# Failure Modes, Effects and Diagnostic Analysis

Project:
Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**

Customer:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: Stahl Q18-07-006
Report No.: Stahl Q18-07-006 R033
Version V1, Revision R1; October, 2018

Jürgen Hochhaus

## Management summary

This report summarizes the results of the hardware assessment carried out on the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** with hardware version as listed in the drawings referenced in section 2.5.1. Table 1 gives an overview of the considered variants and Table 2 shows the considered configurations.

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 variants**

| Variant | Description |
|---|---|
| 9270/11-16-14s | One input channel module with one output relay and screw terminals. |
| 9270/11-16-14k | One input channel module with one output relay and spring pressure clamps. |
| 9270/11-17-15s | One input channel module with two output relays and screw terminals. |
| 9270/11-17-15k | One input channel module with two output relays and spring pressure clamps. |
| 9270/21-17-14s | Two input channel module with two output relays and screw terminals. |
| 9270/21-17-14k | Two input channel module with two output relays and spring pressure clamps. |

All variants can be configured to have standard (“N”) or inverting (“I”) switching behavior.

The performed analysis showed that the one input, one output relay variant can be considered to show the worst-case results. Therefore, this report displays the results based on the numbers of this version.

**Table 2: List of considered configurations**

| Configuration | Signal phase | Relay Contact | Relay Load |
|---|---|---|---|
| C1 | Normal | Normally Open | Stress region IV, up to 250V AC / 2A or 30V DC / 2A resistive load or slightly inductive (cos φ > 0,95) |
| C2 | Normal | Normally Open | Stress region II, up to 120V DC / 0,2 A resistive load or slightly inductive (cos φ > 0,95) |
| C3 | Inverted | Normally Open | Stress region IV, up to 250V AC / 2A or 30V DC / 2A resistive load or slightly inductive (cos φ > 0,95) |
| C4 | Inverted | Normally Open | Stress region II, up to 120V DC / 0,2 A resistive load or slightly inductive (cos φ > 0,95) |
| C5 | Normal | Normally Closed | Stress region[1] IV, up to 250V AC / 2A or 30V DC / 2A resistive load or slightly inductive (cos φ > 0,95) |
| C6 | Normal | Normally Closed | Stress region II, up to 120V DC / 0,2 A resistive load or slightly inductive (cos φ > 0,95) |
| C7 | Inverted | Normally Closed | Stress region IV, up to 250V AC / 2A or 30V DC / 2A resistive load or slightly inductive (cos φ > 0,95) |
| C8 | Inverted | Normally Closed | Stress region II, up to 120V DC / 0,2 A resistive load or slightly inductive (cos φ > 0,95) |

For safety applications only the described variants of the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**.

The Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** can be considered to be Type A[2] elements with a hardware fault tolerance of 0.

The following tables show how the above stated requirements are fulfilled for the considered Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**.

[1] Stress regions according to SN29500-7:2005-11

[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.

**Table 3: 9270/*1-16-1** and 9270/*1-17-1**, Normally Open Configurations C1-C4**

| Failure category | IEC 61508:2010 Failure rates (in FIT) | | | |
|---|---|---|---|---|
| | C1 Normal | C2 Normal | C3 Inverted | C4 Inverted |
| **Safe Detected ($\lambda_{SD}$)** | **6** | **6** | **7** | **7** |
| **Safe Undetected ($\lambda_{SU}$)** | **165** | **230** | **168** | **233** |
| **Dangerous Detected ($\lambda_{DD}$)** | **7** | **7** | **6** | **6** |
| **Dangerous Undetected ($\lambda_{DU}$)** | **55** | **90** | **55** | **90** |
| No effect | 87 | 87 | 87 | 87 |
| **Total failure rate (safety function)** | **233** | **333** | **236** | **336** |
| **SFF** [3] | **76%** | **72%** | **76%** | **73%** |
| **DC** | **9%** | **7%** | **9%** | **6%** |
| **SIL AC** [4] | **SIL 2** | **SIL 2** | **SIL 2** | **SIL 2** |

