



Failure Modes, Effects and Diagnostic Analysis

Project:

9106 HART Transparent Repeater and 9107 HART Transparent Driver

Customer:

PR electronics A/S

Rønde

Denmark

Contract No.: PR electronics 06/03-19

Report No.: PR electronics 06/03-19 R025

Version V2, Revision R1; July 2016

Piotr Serwa, Jan Hettenbach

Management summary

This report summarizes the results of the hardware assessment carried out on the 9106 HART Transparent Repeater with hardware version as shown in Table 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.

For safety applications, only the described order numbers, with the described input/output configurations, are considered:

1. 9106B1A and 9106B2A (Ex) / 9106A1A and 9106A2A (Standard) - 1 channel
2. 9106B1B and 9106B2B (Ex) / 9106A1B and 9106A2B (Standard) - 2 channel
3. 9107BA (Ex) / 9107AA (Standard) - 1 channel
4. 9107BB (Ex) / 9107AB (Standard) - 2 channel

The only difference between 9106B1A / 9106B1B and 9106B2A / 9106B2B are the Ex data for the passive input terminals.

The 9107BB (Ex) / 9107AB (Standard) is a dual channel configuration of 9107BA (Ex) / 9107AA (Standard) and has two complete independent channels. The Failure rates are calculated for one channel.

All other possible input/output configurations and order numbers are not covered by this report.

Table 1 shows the input/output configurations of the 9106 HART Transparent Repeater and 9107 HART Transparent Driver that have been assessed. The usage of the different configurations is described in Figure 3 to Figure 5.

Table 1: 9106 HART Transparent Repeater and 9107 HART Transparent Driver

| | FMEDA name | HW/SW version | Configuration description |
|------|--|---------------|---|
| [C1] | 9106 Single, active input and active output | 9106 V5R1 | Active input ¹ : the input signal of the 9106 HART Transparent Repeater is driven by the external device. Active output: the 9106 HART Transparent Repeater works as a current source. This configuration is provided by (1) 9106BA (Ex) / 9106AA (Standard) and by (2) 9106BB (Ex) / 9106AB (Standard) working in single-channel mode. |
| [C2] | 9106 Single, active input and passive output | 9106 V5R1 | Active input ¹ : the input signal of the 9106 HART Transparent Repeater is driven by the external device. Passive output: the 9106 HART Transparent Repeater works as a passive current regulator with external voltage source. This configuration is provided by (1) 9106BA (Ex) / 9106AA (Standard) and by (2) 9106BB (Ex) / 9106AB (Standard) working in single-channel mode. |

¹ "Active input" of the 9106 HART Transparent Repeater means that an external device has a separate supply voltage and is thereby an active current source.

| | FMEDA name | HW/SW version | Configuration description |
|------|--|---------------|--|
| [C3] | 9106 Single, passive input and active output | 9106 V5R1 | Passive input (transmitter input) ² : the input signal of the external device is driven by the 9106 HART Transparent Repeater. Active output: the 9106 HART Transparent Repeater works as a current source. This configuration is provided by (1) 9106BA (Ex) / 9106AA (Standard) and by (2) 9106BB (Ex) / 9106AB (Standard) working in single-channel mode. |
| [C4] | 9106 Single, passive input and passive output | 9106 V5R1 | Passive input (transmitter input) ² : the input signals of the external device are driven by the 9106 HART Transparent Repeater. Passive output: the 9106 HART Transparent Repeater works as a passive current regulator with external voltage source. This configuration is provided by (1) 9106BA (Ex) / 9106AA (Standard) and by (2) 9106BB (Ex) / 9106AB (Standard) working in single-channel mode. |
| [C5] | 9106 Dual active input and dual active output | 9106 V5R1 | Dual active input ¹ : the input signals of the 9106 HART Transparent Repeater are driven by the external device. Dual active output: the 9106 HART Transparent Repeater works as a current source with two identical output currents. |
| [C6] | 9106 Dual active input and dual passive output | 9106 V5R1 | Dual active input ¹ : the input signals of the 9106 HART Transparent Repeater are driven by the external device. Dual passive outputs: each output of the 9106 HART Transparent Repeater works as independent passive current regulator with external voltage source. |
| [C7] | 9106 One passive input and one active and dual active outputs | 9106 V5R1 | Mixed inputs: one input is active and one input is passive, both are connected in series to one external device. Dual active output: the 9106 HART Transparent Repeater works as a current source with two identical output currents. |
| [C8] | 9106 One passive input and one active and dual passive outputs | 9106 V5R1 | Mixed inputs: one input is active and one input is passive, both are connected in series to one external device. Dual passive outputs: each output of the 9106 HART Transparent Repeater works as independent passive current regulator with external voltage source. |
| [C9] | 9107 Single, active input and active output | 9107 V1R1 | Active input ³ : the input signal of the 9107 HART Transparent Driver driven by the external device Active output: the 9107 HART Transparent Repeater works as a current source. This FMEDA includes the dual channel type, which is considered as two separate 9107BA (Ex) / 9107AA (Standard) types in one enclosure. |

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1⁴. The analysis was carried out with the basic failure rates from the Siemens standard SN 29500. However, as the comparison between these two databases has shown that the differences are within an acceptable tolerance the failure rates of the *exida* database are listed.

² "Passive input" of the 9106 HART Transparent Repeater means that the external device is passive and supplied by the Transparent Repeater.

³ "Active input" of the 9107 HART Transparent Driver means that an external device has a separate supply voltage and is thereby an active current source.

⁴ For details, see Appendix 3.

The 9106 HART Transparent Repeater and 9107 HART Transparent Driver contains a CPU, but the CPU is not a part of the safety function. The safety function of the 9106 HART Transparent Repeater and 9107 HART Transparent Driver (current in - current out) is done in discrete hardware. Therefore, the 9106 HART Transparent Repeater and the 9107 HART Transparent Driver are considered to be Type A⁵ subsystems.

The 9106 HART Transparent Repeater and the 9107 HART Transparent Driver have a hardware fault tolerance of 0. For Type A subsystems with a hardware fault tolerance of 0 the SFF has to be $\geq 60\%$ for SIL 2 subsystems according to table 2 of IEC 61508-2. For Type A subsystems with a hardware fault tolerance of 0 the SFF has to be $\geq 90\%$ for SIL 3 subsystems.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the 9106 HART Transparent Repeater or 9107 HART Transparent Driver with 4..20 mA current output communicate detected faults by an alarm output current $\leq 3,6\text{mA}$ or $\geq 21\text{mA}$. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures.

Dangerous detected (DD) failures can only be detected by an external logic solver, which is assumed to be connected to the 9106 Transparent Repeater or 9107 Transparent Driver. Internally, the 9106 Transparent Repeater and 9107 Transparent Driver don't have any diagnostic function. For the dual channel configuration, an internal dangerous detected failure is assumed if the difference between both output signals is more than 2% full span. This difference must be detected by the external logic solver.

