



Failure Modes, Effects and Diagnostic Analysis

Project:

Transmitter supply unit with limit values 9162

Company:

R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 13/12-013

Report No.: STAHL 13/12-013 R029

Version V1, Revision R2; January 2016

Jan Hettenbach

Management Summary

This report summarizes the results of the hardware assessment of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Transmitter supply unit 9162. All covered configurations are listed in Table 1 and all related drawings are referenced in section 2.4.1.

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 failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook for Profile 1.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.3.

The Transmitter supply unit 9162 can be considered to be a Type B¹ element with a hardware fault tolerance of 0. The failure rates according to IEC 61508:2010 for the Transmitter supply unit 9162 are listed in Table 2 to Table 4. The Transmitter supply unit 9162 is available in different configurations, which have no influence on the FMEDA assessment.

Table 1: Covered configurations of Transmitter supply unit 9162

| Types | Description of configuration |
|---|---|
| Hardware revision: C | |
| Software versions: V01-05, V01-06 | |
| Lead breakage detection: activated | |
| Short circuit detection: activated | |
| 9162 Current output configuration (Table 2) | Using the 4...20mA current output |
| 9162 dual relay output (Table 3) | Using both relay outputs in series as limit switch function to reduce risk of single faults in the output stage |
| 9162 single relay output (Table 4) | Using only one relay output for limit switch function |

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

Table 2: Failure rates of Transmitter supply unit 9162 in current output configuration

| <i>exida</i> Profile 1 | |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 416 |
| Fail Dangerous Detected (λ_{DD}) | 244 |
| Fail High (H) | 12 |
| Fail Low (L) | 160 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 27 |
| Fail Annunciation Undetected (λ_{AU}) | 89 |
| No effect | 251 |
| No part | 249 |
| Total failure rate (safety function) | 443 |
| Safe failure fraction (SFF)² | 93% |
| SIL AC³ | SIL2 |

² The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³ 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table 3: Failure rates of Transmitter supply unit 9162 in dual relay output configuration

| <i>exida</i> Profile 1 | |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 447 |
| Fail Dangerous Detected (λ_{DD}) | 344 |
| Fail High (H) | 0 |
| Fail Low (L) | 103 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 26 |
| Fail Annunciation Undetected (λ_{AU}) | 81 |
| No effect | 245 |
| No part | 238 |
| Total failure rate (safety function) | 473 |
| Safe failure fraction (SFF) ⁴ | 94% |
| SIL AC ⁵ | SIL2 |

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

⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table 4: Failure rates of Transmitter supply unit 9162 in one relay output configuration

| <i>exida</i> Profile 1 | |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 436 |
| Fail Dangerous Detected (λ_{DD}) | 333 |
| Fail High (H) | 0 |
| Fail Low (L) | 103 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 46 |
| Fail Annunciation Undetected (λ_{AU}) | 70 |
| No effect | 245 |
| No part | 236 |
| Total failure rate (safety function) | 482 |
| Safe failure fraction (SFF) ⁶ | 90% |
| SIL AC ⁷ | SIL2 |

⁶ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁷ 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table of Contents

| | |
|---|----|
| Management Summary | 2 |
| 1 Purpose and Scope..... | 7 |
| 2 Project Management..... | 8 |
| 2.1 <i>exida</i> | 8 |
| 2.2 Roles of the parties involved..... | 8 |
| 2.3 Standards and Literature used | 8 |
| 2.4 Reference documents | 9 |
| 2.4.1 Documentation provided by the customer | 9 |
| 2.4.2 Documentation generated by <i>exida</i> | 9 |
| 2.5 <i>exida</i> tools used | 9 |
| 3 Product Description..... | 10 |
| 4 Failure Modes, Effects, and Diagnostic Analysis..... | 11 |
| 4.1 Description of the failure categories | 11 |
| 4.2 Methodology – FMEDA, Failure Rates | 12 |
| 4.2.1 FMEDA | 12 |
| 4.2.2 Failure Rates | 12 |
| 4.2.3 Assumptions | 13 |
| 4.3 Results of the assessment | 14 |
| 4.3.1 Results of Transmitter supply unit 9162 in current output configuration..... | 15 |
| 4.3.2 Results of Transmitter supply unit 9162 in dual relay output configuration | 16 |
| 4.3.3 Results of Transmitter supply unit 9162 in single relay output configuration..... | 17 |
| 5 Using the FMEDA Results | 18 |
| 5.1 Example PFD _{AVG} calculation..... | 18 |
| 6 Terms and Definitions | 19 |
| 7 Status of the Document..... | 20 |
| 7.1 Liability..... | 20 |
| 7.2 Releases..... | 20 |
| 7.3 Release Signatures | 20 |
| Appendix A: Possibilities to reveal dangerous undetected faults during the proof test.. | 21 |
| Appendix A.1: Possible proof tests to detect dangerous undetected faults | 21 |
| Appendix B: Impact of lifetime of critical components on the failure rate..... | 22 |
| Appendix C: <i>exida</i> Environmental Profiles | 23 |

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Transmitter supply unit 9162.