[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 4: 9270/*1-16-1** and 9270/*1-17-1**, Normally Closed Configurations C5-C8**

| Failure category | IEC 61508:2010 Failure rates (in FIT) | | | |
|---|---|---|---|---|
| | C5 Normal | C6 Normal | C7 Inverted | C8 Inverted |
| **Safe Detected ($\lambda_{SD}$)** | **6** | **6** | **7** | **7** |
| **Safe Undetected ($\lambda_{SU}$)** | **155** | **210** | **158** | **213** |
| **Dangerous Detected ($\lambda_{DD}$)** | **7** | **7** | **6** | **6** |
| **Dangerous Undetected ($\lambda_{DU}$)** | **65** | **110** | **65** | **110** |
| No effect | 87 | 87 | 87 | 87 |
| **Total failure rate (safety function)** | **233** | **333** | **236** | **336** |
| **SFF** [5] | **72%** | **67%** | **72%** | **67%** |
| **DC** | **9%** | **6%** | **9%** | **5%** |
| **SIL AC** [6] | **SIL 2** | **SIL 2** | **SIL 2** | **SIL 2** |

The failure rates are valid for the useful life of the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** (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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 cybersecurity, and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion unit operating hours of field failure data.

## 2.2 Roles of the parties involved

| | |
|---|---|
| R. STAHL Schaltgeräte GmbH | Supplier of the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**. |
| *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<br>SN 29500-1 H1:07.2013<br>SN 29500-2:09.2010<br>SN 29500-3:06.2009<br>SN 29500-4:03.2004<br>SN 29500-5:06.2004<br>SN 29500-7:11.2005<br>SN 29500-9:11.2005<br>SN 29500-10:12.2005<br>SN 29500-11:07.2013<br>SN 29500-12:02.2008<br>SN 29500-15:07.2009<br>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 |
| [T2] | exSILentia Ultimate V3.3.0.903 | SIL Verification Tool |

## 2.5 Reference documents

### 2.5.1 Documentation provided by the customer

| | | |
|---|---|---|
| [D1] | Kurzumschreibung von FMEDA-Berichten | Mail from Sabine Reistle, dated 19.6.2018. showing the device variant names. |
| [D2] | Einverständniserklärung_Nam-RO_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 and reviewed by *exida*

| | |
|---|---|
| [R1] | FMEDA files listed in 07/06-39 R005 |

# 3 Product Description

The Modules 9270/*1-16-1** and 9270/*1-17-1** are switching repeaters. They have intrinsically safe input circuits and are designed for the operation of proximity switches with Namur behaviour.

The Module 9270/11-16-14s is the one channel version, which is able to operate only one proximity switch. The module has only one relay output.

The module 9270/11-17-15s is as well a one input channel version for the connection of a single proximity switch, but it has two independent relay outputs.

The module 9270/21-17-14s is the two input channel version for the connection of two proximity switches with two relay outputs. The two intrinsically safe circuits are not galvanically separated. The signals from the proximity switches will be transferred via relays to the plc.

All three version are available with screw terminals and with spring pressure clamps. The spring pressure variants are labelled 9270/*1-16-1*k and 9270/*1-17-1*k.

The switching repeaters are supplied with a galvanic isolation between input and output circuit and between input circuit and supply.

The modules are supplied with a circuit for the detection of line faults, which can be switched on or off depending on the application. Detected line faults are available as an additional signal on contacts in the bottom of the module. The module can be supplied via other contacts in this area alternatively.

The switching behaviour - standard (“N”) or inverted (“I”) - of the modules can be selected via DIP - switches in their front.

The switching repeaters are designed for an operating voltage range of 20 to 30 V and an operating temperature range of -20 to 60 °C.

See Table 1 and Table 2 for the analyzed modules and configurations.

The modules can be considered to be Type A[7] elements with a hardware fault tolerance of 0.

The safety function of the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** are defined as follows:

The output relay is de-energized according to the input signal and the configuration (normal or inverted mode).

[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.

The following figures show the hardware structure of the switching repeaters.