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

⁵ Type A subsystem: Non-complex system. For details, see 7.4.3.1.2 of IEC 61508-2.

Table 2: Summary for [C1] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 173 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 27 |
| Fail Low (L) | 146 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 177 |
| No part | 713 |

| | |
|---|------------|
| Total failure rate (safety function) | 214 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF ⁶ | 80% |
| SIL AC ⁷ | SIL2 |
| PFH | 4,1E-08 1/h |

⁶ The complete 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. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 3: Summary for [C2] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 174 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 35 |
| Fail Low (L) | 139 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 177 |
| No part | 711 |

| | |
|---|------------|
| Total failure rate (safety function) | 215 |
|---|------------|

| | |
|---------------------------|--------------------|
| SFF⁸ | 80% |
| SIL AC⁹ | SIL2 |
| PFH | 4,1E-08 1/h |

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

⁹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 4: Summary for [C3] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 27 |
| Fail Low (L) | 133 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 40 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 164 |
| No part | 739 |

| | |
|---|------------|
| Total failure rate (safety function) | 200 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ¹⁰ | 80% |
| SIL AC ¹¹ | SIL2 |
| PFH | 4,0E-08 1/h |

¹⁰ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹¹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 5: Summary for [C4] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 35 |
| Fail Low (L) | 125 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 165 |
| No part | 738 |

| | |
|---|------------|
| Total failure rate (safety function) | 201 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ¹² | 79% |
| SIL AC ¹³ | SIL2 |
| PFH | 4,1E-08 1/h |

¹² The complete 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. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 6: Summary for [C5] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 382 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 55 |
| Fail Low (L) | 263 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 315 |
| No part | 1201 |

| | |
|---|------------|
| Total failure rate (safety function) | 391 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ¹⁴ | 97% |
| SIL AC ¹⁵ | SIL3 |
| PFH | 9,0E-09 1/h |

¹⁴ The complete 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. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 7: Summary for [C6] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 381 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 70 |
| Fail Low (L) | 247 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 316 |
| No part | 1199 |

| | |
|---|------------|
| Total failure rate (safety function) | 390 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ¹⁶ | 97% |
| SIL AC ¹⁷ | SIL3 |
| PFH | 9,0E-09 1/h |

¹⁶ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁷ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 8: Summary for [C7] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 368 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 54 |
| Fail Low (L) | 250 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 304 |
| No part | 1228 |
| Total failure rate (safety function) | 377 |
| SFF ¹⁸ | 97% |
| SIL AC ¹⁹ | SIL3 |
| PFH | 9,0E-09 1/h |

¹⁸ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 9: Summary for [C8] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 368 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 70 |
| Fail Low (L) | 234 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 305 |
| No part | 1225 |

| | |
|---|------------|
| Total failure rate (safety function) | 377 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF²⁰ | 97% |
| SIL AC²¹ | SIL3 |
| PFH | 9,0E-09 1/h |

²⁰ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²¹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 10: Summary for [C9] - IEC 61508:2010 failure rates

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 127 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 1 |
| Fail Low (L) | 126 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 48 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 164 |
| No part | 506 |

| | |
|---|------------|
| Total failure rate (safety function) | 175 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ²² | 72% |
| SIL AC ²³ | SIL2 |
| PFH | 4,8E-08 1/h |

²² The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²³ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

Table of Contents

| | |
|---|----|
| Management summary | 2 |
| 1 Purpose and Scope..... | 15 |
| 2 Project management | 16 |
| 2.1 <i>exida</i> | 16 |
| 2.2 Roles and parties..... | 16 |
| 2.3 Standards / Literature used | 16 |
| 2.4 Reference documents | 17 |
| 2.4.1 Documentation provided by the customer | 17 |
| 2.4.2 Documentation generated by <i>exida</i> | 17 |
| 3 Description of the analyzed subsystems | 18 |
| 4 Failure Modes, Effects, and Diagnostic Analysis..... | 21 |
| 4.1 Description of the failure categories | 21 |
| 4.2 Methodology – FMEDA, Failure rates..... | 22 |
| 4.2.1 FMEDA | 22 |
| 4.2.2 Failure rates..... | 22 |
| 4.2.3 Assumptions | 23 |
| 4.3 Results according to IEC 61508:2010 | 23 |
| 4.3.1 Type 9106, configuration active input and active output..... | 24 |
| 4.3.2 Type 9106, configuration active input and passive output..... | 25 |
| 4.3.3 Type 9106, configuration passive input and active output..... | 26 |
| 4.3.4 Type 9106, configuration passive input and passive output..... | 27 |
| 4.3.5 Type 9106, configuration two active inputs, two active outputs..... | 28 |
| 4.3.6 Type 9106, configuration two active inputs, two passive outputs..... | 29 |
| 4.3.7 Type 9106, configuration active and passive inputs, two active outputs | 30 |
| 4.3.8 Type 9106, configuration active and passive inputs, two passive outputs | 31 |
| 4.3.9 Type 9107, configuration active input and active output,..... | 32 |
| 5 Using the FMEDA results | 33 |
| 5.1 Example PFD _{AVG} calculation..... | 33 |
| 6 Terms and Definitions | 35 |
| 7 Status of the document | 36 |
| 7.1 Liability..... | 36 |
| 7.2 Releases..... | 36 |
| 7.3 Release Signatures | 36 |
| Appendix 1 Possibilities to reveal dangerous undetected faults during proof test..... | 37 |
| Appendix 1.1 Possible proof tests to detect dangerous undetected faults | 37 |
| Appendix 2 Impact of lifetime of critical components on the failure rate..... | 38 |
| Appendix 3 Description of the considered profiles | 39 |
| Appendix 3.1 <i>exida</i> electronic database..... | 39 |
| Appendix 4 FIT values according to IEC 61508:2000 | 40 |

1 Purpose and Scope

This document describes the results of the FMEDA carried out on the 9106 HART Transparent Repeater and the 9107 HART Transparent Driver. Table 1 shows the input/output configurations of the 9106 HART Transparent Repeater and the 9107 HART Transparent Driver that have been assessed. The FMEDA is part of a full functional safety assessment according to IEC 61508.

2 Project management

2.1 *exida*

exida is one of the world's leading 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 partnership company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail 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 and parties

PR electronics A/S Manufacturer of the 9106 HART Transparent Repeater and the 9107 HART Transparent Driver.

exida Performed the hardware assessment and reviewed the FMEDA provided by the customer.