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the described Transmitter supply unit 9162 meets the average Probability of Failure on Demand (PFD_{AVG}) 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 product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

R. STAHL Schaltgeräte GmbH Manufacturer of the Transmitter supply unit 9162 and carried out the FMEDA.

exida Reviewed the FMEDAs and issued this report.

R. STAHL Schaltgeräte GmbH contracted *exida* in December 2013 with review of the FMEDAs and the preparation of this report.

2.3 Standards and 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; 2 nd edition |
| [N2] | SN 29500-1:01.2004 SN 29500-1 H1:12.2005 SN 29500-2:12.2004 SN 29500-3:12.2004 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:08.1990 SN 29500-12:03.1994 SN 29500-13:03.1994 SN 29500-14:03.1994 | Siemens standard with failure rates for components |
| [N3] | Electrical Component Reliability Handbook, 3rd Edition, 2012 | <i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0 |

2.4 Reference documents

2.4.1 Documentation provided by the customer

| | | |
|------|--|--|
| [D1] | 9162 6 020 003 0_00.pdf | Schematic diagram of 16.04.2014 |
| [D2] | 9162 6 020 003 0_02.pdf ⁸ | Schematic diagram of 22.05.2015 |
| [D3] | Fehlerversuche_9162_V1R0.xlsx | Fault insertion test results of 27.01.2014 |
| [D4] | FMEDA V7 9162 current output V2R04.efm | FMEDA of Transmitter supply unit 9162 in current output configuration, V2R4 of 29.04.2014 |
| [D5] | FMEDA V7 9162 relay output in series V2R04.efm | FMEDA of Transmitter supply unit 9162 in dual relay output configuration, V2R4 of 29.04.2014 |
| [D6] | FMEDA V7 9162 relay output V2R04.efm | FMEDA of Transmitter supply unit 9162 in single relay output configuration, V2R4 of 29.04.2014 |
| [D7] | MANTIS_ID0000098_V0R1.docx | Impact analysis of SW and HW changes, V0R1 of 21.05.2015 |

2.4.2 Documentation generated by *exida*

| | |
|------|---|
| [R1] | Summary FMEDA results 9162.xls of 13.05.2014 |
| [R2] | PFDavg Calc 9162.xls of 13.05.2014 |
| [R3] | FMEDA review checklist 9162.xls of 24.03.2014 |

2.5 *exida* tools used

| | | |
|------|-----------|------------|
| [T1] | SILcal V7 | FMEDA Tool |
|------|-----------|------------|

⁸ Changes of schematic file have no influence on FMEDA result since no components had been removed or added. The shown FMEDA results are also valid for the new schematic file.

3 Product Description

The Transmitter supply unit 9162 can be considered as a Type B⁹ element according to IEC 61508, having a hardware fault tolerance of 0.

The Transmitter supply unit 9162 is used for the operation of intrinsically safe 4...20 mA signal from a transmitter located in the field to a non-intrinsically safe signal. Internal calibration is done by a microcontroller. The connected transmitter is supplied by the Transmitter supply unit 9162.

The current output function converts the input current to the output. The relay output function can be configured to switch a digital output according to defined values. In the single relay output, only one output is used to provide the switching function. In the redundant / dual relay output configuration, two relay outputs are connected in series to reduce the risk of dangerous failures. The limit switch function can be configured by the user.

Figure 1 shows the connection diagram of the Transmitter supply unit 9162. The signal current of the field device is electrically insulated transferred to the output. Signal calibration, diagnostics and switching level monitoring for the relay outputs is done by a microcontroller.

