



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

Contact elements Type 8082 and Type 8208  
with or without 8602 actuator

Customer:

R. STAHL Schaltgeräte GmbH  
Waldenburg  
Germany

Contract No.: Stahl 04/11-05

Report No.: Stahl 04/11-05 R007

Version V2, Revision R0, August 2015

Stephan Aschenbrenner

### **R. STAHL remark:**

Report is just valid for R. STAHL actuator types  
8602/3-006-\* - Mushroom stay-put button with key,  
8602/3-009-\* - Mushroom stay-put button with key EM-STOP,  
8602/3-010-\* - Mushroom stay-put button EM-STOP or  
8602/3-012-\* - Mushroom stay-put button Black  
in combination with  
type 8082 Contact Elements or  
type 8208 Control unit

## Management summary

This report summarizes the results of the hardware assessment carried out on the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator in the version as shown in the referred mechanical drawings (see section 2.4.1).

The internal resistors are needed for the lead breakage and short circuit detection. As a short circuit can be excluded for metal film resistors only open circuit and drift of the resistors have to be assumed. These failure modes, however, have either no effect on the safety function or do lead to unintended lead breakage detection. The failure rates listed below are without resistors as this application represents the worst-case.

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

The contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator can be considered to be Type A<sup>1</sup> elements with a hardware fault tolerance of 0.

*exida* did a quantitative analysis of the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator to calculate the failure rates using *exida*'s component database (see [N2]) for the different mechanical components.

The following tables show how the above stated requirements are fulfilled.

---

<sup>1</sup> Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Contact element type 8082 – Failure rates according to IEC 61508:2010

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	10
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	1

<b>Total failure rate (safety function)</b>	<b>11</b>
---	-----------

No effect	18
-----------	----

<b>SFF <sup>2</sup></b>	<b>90%</b>
-------------------------	------------

<b>SIL AC <sup>3</sup></b>	<b>SIL3</b>
----------------------------	-------------

<sup>2</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>3</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

Contact element type 8208 – Failure rates according to IEC 61508:2010

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	0

<b>Total failure rate (safety function)</b>	<b>18</b>
---	-----------

No effect	9
-----------	---

<b>SFF <sup>4</sup></b>	<b>100%</b>
-------------------------	-------------

<b>SIL AC <sup>5</sup></b>	<b>SIL3</b>
----------------------------	-------------

<sup>4</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>5</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

**Fail safe state 1: Open contact, non-latching**

**Contact element 8082 with 8602 actuator – Failure rates according to IEC 61508:2010**

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	1

<b>Total failure rate (safety function)</b>	<b>19</b>
---	-----------

No effect	80
-----------	----

<b>SFF <sup>6</sup></b>	<b>99%</b>
-------------------------	------------

<b>SIL AC <sup>7</sup></b>	<b>SIL3</b>
----------------------------	-------------

<sup>6</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>7</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

**Contact element 8208 with 8602 actuator – Failure rates according to IEC 61508:2010**

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	26
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	0

<b>Total failure rate (safety function)</b>	<b>26</b>
---	-----------

No effect	71
-----------	----

<b>SFF<sup>8</sup></b>	<b>100%</b>
------------------------	-------------

<b>SIL AC<sup>9</sup></b>	<b>SIL3</b>
---------------------------	-------------

<sup>8</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>9</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

**Fail safe state 2: Open Contact, Latching**

**Contact element 8082 with 8602 actuator – Failure rates according to IEC 61508:2010**

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	4

<b>Total failure rate (safety function)</b>	<b>22</b>
---	-----------

No effect	78
-----------	----

<b>SFF <sup>10</sup></b>	<b>84%</b>
--------------------------	------------

<b>SIL AC <sup>11</sup></b>	<b>SIL2</b>
-----------------------------	-------------

<sup>10</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>11</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD<sub>AVG</sub> / PFH values.