PR electronics A/S contracted *exida* with the review of the FMEDA of the devices mentioned above.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

| | | |
|------|---|--|
| [N1] | IEC 61508-2:2000 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |
| [N2] | IEC 61508-2:2010 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2 nd edition |
| [N3] | Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008 | <i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6 |

2.4 Reference documents

2.4.1 Documentation provided by the customer

| | | |
|-------|--|--|
| [D1] | 9106 Safety Concept.doc of 25.05.2010, version V3R0 | 9106 Safety Concept |
| [D2] | 9106-1-V5R1-X.pdf of 12.06.2011, version V5R1 | Circuit schematics and layout diagrams |
| [D3] | 9106 Derating Analysis V0R2 of 23.01.2012, version V0R6 | Derating analysis |
| [D4] | 9106 FMEDA AI-AO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Single, active input and active output |
| [D5] | 9106 FMEDA AI-PO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Single, active input and passive output |
| [D6] | 9106 FMEDA PI-AO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Single, passive input and active output |
| [D7] | 9106 FMEDA PI-PO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Single, passive input and passive output |
| [D8] | 9106 FMEDA Dual AI_AI-AO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Dual active input and dual active output |
| [D9] | 9106 FMEDA Dual AI_AI-PO V0R9.xls of 24.01.2012 | FEMDA results for 9106 Dual active input and dual passive output |
| [D10] | 9106 FMEDA Dual PI_AI-AO V0R9.xls of 24.01.2012 | FEMDA results for 9106 One passive input and one active and dual active outputs |
| [D11] | 9106 FMEDA Dual PI_AI-PO V0R9.xls of 24.01.2012 | FEMDA results for 9106 One passive input and one active and dual passive outputs |
| [D12] | 9107 FMEDA V0R2.xls of 24.01.2012 | FEMDA results for 9107 Single, active input and active output |
| [D13] | 9106 Hardware Fault Insertion Test Report V4R0 | Fault insertion test of 9106 Transparent Repeater |
| [D14] | 9107 Hardware Fault Insertion Test Report V2R0 | Fault insertion test of 9107 Transparent Driver |
| [D15] | 9107 schematic V1R1 | Circuit diagram of 9107 Transparent Driver |
| [D16] | New A variant to the 9000 series of transmitters with grey terminals.msg of 15.05.14 | Description of changes between Ex and standard versions. |

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] | 9106 and 9107 PFDavg Calc.xls of 22.02.2012 | PFDavg calculation of the 9106 HART Transparent Repeater and 9107 HART Transparent Driver |
|------|---|---|

3 Description of the analyzed subsystems

The 9106 HART Transparent Repeater repeats the Ex current input signal into current output signal. Both inputs and output ports of the 9106 HART Transparent Repeater can be active and passive.

The 9106 HART Transparent Repeater is available in a version with one measurement channel and a version with two channels.

The dual channel version has two separate and independent hardware measurement channels. The required level of independence between them is provided by the clear separation of the channel-related hardware circuitry.

The 9107 HART Transparent Driver is functional identical with the single channel 9106 HART Transparent Repeater, but has an Ex output instead an Ex input.

The 9106 HART Transparent Repeater and the 9107 HART Transparent Driver contain each a CPU, but the CPU is not a part of the safety function and therefore the 9106 HART Transparent Repeater and 9107 HART Transparent Driver is considered a type A subsystem.

The CPU is only used for displaying the process value on the 4501 display and for trimming the current output, not affecting the safety. The device is manufactured to an accuracy of ~0.3%. To increase the accuracy to 0.1%, the CPU trims the output. The CPU has the possibility to trim the output signal (i.e. the safety output) only within the range +/- 1% (this limit is insured by hardware). The device has a safety accuracy of +/- 2%. The control signal from the CPU is a PWM signal (0-100%), so whatever happens to the microcontroller, the PWM cannot go outside 0-100%, which corresponds to the maximal trimming of +/-1% on the output current. Therefore, any failure of the CPU can cause an error in the output signal of up to +/-1%, which, taking into account the accuracy of the hardware channels, guarantees the safety accuracy of +/- 2%.

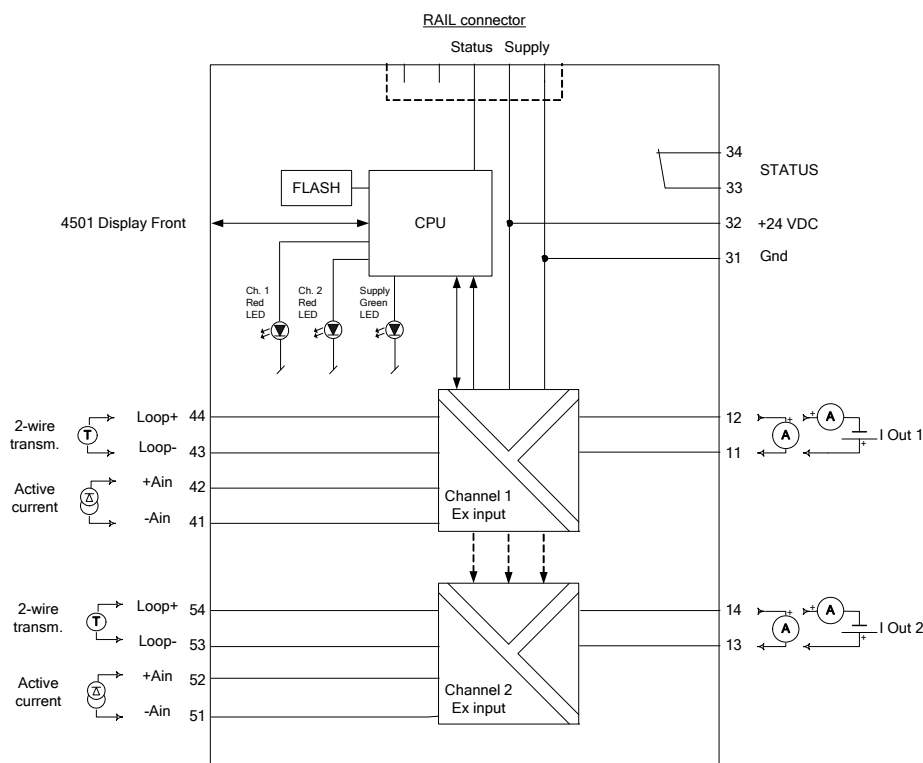


Figure 1: 9106 HART Transparent Repeater block diagram (dual channel version)

As shown by Figure 1, the 9106 HART Transparent Repeater and the 9107 HART Transparent Driver have the current inputs and current outputs.