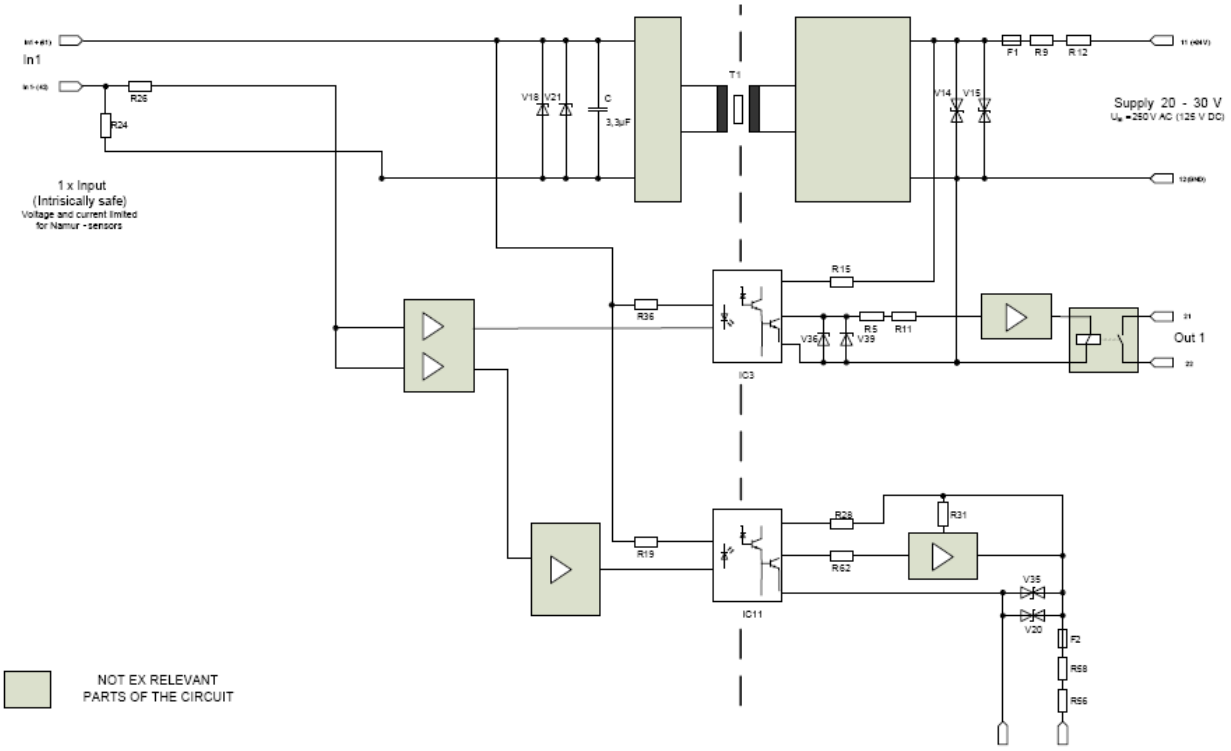



**Figure 1: 9270/11-16-14***

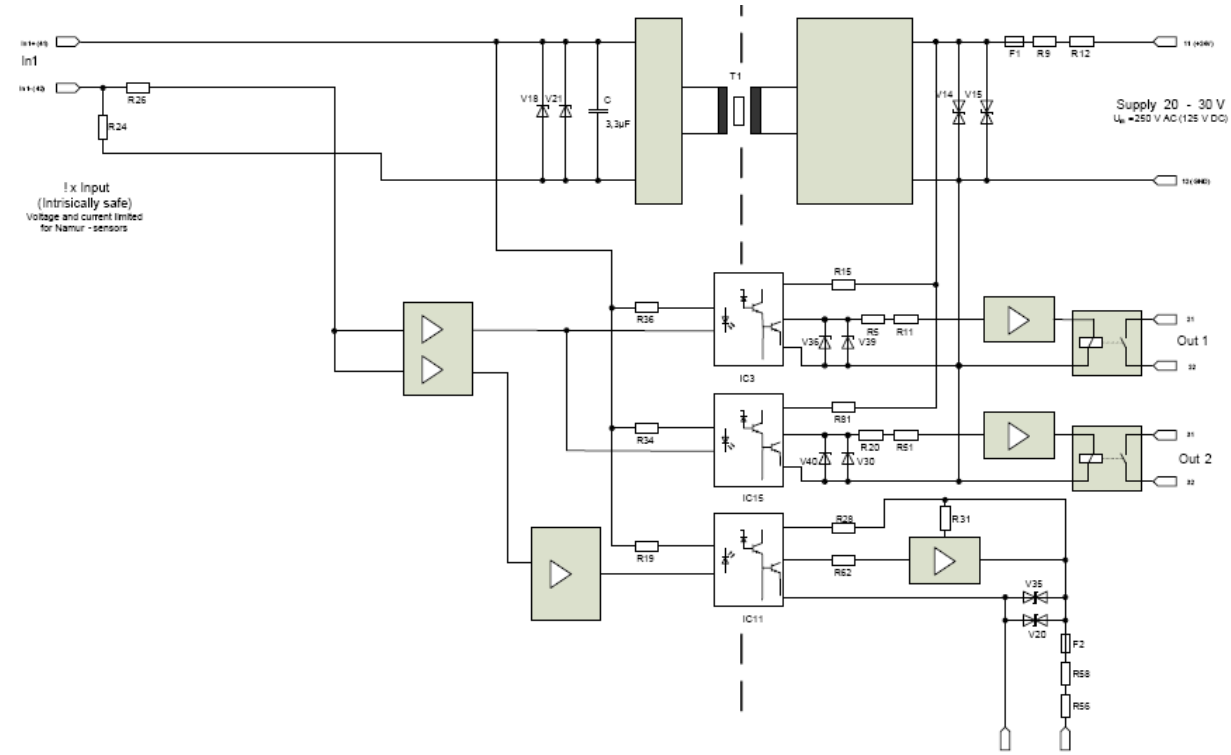



**Figure 2: 9270/11-17-15***

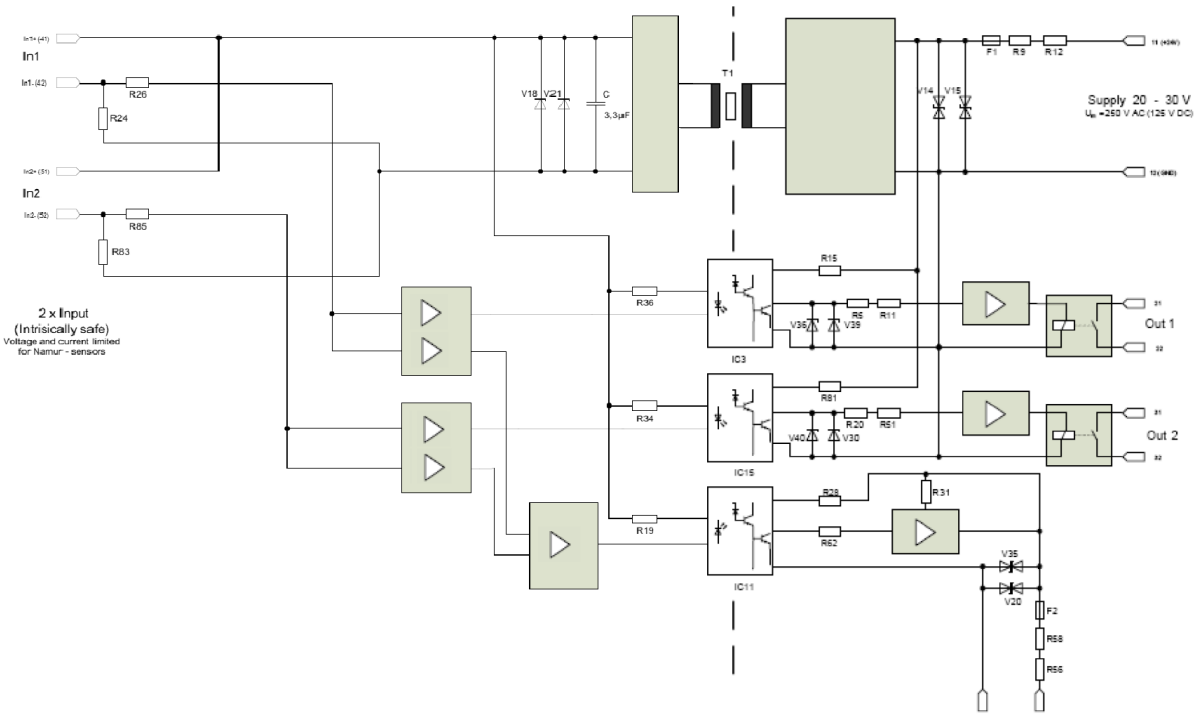



**Figure 3: 9270/21-17-14***

# 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 [R1].

## 4.1 Description of the failure categories

In order to judge the failure behavior of the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**, the following definitions for the failure of the products were considered.

| | |
|---|---|
| Fail-Safe State | Relay Output<br>The fail-safe state is defined as the relay output being de-energized. |
| Safe | A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:<br>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,<br>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:<br>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,<br>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™ 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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**.

- 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.
- 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 40ms.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 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 output channels 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. Different protection layers using the signal doubling or two channels shall not be considered to be independent.
- The line monitoring is activated.
- The devices are operated in low or high demand mode.
- The error message output relay configuration is not used for safety functions.
- All components that are not part of the safety function (e.g. alarm output) and cannot influence the safety function (feedback immune) are excluded.

