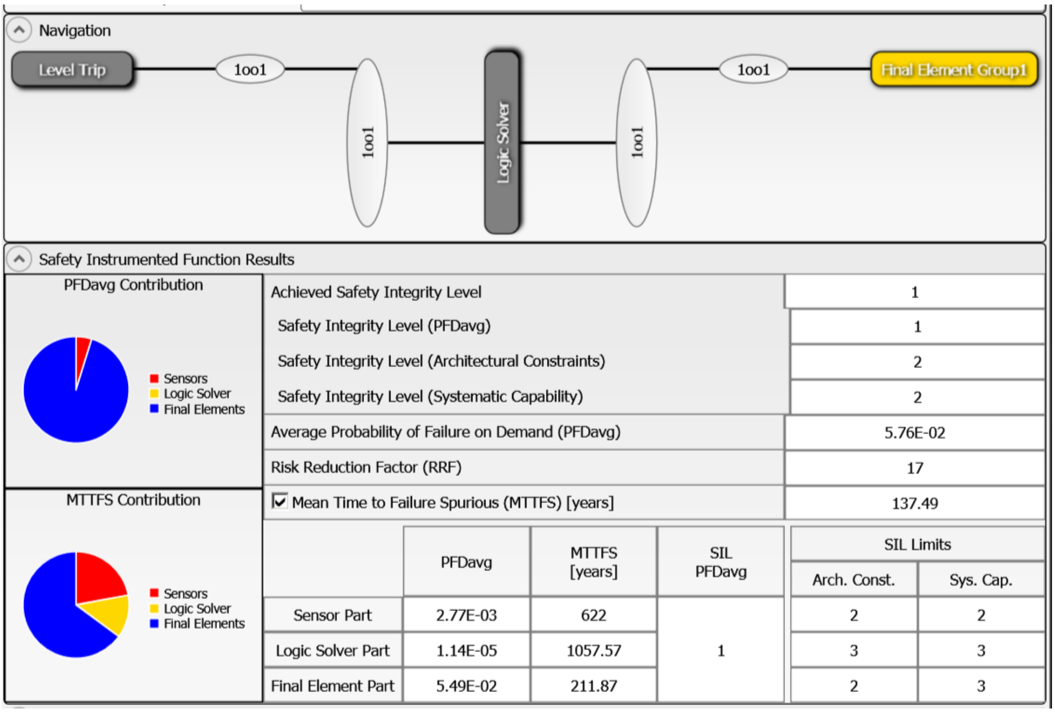


Figure 3: PFD_{AVG} versus Proof Test Interval

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 4).



Achieved Safety Integrity Level	1
Safety Integrity Level (PFDavg)	1
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	5.76E-02
Risk Reduction Factor (RRF)	17
☑ Mean Time to Failure Spurious (MTTFS) [years]	137.49

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	2.77E-03	622	1	2	2
Logic Solver Part	1.14E-05	1057.57		3	3
Final Element Part	5.49E-02	211.87		2	3

Figure 4: 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.