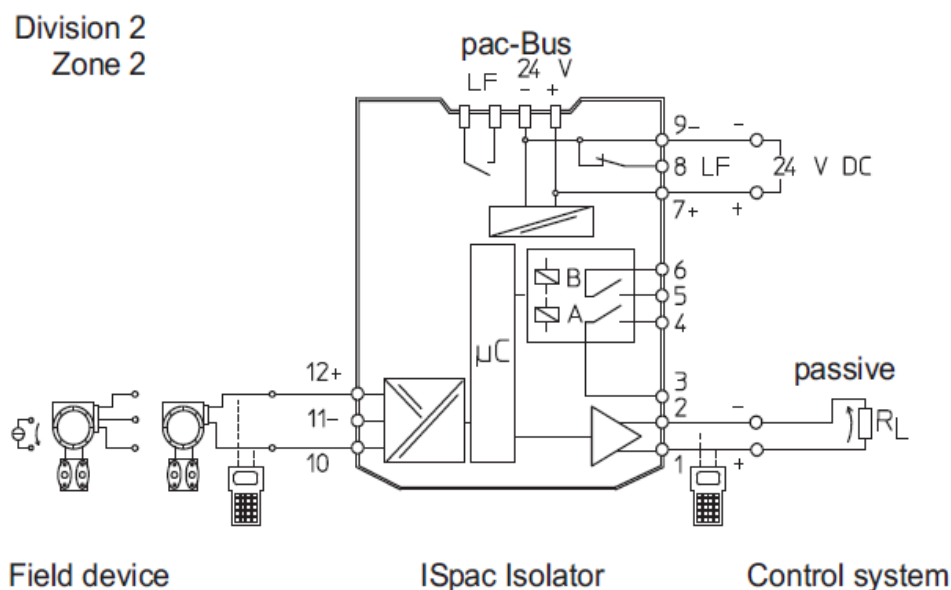


Figure 1: Connection of Transmitter supply unit 9162 standard types in SIL2 application

⁹ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented in [D4] to [D6].

4.1 Description of the failure categories

In order to judge the failure behavior of the Transmitter supply unit 9162, the following definitions for the failure of the device were considered.

| | |
|---------------------------|--|
| Fail-Safe state | The fail-safe state is defined as de-energized current output or deactivated relay output. |
| Fail Safe | A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state. |
| Fail Dangerous | A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required. |
| Fail Dangerous Undetected | Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU). Failures more than 2%FS (Full Scale) of current output are classified as Dangerous Undetected. |
| Fail Dangerous Detected | Failure that is dangerous but is detected by internal or external diagnostics (DD). |
| Fail High | A fail high failure (H) is defined as a failure that causes the output signal to go to a current above 21mA. |
| Fail Low | A fail low failure (L) is defined as a failure that causes the output signal to go to a current below 3.6mA. |
| Annunciation | Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. The Transmitter supply unit 9162 has no special diagnostic function, but failures of the redundant switch off path are classified as AU failures. |
| No effect | Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. |
| No part | Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. |

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 under consideration.

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

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical Component Reliability Handbook [N3] which was derived using over ten 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 operating stress conditions typical of an industrial field environment similar to *exida* Profile 1. 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 however 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. 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. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Transmitter supply unit 9162.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- 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.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described configurations of the Transmitter supply unit 9162 are considered.
- Safety critical failures are defined as a deviation of more than 2% FS (Full Scale) for current output or deviation of relay output switching threshold.
- For the soft errors, a failure rate of 1.2 FIT/kBit was assumed.
- The diagnostic functions lead breakage detection and short circuit detection is activated.
- Only the signal transmission function of the Transmitter Supply Unit 9162 types is part of the FMEDA. The failure rates of the transmitter supply function are not included. It is assumed that a connected transmitter checks the supply voltage which is provided by the Transmitter Supply Unit 9162 and stops operation in case of insufficient supply instead of generating wrong output signals.

4.3 Results of the assessment

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

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

$$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{AU})) + 24\ h$$

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:

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the Transmitter supply unit 9162 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 Results of Transmitter supply unit 9162 in current output configuration

The FMEDA carried out on the Transmitter supply unit 9162 in current output configuration and the assumptions described in section 4.2.3 and 4.3 is leading to the following failure rates:

Table 5: Failure rates of Transmitter supply unit 9162 in current output configuration

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 416 |
| Fail Dangerous Detected (λ_{DD}) | 244 |
| Fail High (H) | 12 |
| Fail Low (L) | 160 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 27 |
| Fail Annunciation Undetected (λ_{AU}) | 89 |
| No effect | 251 |
| No part | 249 |
| Total failure rate (safety function) | 443 |
| Safe failure fraction (SFF) ¹⁰ | 93% |
| SIL AC ¹¹ | SIL2 |

¹⁰ The complete sensor 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

4.3.2 Results of Transmitter supply unit 9162 in dual relay output configuration

The FMEDA carried out on the Transmitter supply unit 9162 configured as dual relay output and the assumptions described in section 4.2.3 and 4.3 is leading to the following failure rates:

Table 6: Failure rates of Transmitter supply unit 9162 in dual relay output configuration

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 447 |
| Fail Dangerous Detected (λ_{DD}) | 344 |
| Fail High (H) | 0 |
| Fail Low (L) | 103 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 26 |
| Fail Annunciation Undetected (λ_{AU}) | 81 |
| No effect | 245 |
| No part | 238 |
| Total failure rate (safety function) | 473 |
| Safe failure fraction (SFF) ¹² | 94% |
| SIL AC ¹³ | SIL2 |

¹² The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹³ 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

4.3.3 Results of Transmitter supply unit 9162 in single relay output configuration

The FMEDA carried out on the Transmitter supply unit 9162 configured as dual relay output and the assumptions described in section 4.2.3 and 4.3 is leading to the following failure rates:

Table 7: Failure rates of Transmitter supply unit 9162 in one relay output configuration

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 436 |
| Fail Dangerous Detected (λ_{DD}) | 333 |
| Fail High (H) | 0 |
| Fail Low (L) | 103 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 46 |
| Fail Annunciation Undetected (λ_{AU}) | 70 |
| No effect | 245 |
| No part | 236 |
| Total failure rate (safety function) | 482 |
| Safe failure fraction (SFF) ¹⁴ | 90% |
| SIL AC ¹⁵ | SIL2 |

¹⁴ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁵ 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. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

5 Using the FMEDA Results

The following section describes how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} calculation

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for Transmitter supply unit 9162 considering a proof test coverage of 99% (see Appendix A.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in sections [R1]. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 8.

For SIL2 applications, the PFD_{AVG} value needs to be $< 1.00E-02$.

Table 8: PFD_{AVG} values

| | T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---------------------|------------------------|------------------------|------------------------|
| 9162 current output | $PFD_{AVG} = 1.30E-04$ | $PFD_{AVG} = 2.43E-04$ | $PFD_{AVG} = 5.81E-04$ |
| 9162 dual relay | $PFD_{AVG} = 1.29E-04$ | $PFD_{AVG} = 2.38E-04$ | $PFD_{AVG} = 5.67E-04$ |
| 9162 single relay | $PFD_{AVG} = 2.23E-04$ | $PFD_{AVG} = 4.19E-04$ | $PFD_{AVG} = 1.01E-03$ |

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval considering is approximately equal to 1.3% for the current output configuration.

Figure 2 shows the time dependent curve of PFD_{AVG} .

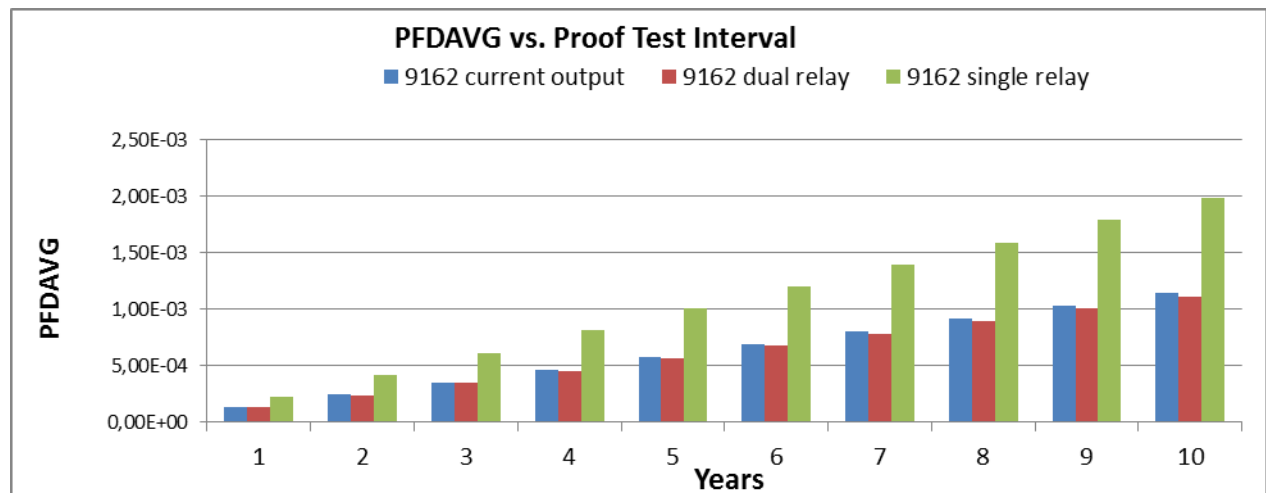


Figure 2: $PFD_{AVG}(t)$ for Transmitter supply unit 9162

6 Terms and Definitions

| | |
|-----------------|--|
| FIT | Failure In Time (1×10^{-9} failures per hour) |
| FMEDA | Failure Mode Effect and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| Low demand mode | Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency. |
| PFD_{AVG} | Average Probability of Failure on Demand |
| SFF | Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action. |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). |
| PLC | Programmable Logic Controller |
| Type B element | “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2 |