**Contact element 8208 with 8602 actuator – Failure rates according to IEC 61508:2010**

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	26
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	3

<b>Total failure rate (safety function)</b>	<b>29</b>
---	-----------

No effect	68
-----------	----

<b>SFF<sup>12</sup></b>	<b>82%</b>
-------------------------	------------

<b>SIL AC<sup>13</sup></b>	<b>SIL2</b>
----------------------------	-------------

The failure rates are valid for the useful life of the considered devices (see Appendix A).

<sup>12</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>13</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.



## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	10
2 Project management .....	11
2.1 <i>exida</i> .....	11
2.2 Roles of the parties involved .....	11
2.3 Standards / Literature used .....	11
2.4 Reference documents .....	12
2.4.1 Documentation provided by R. Stahl Schaltgeräte GmbH .....	12
2.4.2 Documentation generated by <i>exida</i> .....	12
3 Description of the analyzed modules .....	13
4 Failure Modes, Effects, and Diagnostic Analysis .....	15
4.1 Description of the failure categories .....	15
4.2 Methodology – FMEDA, Failure rates .....	16
4.2.1 FMEDA .....	16
4.2.2 Failure rates .....	16
4.2.3 Assumption .....	17
4.3 Results of the assessment .....	18
4.3.1 Fail-safe state 1 – Open contact, non-latching .....	19
4.3.2 Fail-safe state 2 – Open Contact, Latching .....	23
5 Terms and Definitions .....	25
6 Status of the document .....	26
6.1 Liability .....	26
6.2 Releases .....	26
6.3 Release Signatures .....	26
Appendix A: Impact of lifetime of critical components on the failure rate .....	27
Appendix B: Proof tests to reveal dangerous faults .....	28
B.1 Suggested proof test .....	28
Appendix C: <i>exida</i> Environmental Profiles .....	29
Appendix D: Determining Safety Integrity Level .....	30

## 1 Purpose and Scope

This document shall describe the results of the Failure Modes, Effects and Diagnostics Analysis (FMEDA) carried out on the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator in the version as shown in the referred mechanical drawings (see section 2.4.1).

The FMEDA builds the basis for an evaluation whether a sensor element, including the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508.

An FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

## 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 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 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 Manufacturer of the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator.

*exida* Performed the hardware assessment.

R. Stahl Schaltgeräte GmbH contracted *exida* in May 2015 with the update 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]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N3]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions
[N4]	ISA-TR96.05.01-200_; version B of February 2006	Draft technical report "Partial Stroke Testing For Block Valve Actuators in Safety Instrumented Systems Applications"
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3 <sup>rd</sup> edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, <a href="http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers">http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers</a>

[N7]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	<a href="http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design">http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design</a>
[N8]	Final Elements Chris O'Brien & Lindsey Bredemeyer, 2009	<i>exida</i> LLC., Final Elements & the IEC 61508 and IEC 61511 Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

## 2.4 Reference documents

### 2.4.1 Documentation provided by R. Stahl Schaltgeräte GmbH

[D1]	8082601300.pdf	Operating instructions contact element type 8082
[D2]	8082_Befehlstaster_CD60_E.pdf	Data sheet
[D3]	8208S870.pdf	Data sheet
[D4]	Datenblatt-8208-Kontaktelement1.pdf	Data sheet
[D5]	AW NOT-AUS SIL Betrachtung.msg of 15.03.05	Field data evaluation (operating hours, sold devices, returned devices)
[D6]	80_820_01_01_0.pdf	Mechanical drawing 8082 of 12.03.03
[D7]	86_020_10_08_0.pdf	Mechanical Drawing 8602 of 26.05.15
[D8]	86_020_09_08_0_für SIL-Betrachtung	Mechanical Drawing 8602/3
[D9]	86_020_10_08_0_für SIL Pilzsperr	Mechanical Drawing 8602/-010, 26.05.15
[D10]	Email of 26.04.05	Description of the lead breakage and short circuit detection via the internal resistors

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.