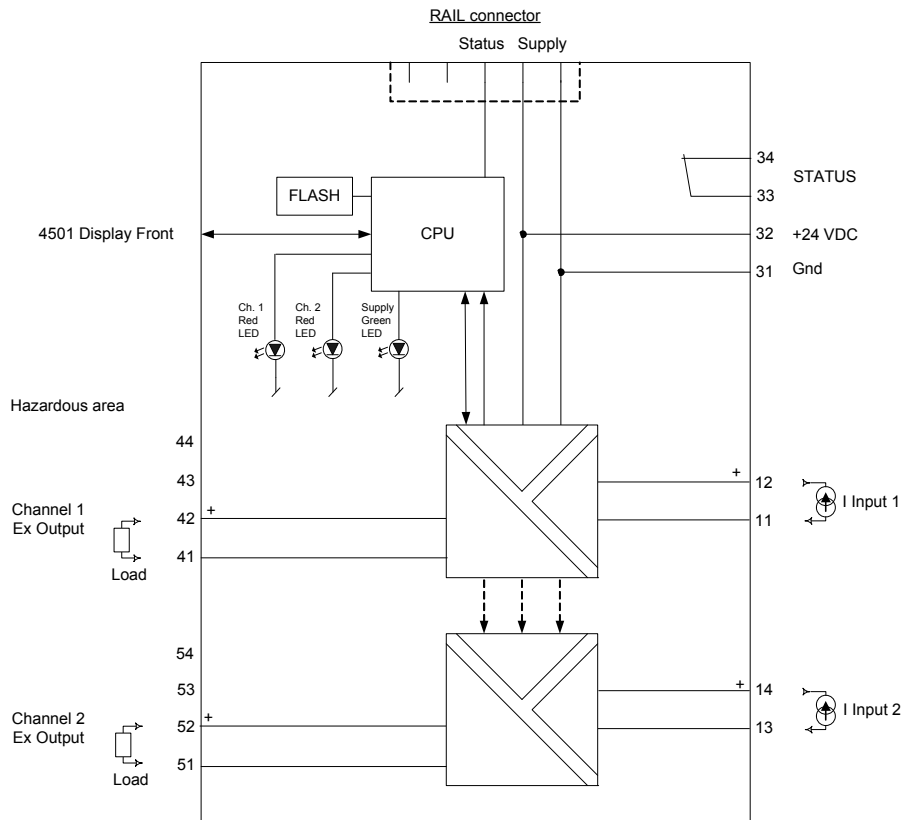


Figure 2: 9107 HART Transparent Driver block diagram (dual channel version)

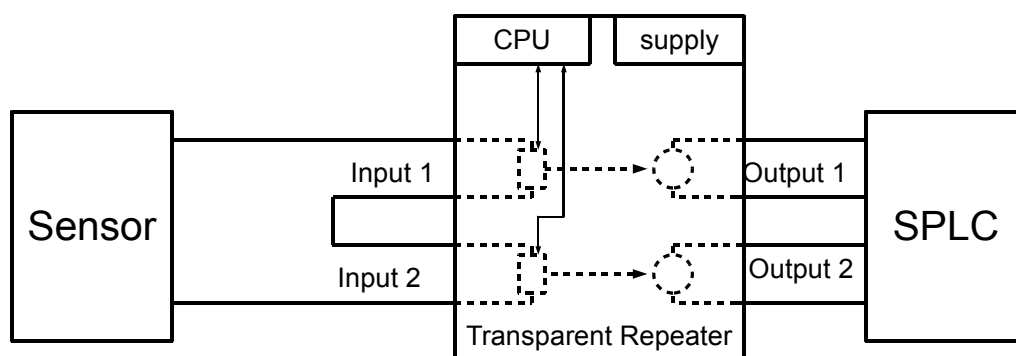


Figure 3: Dual channel Connection of one Sensor

As shown in Figure 2, a sensor is connected to both inputs. Only one input may supply the sensor. Only a passive input can supply a sensor. Active inputs are driven by external sensors or other devices. In this configuration it is required that the Safety PLC (SPLC) compares the two output signals with an accuracy of +/- 2% of full span. A discrepancy of more than +/- 2% shall lead to a fault detection. This configuration is recommended for SIL3 application. The results are shown in section 4.3.5 to section 4.3.8.

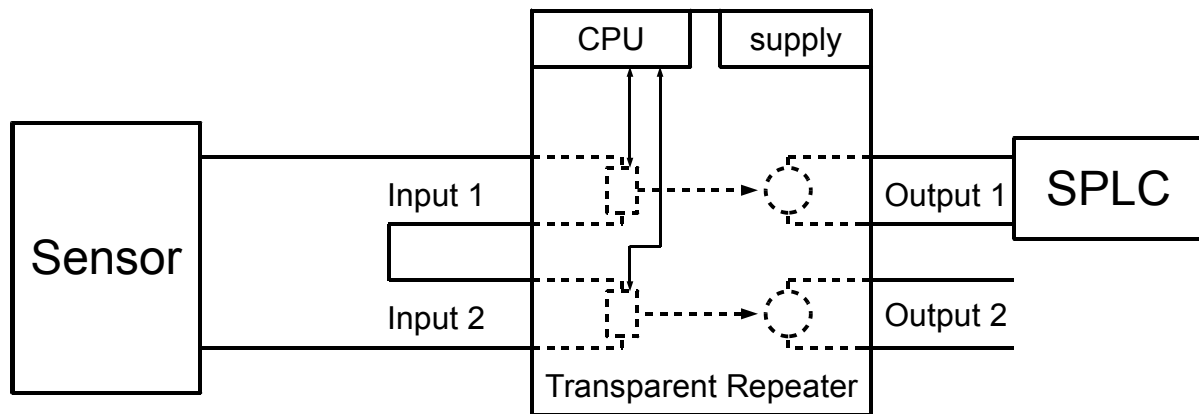


Figure 4: Single channel connection of dual channel transmitter (SIL2 application)

In Figure 4, a single channel connection of a dual channel transmitter is shown. When using 9106B1B, B2B, A1B or A2B in SIL2 applications, only one channel is used for safety loop and the results for single channel versions are valid. Second channel output can be used for non-safety application. The results are shown in section 4.3.1 to 4.3.4 and 4.3.9 Configurations with two active inputs as shown in section 4.3.5 and 4.3.6 cannot be used for the connection as shown in Figure 4.