7 Status of the Document

7.1 Liability

exida prepares FMEDA 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

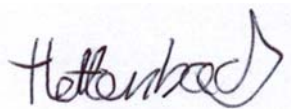
Version History: V1R2: Assumptions added; January 19, 2016
V1R1: Schematic file update, SW version update; June 16, 2015
V1R0: Editorial Changes; June 25, 2014
V0R1: Initial draft for review only; May 13, 2014

Author: Jan Hettenbach

Review: V0R1 Andreas Bagusch (R. Stahl Schaltgeräte GmbH), June 06, 2014;
Stephan Aschenbrenner, June 18, 2014

Release Status: V1R0 Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures



Dipl. -Ing. (Univ.) Jan Hettenbach

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

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

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

Appendix A.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 9. It is assumed that this test will detect 99% of possible dangerous failures.

Table 9: Steps for proof test

| Step | Action |
|------|---|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip. |
| 2. | Apply an input signal with a defined amplitude at the Transmitter supply unit 9162. |
| 3. | Check, if the output current of the Transmitter supply unit 9162 is within the specification. |
| 4. | Check if the relay outputs are switching according to the defined threshold. |
| 5. | Remove the bypass from the monitoring system or otherwise restore normal operation. |

Appendix B: 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 lifetime¹⁶ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve. 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.

The Transmitter supply unit 9162 has no components with reduced life time which are contributing to the dangerous undetected failure rate.

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

¹⁶ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix C: *exida* Environmental Profiles

Table 10 *exida* Environmental Profiles

| <i>exida</i> Profile | 1 | 2 | 3 | 4 | 5 | 6 |
|---|--|-------------------------|------------------------|-------------------|------------------------|---------------------|
| Description (Electrical) | Cabinet mounted/ Climate Controlled | Low Power Field Mounted | General Field Mounted | Subsea | Offshore | N/A |
| | | no self-heating | self-heating | | | |
| Description (Mechanical) | Cabinet mounted/ Climate Controlled | General Field Mounted | General Field Mounted | Subsea | Offshore | Process Wetted |
| IEC 60654-1 Profile | B2 | C3 | C3 | N/A | C3 | N/A |
| | | also applicable for D1 | also applicable for D1 | | also applicable for D1 | |
| Average Ambient Temperature | 30C | 25C | 25C | 5C | 25C | 25C |
| Average Internal Temperature | 60C | 30C | 45C | 5C | 45C | Process Fluid Temp. |
| Daily Temperature Excursion (pk-pk) | 5C | 25C | 25C | 0C | 25C | N/A |
| Seasonal Temperature Excursion (winter average vs. summer average) | 5C | 40C | 40C | 2C | 40C | N/A |
| Exposed to Elements/Weather Conditions | No | Yes | Yes | Yes | Yes | Yes |
| Humidity¹⁷ | 0-95% Non-Condensing | 0-100% Condensing | 0-100% Condensing | 0-100% Condensing | 0-100% Condensing | N/A |
| Shock¹⁸ | 10 g | 15 g | 15 g | 15 g | 15 g | N/A |
| Vibration¹⁹ | 2 g | 3 g | 3 g | 3 g | 3 g | N/A |
| Chemical Corrosion²⁰ | G2 | G3 | G3 | G3 | G3 | Compatible Material |
| Surge²¹ | | | | | | |
| 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 | |
| EMI Susceptibility²² | | | | | | |
| 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 | |
| ESD (Air)²³ | 6kV | 6kV | 6kV | 6kV | 6kV | N/A |

¹⁷ Humidity rating per IEC 60068-2-3

¹⁸ Shock rating per IEC 60068-2-6

¹⁹ Vibration rating per IEC 60770-1

²⁰ Chemical Corrosion rating per ISA 71.04

²¹ Surge rating per IEC 61000-4-5

²² EMI Susceptibility rating per IEC 6100-4-3

²³ ESD (Air) rating per IEC 61000-4-2