### 2.4.2 Documentation generated by *exida*

[R1]	FMEDA V6 8082 V2 R0.xls of 22.05.15
[R2]	FMEDA V6 8208 V2R0.xls of 22.05.15
[R3]	FMEDA V6 8602 V2R0.xls of 26.05.15
[R4]	FMEDA V6 8602 Verriegelung V2R0.xls of 26.05.15
[R5]	FMEDA V6 8082-8602 V2 R0.xls of 26.05.15
[R6]	FMEDA V6 8208-8602 V2 R0.xls of 26.05.15
[R7]	FMEDA V6 8082-8602 Verriegelung V2 R0.xls of 22.05.15
[R8]	FMEDA V6 8208-8602 Verriegelung V2 R0.xls of 26.05.15

### 3 Description of the analyzed modules

The contact elements type 8082 and type 8208 switch power, control and signal circuits.

The contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator can be considered to be Type A<sup>14</sup> elements with a hardware fault tolerance of 0.

Figure 1 and Figure 2 show the block diagram of the contact elements type 8082 and type 8208.

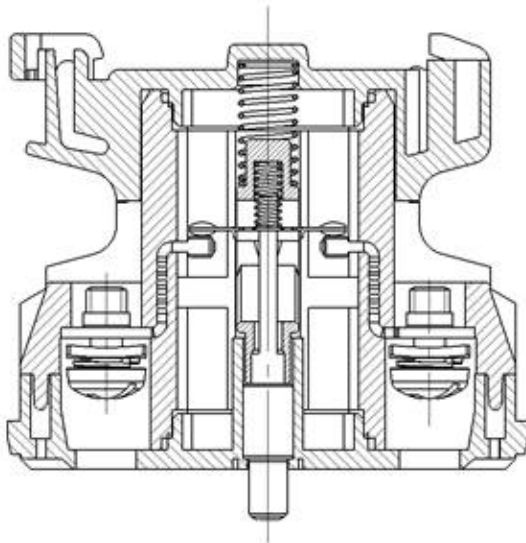


Figure 1: Block diagram of the contact element type 8082

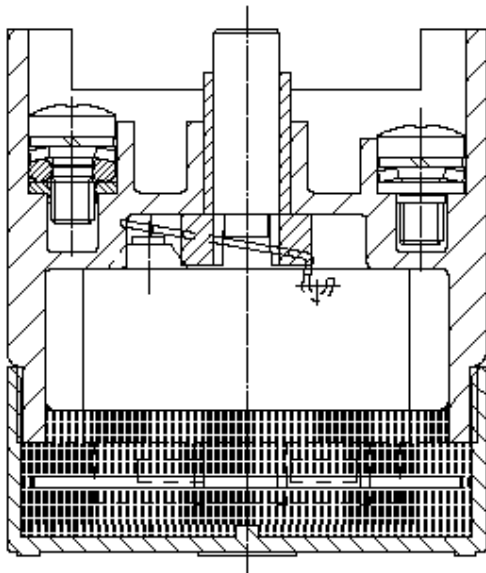
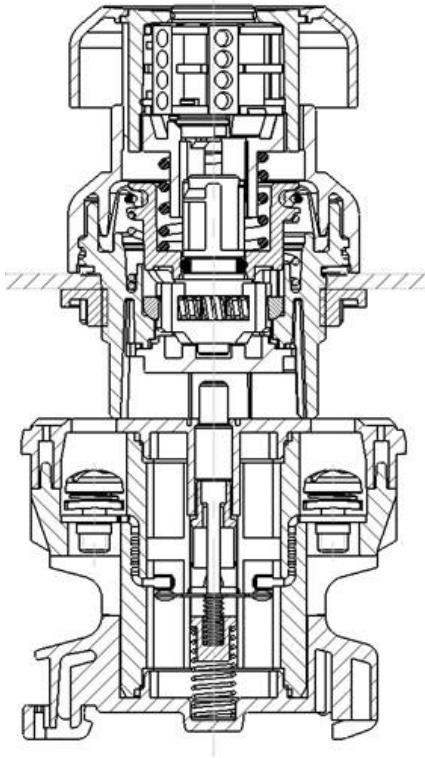


Figure 2: Block diagram of the contact element type 8208

---

<sup>14</sup> Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Figure 3 shows the block diagram of the contact element type 8082 with 8602 actuator.