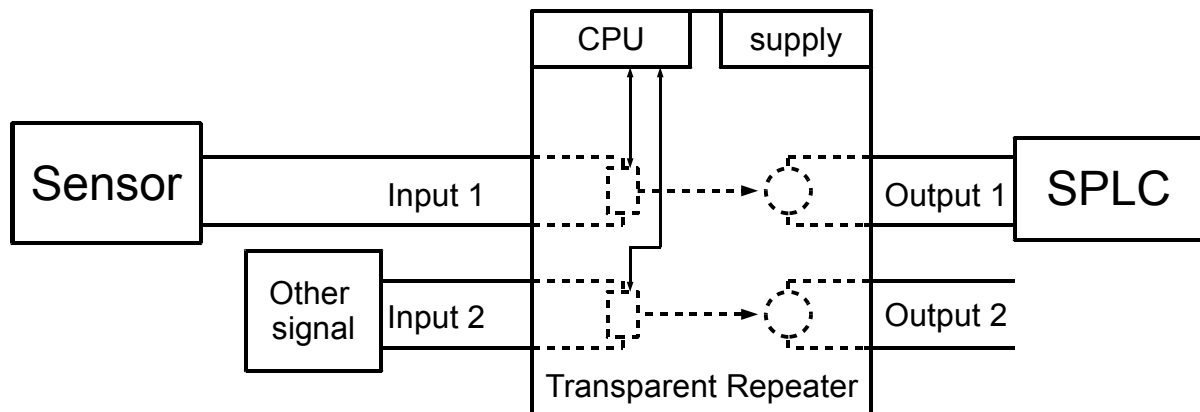


Figure 5: Single channel use of dual channel transmitter (SIL2 application)

Figure 5 shows another configuration of dual channel transmitters in single channel SIL2 applications. All dual channel versions can be used for this configuration, but only the equivalent single channel results shall be used for calculation.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was prepared by PR electronics A/S and reviewed by *exida*. The resulting FMEDAs are documented in [D4] to [D12]. When the effect of a certain component failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see fault insertion test report [D13] to [D14]). This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the 9106 HART Transparent Repeater and 9107 HART Transparent Driver, the following definitions for the failure of the product were considered.

| | |
|---------------------------|---|
| Fail-Safe State | The fail-safe state is defined as the output reaching the user defined threshold value. |
| Fail Safe | Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process. |
| Fail Dangerous | A dangerous failure (D) is defined as a 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 span. |
| Fail Dangerous Undetected | Failure that is dangerous and that is not being diagnosed by internal diagnostics. |
| Fail Dangerous Detected | Failure that is dangerous but is detected by internal diagnostics and causes the output signal to go to the predefined alarm state. |
| Fail High | A fail high failure (H) is defined as a failure that causes the output signal to go to the over-range or high alarm output current (> 21mA). |
| Fail Low | A fail low failure (L) is defined as a failure that causes the output signal to go to the under-range or low alarm output current (< 3.6mA). |
| No Effect | A no effect failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function or deviates the output current by not more than 2% full span. 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. For the calculation of the SFF they are treated as "Dangerous Undetected" failures. |
| No Part | Component that plays no part in implementing the safety function but is 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" and "Annunciation Undetected" 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 from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1. 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 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 9106 HART Transparent Repeater and 9107 HART Transparent Driver.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Failures during parameterization are not considered.
- 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.
- External power supply failure rates are not included.
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to the safe state is identical to MTTR.
- Only the described versions are used for safety applications.
- For the 9106B1A and 9106B2A (Ex) / 9106A1A and 9106A2A (Standard), 9107BA (Ex) / 9107AA (Standard) and 9107BB (Ex) / 9107AB (Standard), only one input and one output are part of the considered safety function.
- For the 9106B1B and 9106B2B (Ex) / 9106A1B and 9106A2B (Standard), both channels are part of the considered safety function. The second channel is used as redundant diagnostic channel.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Short circuit and lead breakage detection are activated.

4.3 Results according to IEC 61508:2010

The 9106 HART Transparent Repeaters 9106B1B and 9106B2B (Ex) / 9106A1B and 9106A2B (Standard) have two separate and independent input/output paths, sharing the same power supply and additional electronics. In the analysis, they could be split into two separate subsystems: (1) channel one representing the first input/output channel plus power supply and additional electronic having a hardware fault tolerance of 0 and (2) channel two representing the second input/output channel. However, this approach does not allow computing the SFF for the entire repeater. Therefore, the analysis was done by considering the second input/output channel to be the "diagnostics" for the first "primary" input/output channel. On the first input/output channel a $DC_{\text{dangerous}}$ of 90% was considered because of redundancy with the second input/output channel and because of common cause failures (beta = 10%) between input/output channel 1 and 2. On the second input/output channel, the failures are considered as annunciation failures (rather than dangerous failures) with $DC_{\text{annunciation}}$ of 95%.

For the calculation of the Safe Failure Fraction (SFF) and λ_{total} the following has to be noted:

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

$$\text{SFF} = 1 - \lambda_{\text{DU}} / \lambda_{\text{total}}$$

$$DC_{\text{D}} = \lambda_{\text{DD}} / (\lambda_{\text{DD}} + \lambda_{\text{DU}})$$

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

4.3.1 Type 9106, configuration active input and active output

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration active input and active output ([C1]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 173 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 27 |
| Fail Low (L) | 146 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 177 |
| No part | 713 |

| | |
|---|------------|
| Total failure rate (safety function) | 214 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF²⁴ | 80% |
| SIL AC²⁵ | SIL2 |
| PFH | 4,1E-08 1/h |

²⁴ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.2 Type 9106, configuration active input and passive output

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration active input and passive output ([C2]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 174 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 35 |
| Fail Low (L) | 139 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 177 |
| No part | 711 |

| | |
|---|------------|
| Total failure rate (safety function) | 215 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF²⁶ | 80% |
| SIL AC²⁷ | SIL2 |
| PFH | 4,1E-08 1/h |

²⁶ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²⁷ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.3 Type 9106, configuration passive input and active output

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration passive input and active output ([C3]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 27 |
| Fail Low (L) | 133 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 40 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 164 |
| No part | 739 |

| | |
|---|------------|
| Total failure rate (safety function) | 200 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF²⁸ | 80% |
| SIL AC²⁹ | SIL2 |
| PFH | 4,0E-08 1/h |

²⁸ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²⁹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.4 Type 9106, configuration passive input and passive output

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration passive input and passive output ([C4]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 35 |
| Fail Low (L) | 125 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 165 |
| No part | 738 |

| | |
|---|------------|
| Total failure rate (safety function) | 201 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF³⁰ | 79% |
| SIL AC³¹ | SIL2 |
| PFH | 4,1E-08 1/h |

³⁰ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³¹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.5 Type 9106, configuration two active inputs, two active outputs

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration of two active inputs and two active outputs ([C5]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 382 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 55 |
| Fail Low (L) | 263 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 315 |
| No part | 1201 |

| | |
|---|------------|
| Total failure rate (safety function) | 391 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ³² | 97% |
| SIL AC ³³ | SIL3 |
| PFH | 9,0E-09 1/h |

³² The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³³ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.6 Type 9106, configuration two active inputs, two passive outputs

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration of two active inputs and two passive outputs ([C6]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 381 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 70 |
| Fail Low (L) | 247 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 316 |
| No part | 1199 |

| | |
|---|------------|
| Total failure rate (safety function) | 390 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF³⁴ | 97% |
| SIL AC³⁵ | SIL3 |
| PFH | 9,0E-09 1/h |

