



Failure Modes, Effects and Diagnostic Analysis

Project:

Isolating Repeater Output 9165

Customer:

R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 04/04-03

Report No.: STAHL 04/04-03 R004

Version V5, Revision R0; September 2015

Jan Hettenbach

Management summary

This report summarizes the results of the hardware assessment carried out on the Isolating Repeater Output 9165 revision Rev. C and Rev. D. Table 1 gives an overview of the different configurations that belong to the considered Isolating Repeater Output 9165.

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.

Table 1: Configuration overview

| Isolating Repeater | Type 9165 / | a | b | - | 1 | 1 | - | e | f |
|----------------------------------|-------------|---|---|---|---|---|---|---|---|
| Number of Channels: | | | | | | | | | |
| 1 | 1 | | | | | | | | |
| 2 | 2 | | | | | | | | |
| Signal: | | | | | | | | | |
| 0/4 ... 20 mA with HART | 6 | | | | | | | | |
| Design: | | | | | | | | | |
| 24 V, I.S. ¹ version | 1 | | | | | | | | |
| 24 V, non I.S. version | 6 | | | | | | | | |
| Line fault detection: | | | | | | | | | |
| without | 0 | | | | | | | | |
| open and short circuit detection | 1 | | | | | | | | |

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

The two channels on the dual channel devices shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

The Isolating Repeater Output 9165 is considered to be a Type A² element with a hardware fault tolerance of 0.

The following table shows how the above stated requirements are fulfilled.

¹ I.S. Intrinsic Safety

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 2: Failure rates according to IEC 61508: 2010

| | SN29500 at 40°C |
|--|-------------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 150 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 15 |
| Fail Low (L) | 135 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 58 |
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 213 |
| No part | 172 |
| Total failure rate (safety function) | 208 |
| Safe failure fraction (SFF) | 72% |
| SIL AC | SIL2 |
| PFH | 5.8E-8 1/h |

The failure rates are valid for the useful life of the Isolating Repeater Output 9165 (see Appendix 2).

Table of Contents

| | |
|---|----|
| Management summary | 2 |
| 1 Purpose and Scope | 5 |
| 2 Project management..... | 6 |
| 2.1 <i>exida</i> | 6 |
| 2.2 Roles of the parties involved..... | 6 |
| 2.3 Standards / Literature used..... | 6 |
| 2.4 Reference documents..... | 7 |
| 2.4.1 Documentation provided by the customer..... | 7 |
| 2.4.2 Documentation generated by <i>exida</i> | 7 |
| 3 Description of the analyzed module | 8 |
| 3.1 Isolating Repeater Output 9165 | 8 |
| 4 Failure Modes, Effects, and Diagnostic Analysis | 9 |
| 4.1 Description of the failure categories..... | 9 |
| 4.2 Methodology – FMEDA, Failure rates | 10 |
| 4.2.1 FMEDA..... | 10 |
| 4.2.2 Failure rates | 10 |
| 4.2.3 Assumption | 10 |
| 5 Results of the assessment..... | 11 |
| 5.1 Isolating Repeater Output 9165..... | 12 |
| 6 Using the FMEDA Results | 13 |
| 6.1 Example PFD _{AVG} calculation | 13 |
| 7 Terms and Definitions..... | 14 |
| 8 Status of the document..... | 15 |
| 8.1 Liability..... | 15 |
| 8.2 Releases | 15 |
| 8.3 Release signatures | 15 |
| Appendix 1: Possible proof tests to detect dangerous undetected faults..... | 16 |
| Appendix 2: Impact of lifetime of critical components on the failure rate | 17 |

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 9165.

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the described 9165 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 Isolating Repeater Output 9165.

exida Performed the hardware assessment.