**Figure 3: Block diagram of the contact element type 8082 with 8602 actuator**

## 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 [R7] to [R8].

### 4.1 Description of the failure categories

In order to judge the failure behavior of the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator, the following definitions for the failure of the product were considered.

Fail-Safe State 1	The fail-safe state is defined as the contact opens.
Fail-Safe State 2	The fail-safe state is defined as the contact opens and latches.
Fail Safe	<p>A safe failure (S) is defined as a failure that plays a part in implementing the safety function that:</p> <ul style="list-style-type: none"><li>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,</li><li>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.</li></ul>
Fail Dangerous	<p>A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:</p> <ul style="list-style-type: none"><li>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,</li><li>b) decreases the probability that the safety function operates correctly when required.</li></ul>
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed.
Dangerous Detected	Failure that is dangerous but is detected by external testing.
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.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a 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) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### 4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 3 (General Field Equipment), see Appendix C: *exida* Environmental Profiles. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by R. Stahl Schaltgeräte GmbH. 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, physical abuse, or problems due to intermittent instrument air or hydraulic fluid quality.

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. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C: *exida* Environmental Profiles. 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 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the contact elements type 8082 and type 8208 with or without 8602 actuator.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures caused by operational errors are site specific and therefore are not included.
- Failures caused by maintenance capability are site specific and therefore cannot be 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 mean time to restoration (MTTR) after a safe failure is 24 hours.
- Only the described variants are used for safety applications.
- All modules are operated in the low demand mode of operation.
- The contacts are protected with a fuse against contact welding.
- The contacts fulfill the direct opening action requirements of annex K of EN 60947-5-1.
- External power supply failure rates are not included.
- NC contacts with latching or non-latching operation with low cycle rate (ESD operation).
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 3 (General Field Equipment) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.

### 4.3 Results of the assessment

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

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

The 1<sub>H</sub> approach involves calculating the Safe Failure Fraction for the entire element.

The 2<sub>H</sub> 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<sub>H</sub> 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:

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

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

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

Where:

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

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

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

As the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator are only one part of a sensor element, the architectural constraints should be determined for the entire final element.

Using reliability data extracted from the *exida* Mechanical Component Reliability Handbook ([N2]) the following failure rates resulted from the FMEDA analysis of the contact elements type 8082 and type 8208 with and without internal resistors and with and without 8602 actuator.

### 4.3.1 Fail-safe state 1 – Open contact, non-latching

#### 4.3.1.1 Contact element type 8082

The FMECA carried out on the contact element type 8082 leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	10
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	1
<b>Total failure rate (safety function)</b>	<b>11</b>
No effect	18
<b>SFF <sup>15</sup></b>	<b>90%</b>
<b>SIL AC <sup>16</sup></b>	<b>SIL3</b>

<sup>15</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>16</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

#### 4.3.1.2 Contact element type 8208

The FMEDA carried out on the contact element type 8208 leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	0
<b>Total failure rate (safety function)</b>	<b>18</b>
No effect	9
<b>SFF <sup>17</sup></b>	<b>100%</b>
<b>SIL AC <sup>18</sup></b>	<b>SIL3</b>

<sup>17</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>18</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

#### 4.3.1.3 Contact element type 8082 combined with 8602 actuator

The FMEDA carried out on the contact element type 8082 combined with 8602 actuator leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	1
<b>Total failure rate (safety function)</b>	<b>19</b>
No effect	80
<b>SFF <sup>19</sup></b>	<b>99%</b>
<b>SIL AC <sup>20</sup></b>	<b>SIL3</b>