³⁴ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.7 Type 9106, configuration active and passive inputs, two active outputs

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration one active and one passive input and two active outputs ([C7]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 368 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 54 |
| Fail Low (L) | 250 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 304 |
| No part | 1228 |

| | |
|---|------------|
| Total failure rate (safety function) | 377 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ³⁶ | 97% |
| SIL AC ³⁷ | SIL3 |
| PFH | 9,0E-09 1/h |

³⁶ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³⁷ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.8 Type 9106, configuration active and passive inputs, two passive outputs

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration one active and one passive input and two passive outputs ([C8]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 368 |
| Fail Dangerous Detected (λ_{DD}) | 31 |
| Fail High (H) | 70 |
| Fail Low (L) | 234 |
| Fail Annunciation Detected (λ_{AD}) | 33 |
| Fail Dangerous Undetected (λ_{DU}) | 9 |

| | |
|---|------|
| Fail Annunciation Undetected (λ_{AU}) | 2 |
| No effect | 305 |
| No part | 1225 |

| | |
|---|------------|
| Total failure rate (safety function) | 377 |
|---|------------|

| | |
|----------------------------|--------------------|
| SFF³⁸ | 97% |
| SIL AC³⁹ | SIL3 |
| PFH | 9,0E-09 1/h |

³⁸ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³⁹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

4.3.9 Type 9107, configuration active input and active output,

The FMEDA carried out on the 9107 HART Transparent Driver, configuration active input and active output ([C9]) leads under the assumptions described in section 4.2.3 to the following failure rates:

| Failure category | Failure rates (in FIT) |
|--|------------------------|
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail Safe Undetected (λ_{SU}) | 0 |
| Fail Dangerous Detected (λ_{DD}) | 127 |
| Fail Dangerous Detected (λ_{DD}) | 0 |
| Fail High (H) | 1 |
| Fail Low (L) | 126 |
| Fail Annunciation Detected (λ_{AD}) | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 48 |

| | |
|---|-----|
| Fail Annunciation Undetected (λ_{AU}) | 0 |
| No effect | 164 |
| No part | 506 |

| | |
|---|------------|
| Total failure rate (safety function) | 175 |
|---|------------|

| | |
|-----------------------------|--------------------|
| SFF ⁴⁰ | 72% |
| SIL AC ⁴¹ | SIL2 |
| PFH | 4,8E-08 1/h |

⁴⁰ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴¹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

5 Using the FMEDA results

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

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).

5.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) 9106 or 9107 HART Transparent Repeater considering a proof test coverage of 95% (see Appendix 1.1) and a mission time of 10 years. The failure rate data used in this calculation is displayed in section 4.3. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 11.

Table 11: PFD_{AVG} values

| Configuration | T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|--|------------------------|------------------------|------------------------|
| [C1] 9106 Single, active input and active output | $PFD_{AVG} = 1,92E-04$ | $PFD_{AVG} = 3,67E-04$ | $PFD_{AVG} = 8,92E-04$ |
| [C2] 9106 Single, active input and passive output | $PFD_{AVG} = 1,95E-04$ | $PFD_{AVG} = 3,71E-04$ | $PFD_{AVG} = 9,02E-04$ |
| [C3] 9106 Single, passive input and active output | $PFD_{AVG} = 1,91E-04$ | $PFD_{AVG} = 3,64E-04$ | $PFD_{AVG} = 8,84E-04$ |
| [C4] 9106 Single, passive input and passive output | $PFD_{AVG} = 1,93E-04$ | $PFD_{AVG} = 3,68E-04$ | $PFD_{AVG} = 8,94E-04$ |
| [C9] 9107 Single, active input and active output | $PFD_{AVG} = 2,29E-04$ | $PFD_{AVG} = 4,37E-04$ | $PFD_{AVG} = 1,06E-03$ |

As the single channel 9106 HART Transparent Repeater or 9107 HART Transparent Driver are a part of an entire safety function they should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget they should be better than or equal to $1.00E-03$. The calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of this range, i.e. to be better than or equal to $1.00E-03$. Figure 6 shows the time-dependent value of PFD_{AVG} .

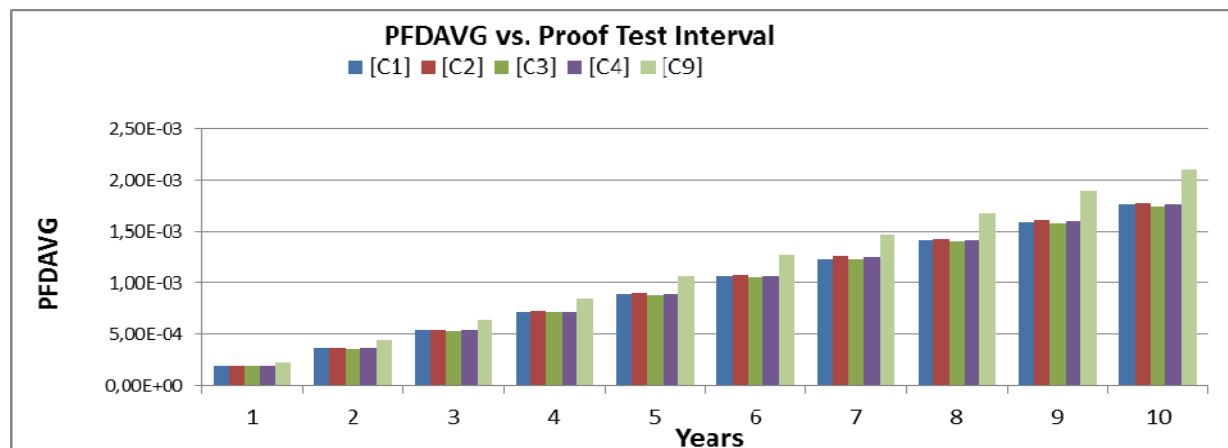


Figure 6: $PFD_{AVG}(t)$ of SIL2 single channel devices

Table 12: PFD_{AVG} values

| Configuration | T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---|-------------------------------|-------------------------------|-------------------------------|
| [C5] 9106 Dual active input and dual active output | PFD _{AVG} = 4,25E-05 | PFD _{AVG} = 8,04E-05 | PFD _{AVG} = 1,94E-04 |
| [C6] 9106 Dual active input and dual passive output | PFD _{AVG} = 4,27E-05 | PFD _{AVG} = 8,09E-05 | PFD _{AVG} = 1,95E-04 |
| [C7] 9106 One passive input and one active and dual active outputs | PFD _{AVG} = 4,23E-05 | PFD _{AVG} = 8,01E-05 | PFD _{AVG} = 1,93E-04 |
| [C8] 9106 One passive input and one active and dual passive outputs | PFD _{AVG} = 4,26E-05 | PFD _{AVG} = 8,05E-05 | PFD _{AVG} = 1,94E-04 |

As the dual channel 9106 HART Transparent Repeater are a part of an entire safety function they should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget they should be better than or equal to 1.00E-04. The calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of this range, i.e. to be better than or equal to 1.00E-04.