## 4.3 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:

$\lambda_S =$ Fail Safe

$\lambda_{DD} =$ Fail Dangerous Detected

$\lambda_{DU} =$ Fail Dangerous Undetected

As the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** is only one part of an element, the architectural constraints should be determined for the entire sensor element.

### 4.3.1 9270/*1-16-1** and 9270/*1-17-1**, Normally Open Configurations

The FMEDA carried out on the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**, Configuration C1 to C4 under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.3 leads to the following failure rates.

**Table 5: 9270/*1-16-1** and 9270/*1-17-1**, Normally Open Configurations C1-C4**

| **Failure category** | **IEC 61508:2010 Failure rates (in FIT)** | | | |
|---|---|---|---|---|
| | **C1 Normal** | **C2 Normal** | **C3 Inverted** | **C4 Inverted** |
| **Safe Detected ($\lambda_{SD}$)** | **6** | **6** | **7** | **7** |
| **Safe Undetected ($\lambda_{SU}$)** | **165** | **230** | **168** | **233** |
| **Dangerous Detected ($\lambda_{DD}$)** | **7** | **7** | **6** | **6** |
| **Dangerous Undetected ($\lambda_{DU}$)** | **55** | **90** | **55** | **90** |
| No effect | 87 | 87 | 87 | 87 |
| **Total failure rate (safety function)** | **233** | **333** | **236** | **336** |
| **SFF** [8] | **76%** | **72%** | **76%** | **73%** |
| **DC** | **9%** | **7%** | **9%** | **6%** |
| **SIL AC** [9] | **SIL 2** | **SIL 2** | **SIL 2** | **SIL 2** |

[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 9270/*1-16-1** and 9270/*1-17-1**, Normally Closed Configurations