<sup>19</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>20</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

#### 4.3.1.4 Contact element type 8208 combined with 8602 actuator

The FMEDA carried out on the contact element type 8208 combined with 8602 actuator leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	26
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	0

<b>Total failure rate (safety function)</b>	<b>26</b>
---	-----------

No effect	71
-----------	----

<b>SFF <sup>21</sup></b>	<b>100%</b>
--------------------------	-------------

<b>SIL AC <sup>22</sup></b>	<b>SIL3</b>
-----------------------------	-------------

<sup>21</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>22</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

### 4.3.2 Fail-safe state 2 – Open Contact, Latching

#### 4.3.2.1 Contact element type 8082 combined with 8602 actuator

The FMEDA carried out on the contact element type 8082 combined with 8602 actuator leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	18
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	4
<b>Total failure rate (safety function)</b>	<b>22</b>
No effect	78
<b>SFF <sup>23</sup></b>	<b>84%</b>
<b>SIL AC <sup>24</sup></b>	<b>SIL2</b>

<sup>23</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>24</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.

#### 4.3.2.2 Contact element type 8208 combined with 8602 actuator

The FMEDA carried out on the contact element type 8208 combined with 8602 actuator leads under the assumptions described in section 4.2.3 to the following failure rates.

Failure category	Failure rates (in FIT) , Profile 3 data
Fail Safe ( $\lambda_{SD}$ )	0
Fail Safe ( $\lambda_{SU}$ )	26
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	3
<b>Total failure rate (safety function)</b>	<b>29</b>
No effect	68
<b>SFF <sup>25</sup></b>	<b>82%</b>
<b>SIL AC <sup>26</sup></b>	<b>SIL2</b>

<sup>25</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>26</sup> 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 devices have a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required  $PFD_{AVG}$  / PFH values.



## 5 Terms and Definitions

FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTTR	Mean Time To Restoration
$PFD_{AVG}$	Average Probability of Failure on Demand
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

## 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: V2R0: Updated to IEC 61508:2010 (2<sup>nd</sup> edition); August 17, 2015

V1, R1.0: External review comments integrated, May 20, 2005

V0, R2.0: Internal review comments integrated, April 4, 2005

V0, R1.0: Initial version; March 16, 2005

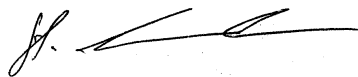
Authors: Stephan Aschenbrenner

Review: V0, R1.0: Rachel Amkreutz (*exida*); April 4, 2005

V0, R2.0: R. Stahl Schaltgeräte GmbH; April 25, 2005

Release status: Released to R. Stahl Schaltgeräte GmbH

### 6.3 Release Signatures

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

---

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

A handwritten signature in black ink, appearing to read "J. Hochhaus".

---

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

## Appendix A: Impact of lifetime of critical components on the failure rate

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<sup>27</sup> 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 1 shows 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 1: Useful lifetime of components contributing to  $\lambda_{du}$**

Name	Useful life
Contact element	1 x 10 <sup>6</sup> mechanical operations

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

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

---

<sup>27</sup> 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 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.

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

### B.1 Suggested proof test

A suggested proof test consists of the following steps, as described in Table 2.

**Table 2: Steps for a suggested proof test**

Step	Action
1	Bypass the safety function and take care that emergency stop is assured by other measures – <i>or</i> – Use maintenance / paused operation of system.
2	Inspect the device for any visible damage,
3	Operate the contact element.
4	Check if contacts are opened. Check if the open contact state is mechanically latched.
5	Restore the contacts to normal operation.