Figure 7 shows the time-dependent value of PFD_{AVG}.

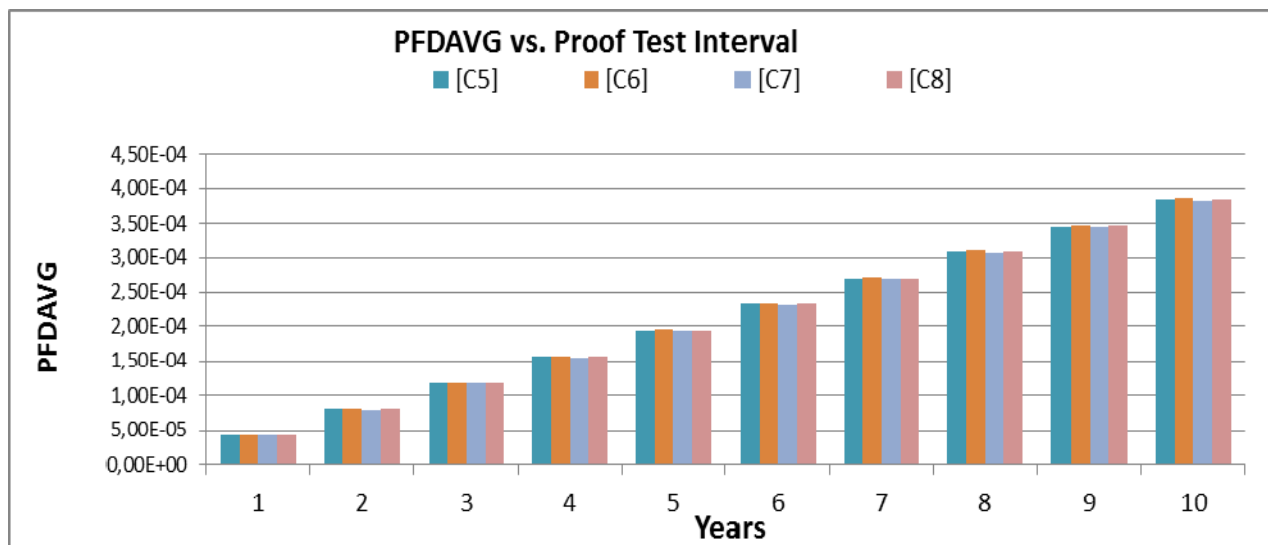


Figure 7: PFD_{AVG}(t) of SIL3 dual channel devices

6 Terms and Definitions

| | |
|--------------------|--|
| DC _D | Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$) |
| FIT | Failure In Time (1×10^{-9} failures per hour) |
| FMEDA | Failure Modes, Effects, 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 one per year and no greater than twice the proof test frequency. |
| MTTR | Mean Time To Restoration |
| 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 subsystem | “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2 |
| T[Proof] | Proof Test Interval |

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

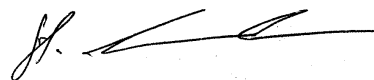
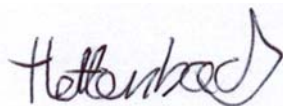
Version History: V2R1: Description SIL2 application added; July 11, 2016
V2R0: Non-Ex versions added; July 8, 2014
V1R1: Changes in product description; July 6, 2012
V1R0: editorial changes; March 07, 2012
V0R1: Initial version; February 24, 2012

Authors: Piotr Serwa, Jan Hettenbach, Stephan Aschenbrenner

Review: V0R1: Stephan Aschenbrenner (*exida*); March 5, 2012
Nikolaj Wehner (PR electronics A/S); March 1, 2012

Release status: Released to PR electronics A/S

7.3 Release Signatures



Dipl.-Ing. (Univ.) Jan Hettenbach

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

Appendix 1 Possibilities to reveal dangerous undetected faults during proof test

According to section 7.4.3.2.2 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 that have been noted during the FMEDA can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1 Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 13.

Table 13: Suggested proof test

| Step | Action |
|------|--|
| 1 | Bypass the safety PLC or take other appropriate action to avoid a false trip |
| 2 | Connect a simulator identical to the input setup |
| 3 | Apply input value corresponding to 0/100% output value for each channel |
| 4 | Observe whether the output channel acts as expected |
| 5 | Restore the input terminals to full operation |
| 6 | Remove the bypass from safety PLC or otherwise restore normal operation |

This test will detect approximately 95% of possible “du” failures in the transmitter and the connected sensing element.

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 lifetime⁴² 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 that 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.

In the 9106 HART Transparent Repeater and 9107 HART Transparent Driver, there are no components with reduced useful lifetime that contribute to λ_{du} .

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

⁴² 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 that covers product obsolescence, warranty, or other commercial issues.

Appendix 3 Description of the considered profiles

Appendix 3.1 *exida* electronic database

| Profile | Profile according to IEC 60654-1 | Ambient Temperature [°C] | | Temperature Cycle [°C / 365 days] |
|---------|----------------------------------|--------------------------|-------------------|-----------------------------------|
| | | Average (external) | Mean (inside box) | |
| 1 | B2 | 30 | 60 | 5 |
| 2 | C3 | 25 | 30 | 25 |
| 3 | C3 | 25 | 45 | 25 |

PROFILE 1:

Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

PROFILE 2:

Low power electrical (two-wire) field products have minimal self-heating and are subjected to daily temperature swings.

PROFILE 3:

General (four-wire) field products may have moderate self-heating and are subjected to daily temperature swings.

Appendix 4 FIT values according to IEC 61508:2000

The following values are calculated according to IEC 61508:2000.

Table 14: Summary for [C1] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration active input and active output ([C1]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 177 |
| Fail safe undetected | 0 |
| No effect | 177 |
| Fail Dangerous Detected (λ_{DD}) | 173 |
| Fail detected (detected by internal diagnostics) | 0 |
| Fail low (detected by safety logic solver) | 146 |
| Fail high (detected by safety logic solver) | 27 |
| Annunciation detected | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |
| Fail dangerous undetected | 41 |
| Annunciation undetected | 0 |
| No part | 713 |

| | |
|---|------------------|
| Total failure rate (safety function) | 391 |
| SFF⁴³ | 89% |
| DC_D | 80% |
| MTBF | 103 years |

| | |
|----------------------------|-------------|
| SIL AC⁴⁴ | SIL2 |
|----------------------------|-------------|

⁴³ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴⁴ 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.