R. STAHL Schaltgeräte GmbH contracted *exida* in May 2015 with update of the report and FMEDA results.

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; 2nd 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 |
| [N4] | Mechanical Component Reliability Handbook, 3rd Edition, 2012 | <i>exida</i> LLC, Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7 |

2.4 Reference documents

2.4.1 Documentation provided by the customer

| | | |
|------|--|---|
| [D1] | 91 656 02 20 0_08.pdf | Circuit diagram „Trennübertrager / Isolating Repeater Typ 9165/**-11-***“ 91 656 02 20 0 Index 08 of 09.10.13 |
| [D2] | STL 9165-02_00_20090407.xlsx | Parts list for Isolating Repeater Output 9165 |
| [D3] | 9165 next Generation_A.docx of 22.05.09 | Description of changes |
| [D4] | 9165 Varianten ohne Fehlermeldung.docx of 04.01.11 | Description of changes |
| [D5] | Useful lifetime 9165.pdf | Useful lifetime analysis of 29.10.13 |
| [D6] | MANTIS ID0000089 V0R1.doc | Impact analysis of changes |
| [D7] | FMEDA V7 9165nG V1R3.efm | FMEDA file of 29.10.2013 / 23.02.2015 of schematic diagram Index 08 |

2.4.2 Documentation generated by exida

| | |
|------|---|
| [R1] | FMEDA V7 9165nG V1 R0_1.efm of 07.07.09 |
| [R2] | 91 656 02 20 0_00_20090407 – marked.pdf of 07.07.09 |
| [R3] | RE Angebot 9165.msg of 07.07.09 |
| [R4] | FMEDA V7 9165nG V1R1.efm of 14.07.09 |

3 Description of the analyzed module

3.1 Isolating Repeater Output 9165

The Isolating Repeater Output 9165 is used for the operation of control valves, I/P converters or displays.

The device can transfer bi-directionally a superimposed HART communication signal.

The Isolating Repeater Output 9165 is considered to be a Type A³ element with a hardware fault tolerance of 0.