## Appendix C: *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
<b>Description (Electrical)</b>	Cabinet mounted/ Climate Controlled	Low Power Field Mounted  no self-heating	General Field Mounted  self-heating	Subsea	Offshore	N/A
<b>Description (Mechanical)</b>	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
<b>IEC 60654-1 Profile</b>	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
<b>Average Ambient Temperature</b>	30C	25C	25C	5C	25C	25C
<b>Average Internal Temperature</b>	60C	30C	45C	5C	45C	Process Fluid Temp.
<b>Daily Temperature Excursion (pk-pk)</b>	5C	25C	25C	0C	25C	N/A
<b>Seasonal Temperature Excursion (winter average vs. summer average)</b>	5C	40C	40C	2C	40C	N/A
<b>Exposed to Elements/Weather Conditions</b>	No	Yes	Yes	Yes	Yes	Yes
<b>Humidity<sup>28</sup></b>	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
<b>Shock<sup>29</sup></b>	10 g	15 g	15 g	15 g	15 g	N/A
<b>Vibration<sup>30</sup></b>	2 g	3 g	3 g	3 g	3 g	N/A
<b>Chemical Corrosion<sup>31</sup></b>	G2	G3	G3	G3	G3	Compatible Material
<b>Surge<sup>32</sup></b>						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
<b>EMI Susceptibility<sup>33</sup></b>						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
<b>ESD (Air)<sup>34</sup></b>	6kV	6kV	6kV	6kV	6kV	N/A

<sup>28</sup> Humidity rating per IEC 60068-2-3

<sup>29</sup> Shock rating per IEC 60068-2-27

<sup>30</sup> Vibration rating per IEC 60068-2-6

<sup>31</sup> Chemical Corrosion rating per ISA 71.04

<sup>32</sup> Surge rating per IEC 61000-4-5

<sup>33</sup> EMI Susceptibility rating per IEC 61000-4-3

<sup>34</sup> ESD (Air) rating per IEC 61000-4-2

## Appendix D: 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 [N5] and [N6].

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 develop 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 [N7].

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.

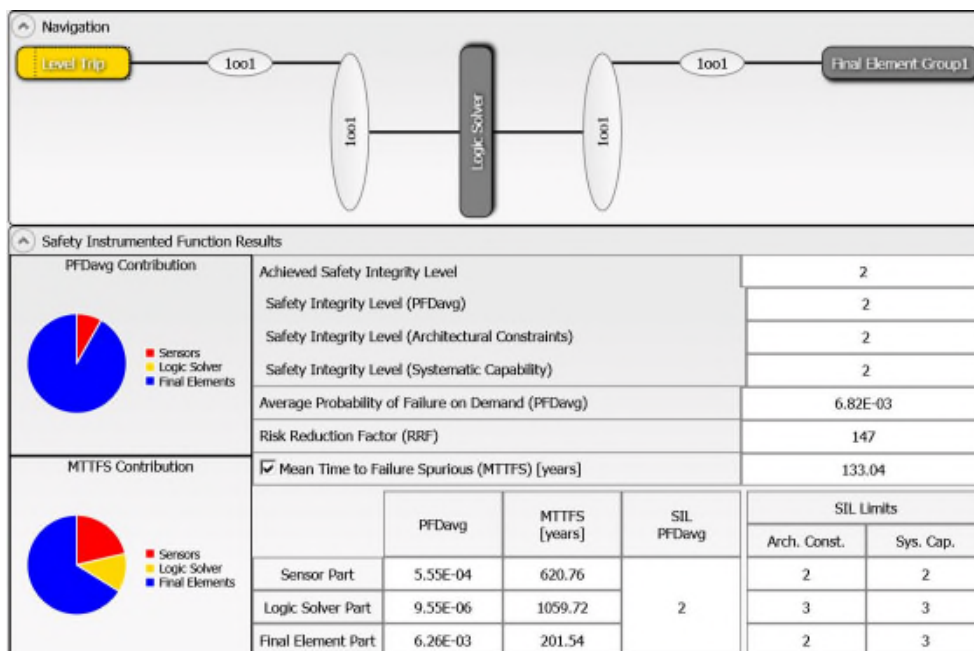
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 cover only the first four variables. IEC 61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions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