The FMEDA carried out on the Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1**, Configuration C5 to C8 under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.3 leads to the following failure rates.

**Table 6: 9270/*1-16-1** and 9270/*1-17-1**, Normally Closed Configurations C5-C8**

| Failure category | IEC 61508:2010 Failure rates (in FIT) | | | |
|---|---|---|---|---|
| | C5 Normal | C6 Normal | C7 Inverted | C8 Inverted |
| **Safe Detected ($\lambda_{SD}$)** | **6** | **6** | **7** | **7** |
| **Safe Undetected ($\lambda_{SU}$)** | **155** | **210** | **158** | **213** |
| **Dangerous Detected ($\lambda_{DD}$)** | **7** | **7** | **6** | **6** |
| **Dangerous Undetected ($\lambda_{DU}$)** | **65** | **110** | **65** | **110** |
| No effect | 87 | 87 | 87 | 87 |
| **Total failure rate (safety function)** | **233** | **333** | **236** | **336** |
| **SFF** [10] | **72%** | **67%** | **72%** | **67%** |
| **DC** | **9%** | **6%** | **9%** | **5%** |
| **SIL AC** [11] | **SIL 2** | **SIL 2** | **SIL 2** | **SIL 2** |

[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 Using the FMEDA results

Using the failure rate data displayed in section 4.3, 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 supplier. Those supplier 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 suppliers 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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** 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 Example $PFD_{AVG}$ / PFH calculation

An average Probability of Failure on Demand ($PFD_{AVG}$) calculation is performed for a single (1oo1) Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.3.2. 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 95% (see Appendix B).