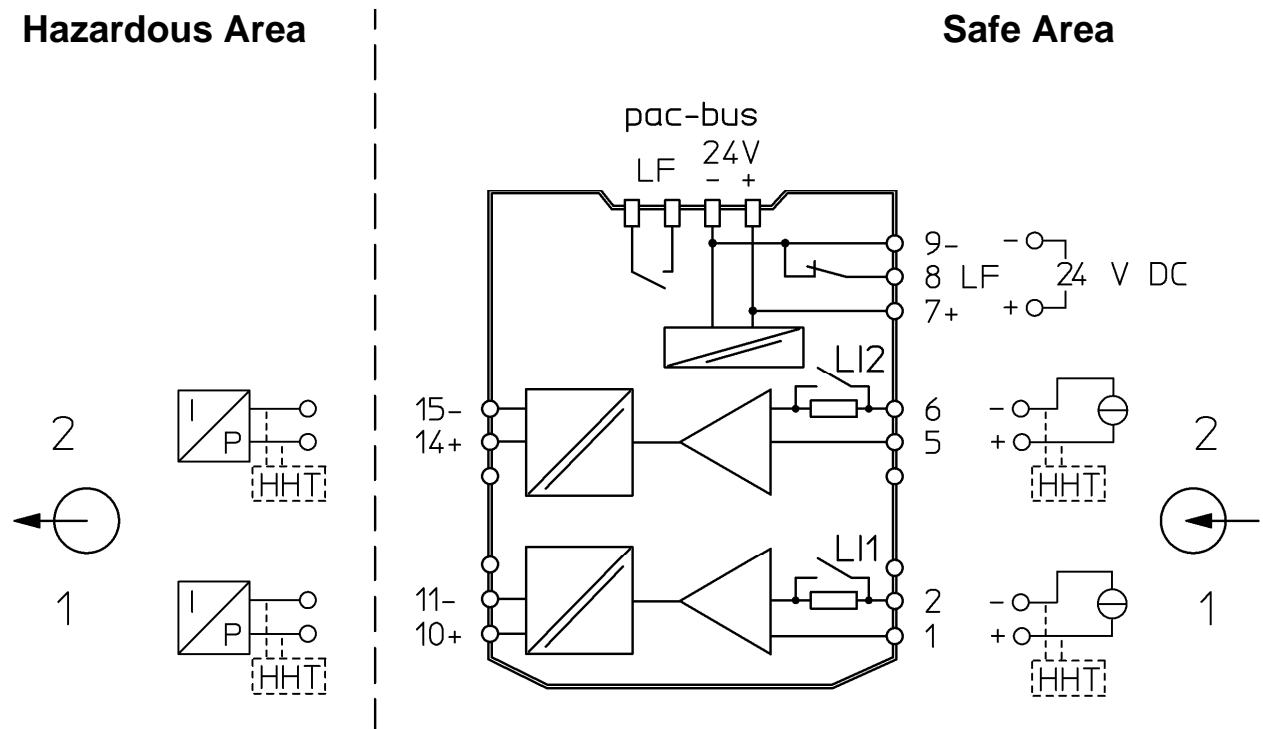


Figure 1: Block diagram of the Isolating Repeater Output 9165

Figure 1 is representative for all Isolating Repeater Output 9165 listed in Table 1.

³ Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented in [R4].

4.1 Description of the failure categories

In order to judge the failure behavior of the Isolating Repeater Output 9165, the following definitions for the failure of the product were considered.

| | |
|-----------------|---|
| Fail-Safe State | The fail-safe state is defined as the output going to < 3.8 mA. |
| Fail Safe | Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process or has no effect on the safety function. |
| Fail Dangerous | Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 2% full scale (± 0.32 mA). |
| Fail High | Failure that causes the output signal to go to the maximum output current (> 20.5 mA) |
| Fail Low | Failure that causes the output signal to go to the minimum output current (< 3.8 mA) |
| Fail No Effect | Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output current by not more than 2% full scale. For the calculation of the SFF it is treated like a safe undetected failure. |
| Not part | Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate. |

The “No Effect” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508:2000 the “No Effect” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

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 are the basic failure rates from the Siemens SN 29500 failure rate database. The rates are considered to be appropriate for safety integrity level verification calculations. The rates match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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 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 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Isolating Repeater Output 9165.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not during normal operation.
- For safety applications only the 4..20 mA output is considered.
- Only one input and one output are part of the considered safety function.
- The two channels on a redundant board are not used to increase the hardware fault tolerance needed for a higher SIL as they contain common components.
- The line break and short circuit detection is not part of the safety function.

5 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 9165 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

5.1 Isolating Repeater Output 9165

The FMEDA carried out on the Isolating Repeater Output 9165 leads under the assumptions described in section 4.2.3 to the following failure rates:

| SN29500 at 40°C | |
|---|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 150 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 15 |
| Fail Low (L) | 135 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 58 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 213 |
| No part | 172 |

| | |
|---|------------|
| Total failure rate (safety function) | 208 |
|---|------------|

| | |
|-----------------------------|------------|
| Safe failure fraction (SFF) | 72% |
| SIL AC | SIL2 |
| PFH | 5.8E-8 1/h |

6 Using the FMEDA Results

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

6.1 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 9165 considering a proof test coverage of 95% (see Appendix 1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 5.1. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 3. Both inputs (input I and input II) have the same PFD_{AVG} values.

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

Table 3: PFD_{AVG} values

| Configuration | T[Proof] = 1 year | T[Proof] = 3 years | T[Proof] = 5 years | T[Proof] = 10 years |
|---------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| 9165 | PFD _{AVG} = 3.63E-04 | PFD _{AVG} = 8.40E-04 | PFD _{AVG} = 1.32E-03 | PFD _{AVG} = 2.51E-03 |

The listed PFD_{AVG} values are calculated for a proof test coverage of 95%.