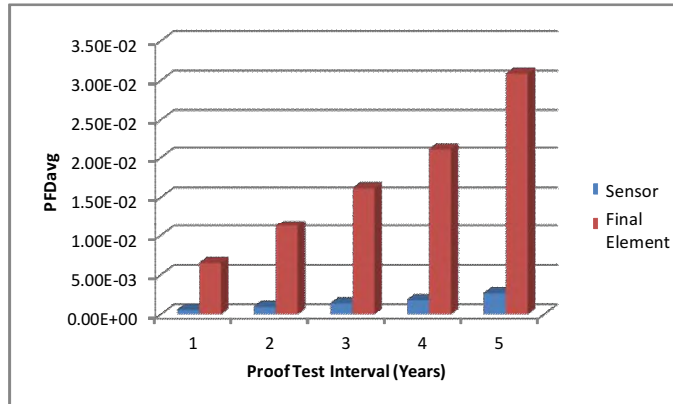
- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

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 4).



**Figure 4: 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 5.



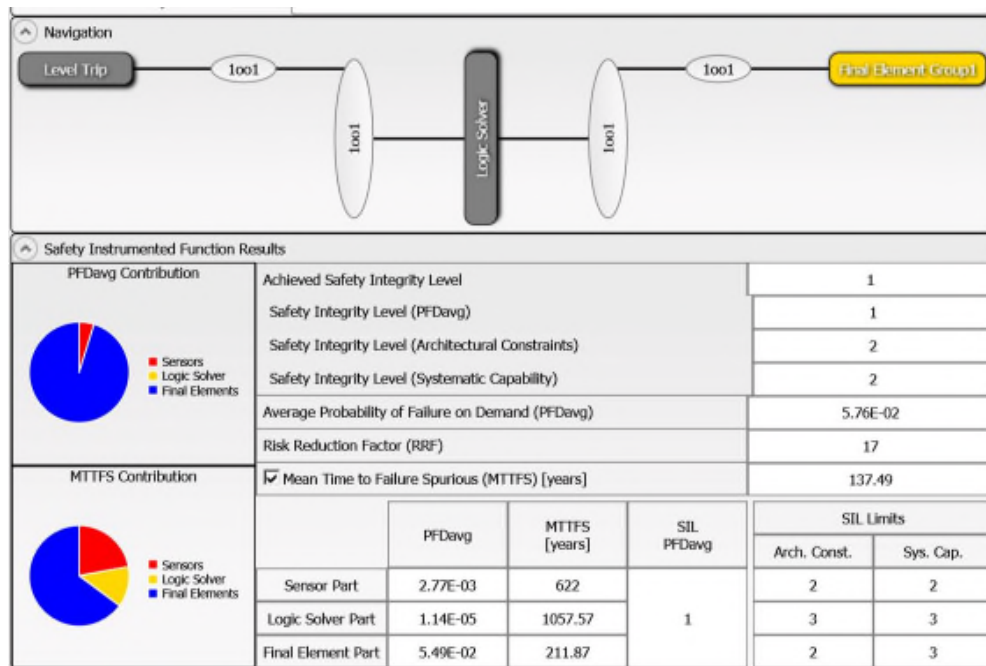
**Figure 5: PFD<sub>AVG</sub> versus Proof Test Interval**

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<sub>AVG</sub> for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD<sub>AVG</sub> contributions are Sensor PFD<sub>AVG</sub> = 2.77E-03, Logic Solver PFD<sub>AVG</sub> = 1.14E-05, and Final Element PFD<sub>AVG</sub> = 5.49E-02 (Figure 6).





**Figure 6: exSILentia results with realistic variables**

It is clear that PFD<sub>AVG</sub> results can change an entire SIL level or more when all critical variables are not used.