**Table 7: values example for 9270/*1-16-1** and 9270/*1-17-1** configuration C6**

| PFH [12] | T[Proof] | |
|---|---|---|
| | 1 year | 3 years |
| PFH = 1.1E-07 1/h | $PFD_{AVG}$ = 6.97 E-04 | $PFD_{AVG}$ = 1.5 E-03 |

[12] The PFH value is based on a worst-case diagnostic test rate and a reaction time of 40ms. The ratio of the diagnostic test rate to the demand rate shall equal or exceed 100.

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 Switching Repeaters 9270/*1-16-1** and 9270/*1-17-1** are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 15% 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 15% of the allowed range, i.e. to be better than or equal to 1.5E-03 or 1.50E-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.

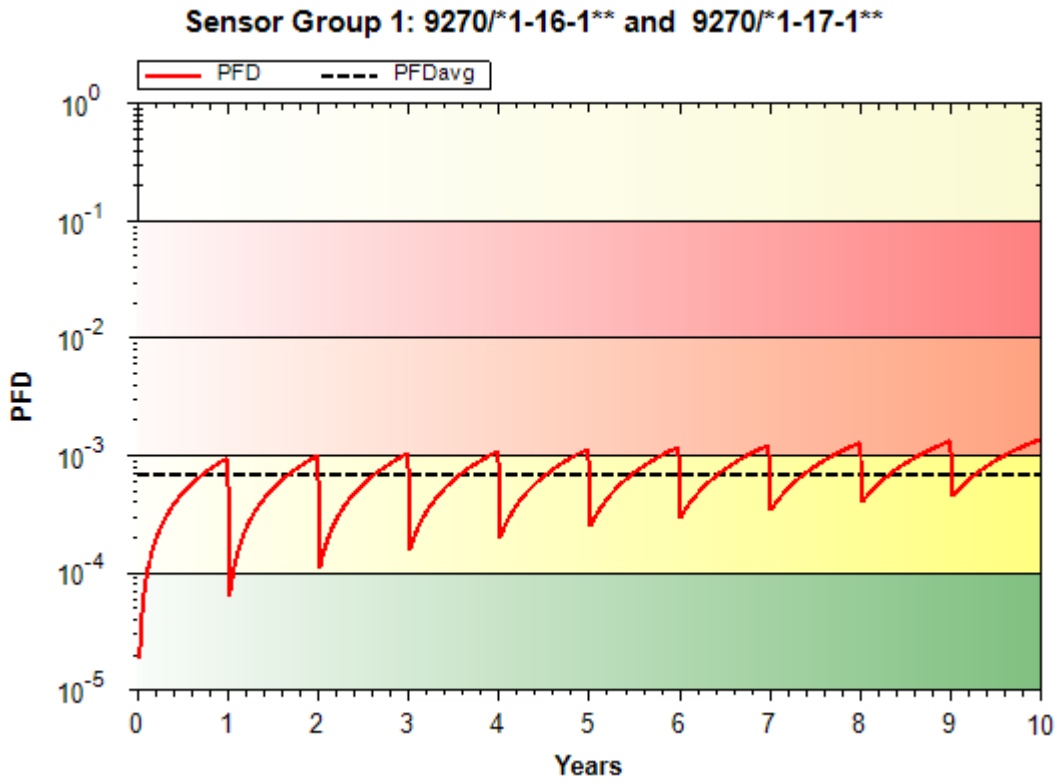



**Figure 4: $PFD_{AVG}(t)$**

# 6 Terms and Definitions

| | |
|---|---|
| Automatic Diagnostics | Tests performed on line internally by the device or, if specified, externally by another device without manual intervention. |
| DC | Diagnostic Coverage of dangerous failures (DC = $\lambda_{DD}$ / ($\lambda_{DD}$ + $\lambda_{DU}$)) |
| FIT | Failure In Time (1x$10^{-9}$ failures per hour) |
| FMEDA | Failure Modes, Effects, and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance<br>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. |
| Continuous mode | Mode, where the safety function retains the EUC in a safe state as part of normal operation |
| 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<br>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.<br>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 |