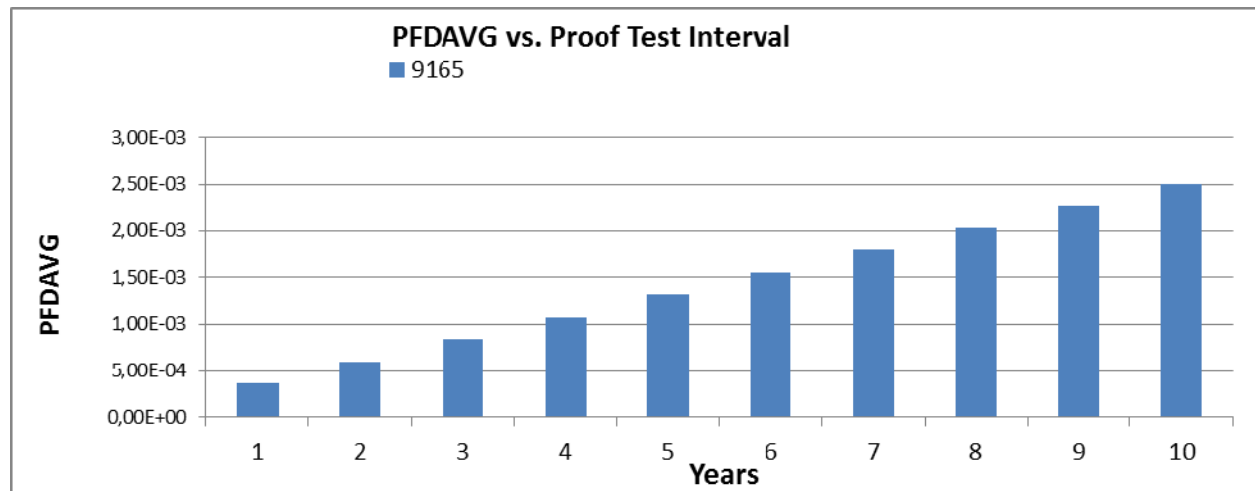


Figure 2: PFD_{AVG} (t)

7 Terms and Definitions

| | |
|-----------------|---|
| FIT | Failure In Time (1×10^{-9} failures per hour) |
| FMEDA | Failure Modes, Effects, and Diagnostic Analysis |
| HART | Highway Addressable Remote Transducer |
| 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 one per year and 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 |
| Type A element | “Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2. |

8 Status of the document

8.1 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.

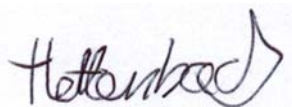
Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

8.2 Releases

Version History: V5R0: Update after review, September 7, 2015
V4R2: Editorial changes, update FMEDA results; July 6, 2015
V4R1: Editorial changes; March 9, 2011
V4R0: Additional variants added; February 8, 2011
V3R0: Adjustments after hardware modifications; July 14, 2009
V2R1: Editorial changes; November 7, 2008
V2R0: Additional devices added, results updated; November 4, 2008
V1, R1.0: Review comments integrated; August 6, 2004
V0, R1.0: Initial version; July 8, 2004

Author: Jan Hettenbach
Review: V4R2: reviewed by J. Hochhaus (*exida*), S. Schultz (R. STAHL),
Release status: Released to R. STAHL Schaltgeräte GmbH

8.3 Release signatures



Dipl.-Ing. (Univ.) Jan Hettenbach



Dipl.-Ing. Jürgen Hochhaus

Appendix 1: Possible 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.

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

Proof test 1 consists of the following steps, as described in Table 4.

Table 4 Steps for Proof Test 1

| Step | Action |
|------|--|
| 1 | Take appropriate action to avoid a false trip |
| 2 | Provide a 4mA control signal to the Isolating Repeater Output 9165 to open/close the valve and verify that the valve is open/closed. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures. It requires, however, that the valve has already been tested without the repeater and does not contain any dangerous undetected faults anymore. |
| 3 | Restore the loop to full operation |
| 4 | Restore normal operation |

This test will detect approximately 70% of possible “du” failures in the Isolating Repeater Output 9165.

Proof test 2 consists of the following steps, as described in Table 5.

Table 5 Steps for Proof Test 2

| Step | Action |
|------|---|
| 1 | Take appropriate action to avoid a false trip |
| 2 | Perform Proof Test 1 |
| 3 | Provide a 4..20 mA control signal in steps of 1 mA to the Isolating Repeater Output 9165 to open/close the valve and verify that the valve opens/closes accordingly. This requires that the valve has already been tested without the repeater and does not contain any dangerous undetected faults anymore. |
| 4 | Restore the loop to full operation |
| 5 | Restore normal operation |

This test will detect approximately 95% of possible “du” failures in the Isolating Repeater Output 9165.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 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 lifetime⁴ 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, which shows the typical behavior for electronic components. 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 6 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 6: Useful lifetime of components with reduced useful lifetime contributing to λ_{du}

| Type | Name | Useful lifetime |
|------------------------------------|----------|--------------------|
| Opto-coupler - With bipolar output | O51, O52 | More than 10 years |

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

⁴ 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.