Table 15: Summary for [C2] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration active input and passive output ([C2]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 177 |
| Fail safe undetected | 0 |
| No effect | 177 |
| Fail Dangerous Detected (λ_{DD}) | 174 |
| Fail detected (detected by internal diagnostics) | 0 |
| Fail low (detected by safety logic solver) | 139 |
| Fail high (detected by safety logic solver) | 35 |
| Annunciation detected | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |
| Fail dangerous undetected | 41 |
| Annunciation undetected | 0 |
| No part | 711 |
| Total failure rate (safety function) | 392 |
| SFF ⁴⁵ | 89% |
| DC_D | 80% |
| MTBF | 103 years |
| SIL AC ⁴⁶ | SIL2 |

⁴⁵ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴⁶ 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.

Table 16: Summary for [C3] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration passive input and active output ([C3]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 164 |
| Fail safe undetected | 0 |
| No effect | 164 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail detected (detected by internal diagnostics) | 0 |
| Fail low (detected by safety logic solver) | 133 |
| Fail high (detected by safety logic solver) | 27 |
| Annunciation detected | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 40 |
| Fail dangerous undetected | 40 |
| Annunciation undetected | 0 |
| No part | 739 |
| Total failure rate (safety function) | 364 |
| SFF ⁴⁷ | 89% |
| DC_D | 80% |
| MTBF | 103 years |
| SIL AC ⁴⁸ | SIL2 |

⁴⁷ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴⁸ 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.

Table 17: Summary for [C4] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration passive input and passive output ([C4]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 165 |
| Fail safe undetected | 0 |
| No effect | 165 |
| Fail Dangerous Detected (λ_{DD}) | 160 |
| Fail detected (detected by internal diagnostics) | 0 |
| Fail low (detected by safety logic solver) | 125 |
| Fail high (detected by safety logic solver) | 35 |
| Annunciation detected | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 41 |
| Fail dangerous undetected | 41 |
| Annunciation undetected | 0 |
| No part | 738 |
| Total failure rate (safety function) | 366 |
| SFF ⁴⁹ | 88% |
| DC_D | 79% |
| MTBF | 103 years |
| SIL AC ⁵⁰ | SIL2 |

⁴⁹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵⁰ 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.

Table 18: Summary for [C5] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration of two active inputs and two active outputs ([C5]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 315 |
| Fail safe undetected | 0 |
| No effect | 315 |
| Fail Dangerous Detected (λ_{DD}) | 377 |
| Fail detected (detected by internal diagnostics) | 28 |
| Fail low (detected by safety logic solver) | 263 |
| Fail high (detected by safety logic solver) | 55 |
| Annunciation detected | 31 |
| Fail Dangerous Undetected (λ_{DU}) | 11 |
| Fail dangerous undetected | 9 |
| Annunciation undetected | 2 |
| No part | 1201 |
| Total failure rate (safety function) | 703 |
| SFF⁵¹ | 98% |
| DC_D | 97% |
| MTBF | 59 years |
| SIL AC⁵² | SIL3 |

⁵¹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵² 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.

Table 19: Summary for [C6] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration of two active inputs and two passive outputs ([C6]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 316 |
| Fail safe undetected | 0 |
| No effect | 316 |
| Fail Dangerous Detected (λ_{DD}) | 376 |
| Fail detected (detected by internal diagnostics) | 28 |
| Fail low (detected by safety logic solver) | 247 |
| Fail high (detected by safety logic solver) | 70 |
| Annunciation detected | 31 |
| Fail Dangerous Undetected (λ_{DU}) | 11 |
| Fail dangerous undetected | 9 |
| Annunciation undetected | 2 |
| No part | 1199 |
| Total failure rate (safety function) | 703 |
| SFF⁵³ | 98% |
| DC_D | 97% |
| MTBF | 60 years |
| SIL AC⁵⁴ | SIL3 |

⁵³ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵⁴ 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.

Table 20: Summary for [C7] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration one active and one passive input and two active outputs ([C7]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 304 |
| Fail safe undetected | 0 |
| No effect | 304 |
| Fail Dangerous Detected (λ_{DD}) | 363 |
| Fail detected (detected by internal diagnostics) | 28 |
| Fail low (detected by safety logic solver) | 250 |
| Fail high (detected by safety logic solver) | 54 |
| Annunciation detected | 31 |
| Fail Dangerous Undetected (λ_{DU}) | 11 |
| Fail dangerous undetected | 9 |
| Annunciation undetected | 2 |
| No part | 1228 |
| Total failure rate (safety function) | 678 |
| SFF⁵⁵ | 98% |
| DC_D | 97% |
| MTBF | 59 years |
| SIL AC⁵⁶ | SIL3 |

⁵⁵ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵⁶ 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.

Table 21: Summary for [C8] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9106 HART Transparent Repeater, configuration one active and one passive input and two passive outputs ([C8]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 305 |
| Fail safe undetected | 0 |
| No effect | 305 |
| Fail Dangerous Detected (λ_{DD}) | 363 |
| Fail detected (detected by internal diagnostics) | 28 |
| Fail low (detected by safety logic solver) | 234 |
| Fail high (detected by safety logic solver) | 70 |
| Annunciation detected | 31 |
| Fail Dangerous Undetected (λ_{DU}) | 11 |
| Fail dangerous undetected | 9 |
| Annunciation undetected | 2 |
| No part | 1225 |
| Total failure rate (safety function) | 679 |
| SFF⁵⁷ | 98% |
| DC_D | 97% |
| MTBF | 59 years |
| SIL AC⁵⁸ | SIL3 |

⁵⁷ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵⁸ 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.

Table 22: Summary for [C9] - IEC 61508:2000 failure rates

The FMEDA carried out on the 9107 HART Transparent Driver, configuration active input and active output ([C9]) leads to the following failure rates:

| | <i>exida</i> Profile 1 |
|--|------------------------|
| Failure category | Failure rates (in FIT) |
| Fail Safe Detected (λ_{SD}) | 0 |
| Fail safe detected | 0 |
| Fail Safe Undetected (λ_{SU}) | 164 |
| Fail safe undetected | 0 |
| No effect | 164 |
| Fail Dangerous Detected (λ_{DD}) | 127 |
| Fail detected (detected by internal diagnostics) | 0 |
| Fail low (detected by safety logic solver) | 126 |
| Fail high (detected by safety logic solver) | 1 |
| Annunciation detected | 0 |
| Fail Dangerous Undetected (λ_{DU}) | 48 |
| Fail dangerous undetected | 48 |
| Annunciation undetected | 0 |
| No part | 506 |

| | |
|---|------------------|
| Total failure rate (safety function) | 339 |
| SFF⁵⁹ | 85% |
| DC_D | 72% |
| MTBF | 135 years |

| | |
|----------------------------|-------------|
| SIL AC⁶⁰ | SIL2 |
|----------------------------|-------------|

⁵⁹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁶⁰ 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.