# 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.

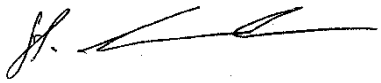
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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: | V1, R1: | Editorial review findings incorporated; October 24, 2018 |
| | 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 | |

## 7.3 Release Signatures



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

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

# 8 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 assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[13] 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.

This assumption of a constant failure rate is based on the bathtub curve. 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 8 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 8: Useful lifetime of components with reduced useful lifetime contributing to $\lambda_{du}$**

| Type | Useful life |
|---|---|
| Relay | 200000 at 24V, 1A; Cos phi = 1,<br>25°C ambient temperature |
| Opto-coupler | More than 10 years |

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 and continuous mode applications the relays can be a limiting factor and have to be considered in the useful lifetime assumption.

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.

# Appendix B: Proof tests to detect 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 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.

A suggested proof test consists of the following steps, as described Table 9.

**Table 9 Steps for Proof Test**

| Step | Action |
|---|---|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip. |
| 2. | Provide appropriate input signals to the interface modules and verify the expected signal on the output. |
| 3. | Verify if the line monitoring (line fault detection) is working. |
| 4. | Remove the bypass and otherwise restore normal operation. |

This test will detect 95% of possible “du” failures.

## 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 [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 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 5).

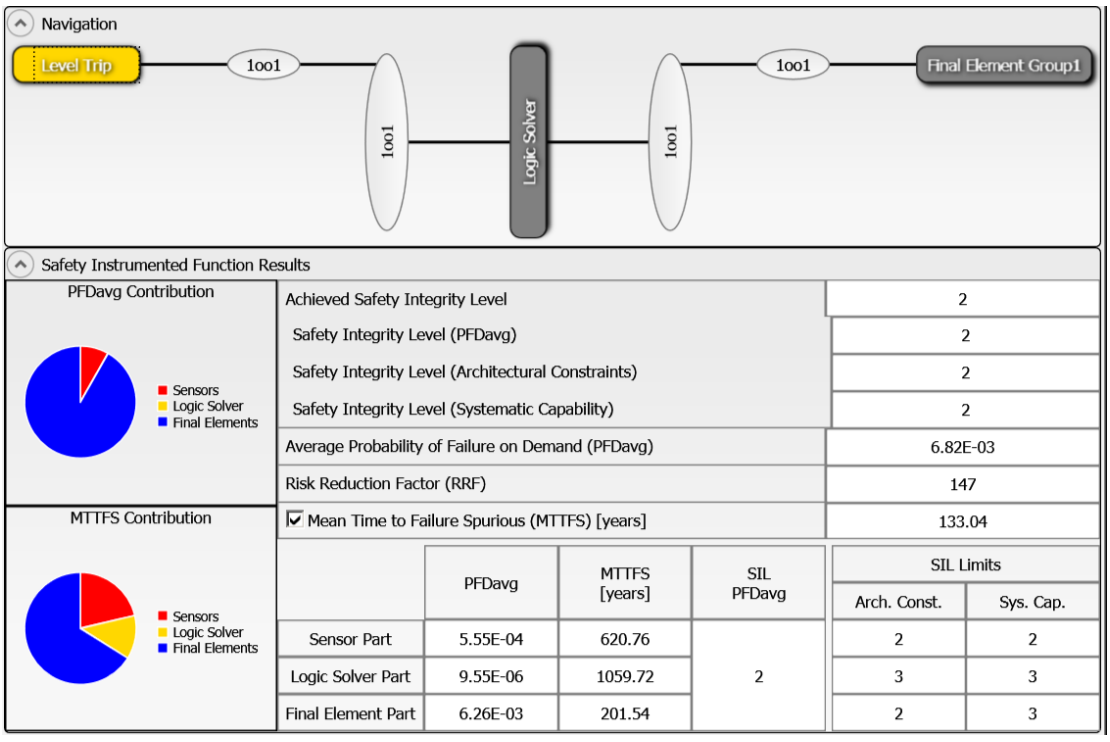


**Figure 5: exSILentia results for idealistic variables**

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

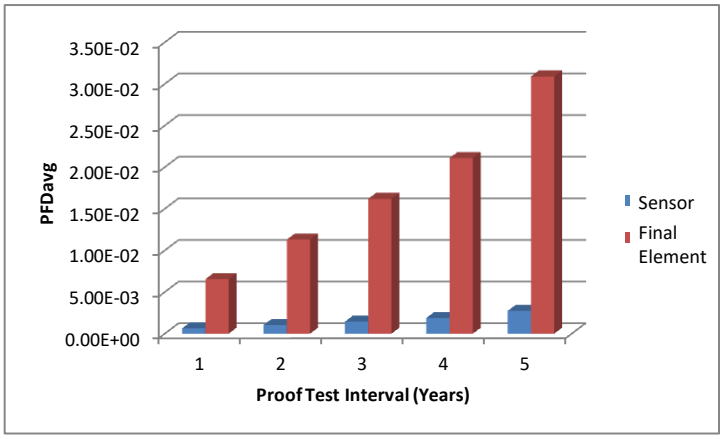



**Figure 6: $PFD_{AVG}$ versus Proof Test Interval**

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).

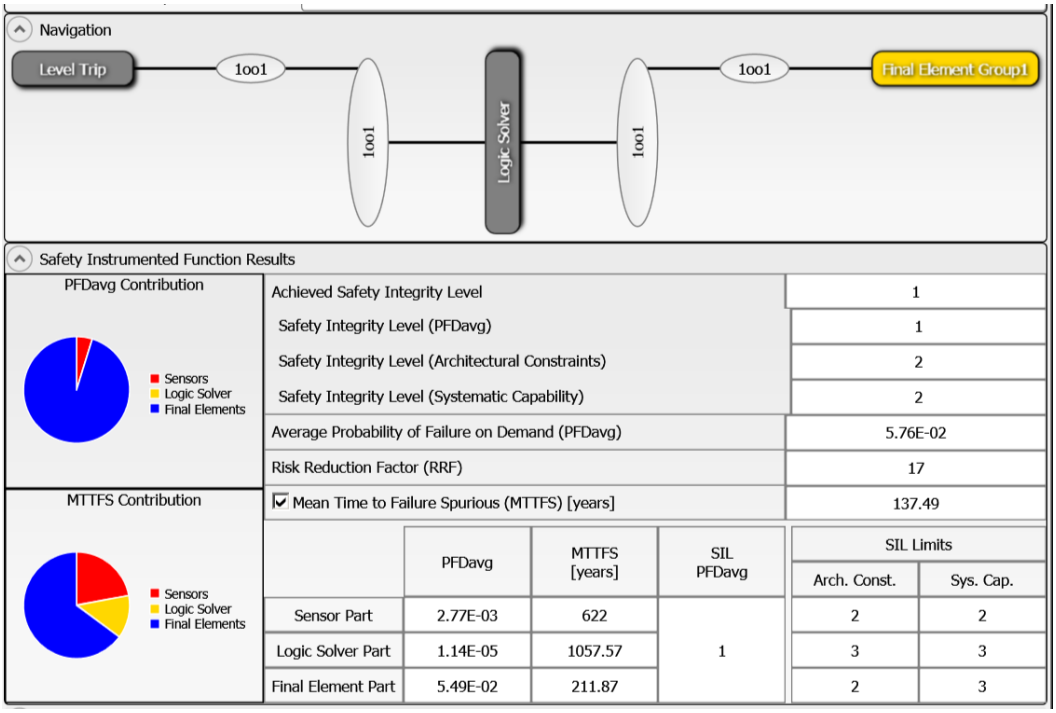



**Figure 7: exSILentia results with realistic variables**

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