



Failure Modes, Effects and Diagnostic Analysis

Project:
Plant-STOP 9469

Customer:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: Stahl 15/05-054
Report No.: Stahl 15/05-054 R036
Version V1, Revision R1; February, 2019

Jan Hettenbach

Management summary

This report summarizes the results of the hardware assessment carried out on the Universal Module HART 9469 with hardware version as listed in the drawings referenced in section 2.5.1. Table 1 gives an overview of the considered variants.

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

Table 1: Configuration overview

Configuration	Description							
9469/35-08-12	2-wire lout (channel 0-7) and 4-wire supply output (channel 4-7), only Plant Stop Function considered							
Channel	0	1	2	3	4	5	6	7
Output (+24 V)	-	-	-	-	9	13	17	21
lout	1	3	5	7	10	14	18	22
Earth (-)	2	4	6	8	12	16	20	24
Because of the functionality, in a mixed input output configuration, the inputs (lin) are switched off as well, but this is not part of the safety function!								

For safety applications only the described variant of the Universal Module HART 9469 have been considered. All other possible variants and configurations are not covered by this report.

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]).

The Universal Module HART 9469 can be considered to be Type A¹ element with a hardware fault tolerance of 0. Only the Plant Stop Function of the Universal Module HART 9469 was considered.

The failure rates are valid for the useful life of the Universal Module HART 9469 (see Appendix A) when operating as defined in the considered scenarios

The following table show how the above stated requirements are fulfilled for the considered Universal Module HART 9469.

¹ 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 of Universal Module HART 9469, 2- wire output per IEC 61508:2010

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	17
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})²	10
Fail Annunciation Undetected (λ_{AU}) ³	9
No effect	138
No part	0
Total failure rate (safety function)	27
Safe failure fraction (SFF)⁴	61%
SIL AC⁵	SIL2

² λ_{DU} includes 5% common cause failures between redundant components of disconnection circuit.

³ Failures of redundant components of the Plant- STOP function are part of Annunciation Undetected failures.

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

⁵ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD values.

Table 3: Failure rates of Universal Module HART 9469, 4- wire output per IEC 61508:2010

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	19
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})⁶	7
Fail Annunciation Undetected (λ_{AU}) ⁷	19
No effect	129
No part	0
Total failure rate (safety function)	26
Safe failure fraction (SFF)⁸	73%
SIL AC⁹	SIL2

⁶ λ_{DU} includes 5% common cause failures between redundant components of disconnection circuit.

⁷ Failures of redundant components of the Plant- STOP function are part of Annunciation Undetected failures.

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

⁹ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD values.

Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved.....	7
2.3 Standards / Literature used.....	8
2.4 <i>exida</i> tools used	8
2.5 Reference documents.....	9
2.5.1 Documentation provided by the customer.....	9
2.5.2 Documentation generated by the customer and <i>exida</i>	9
3 Product Description.....	10
4 Failure Modes, Effects, and Diagnostic Analysis	11
4.1 Description of the failure categories.....	11
4.2 Methodology – FMEDA, Failure rates	12
4.2.1 FMEDA.....	12
4.2.2 Failure rates	12
4.2.3 Assumptions.....	13
4.3 Results.....	14
4.3.1 Failure rates of Universal Module HART 9469, 2- wire output per IEC 61508:2010	15
4.3.2 Failure rates of Universal Module HART 9469, 4- wire output per IEC 61508:2010	16
5 Using the FMEDA results.....	17
5.1 Example PFD _{AVG} / PFH calculation.....	18
6 Terms and Definitions	20
7 Status of the document	21
7.1 Liability.....	21
7.2 Releases	21
7.3 Release Signatures.....	21
Appendix A: Lifetime of Critical Components.....	22
Appendix B: Proof tests to detect dangerous undetected faults	23

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Universal Module HART 9469 with hardware version as listed in the drawings referenced in section 2.5.1.

The FMEDA builds the basis for an evaluation whether an element including the described Universal Module HART 9469 meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

R. STAHL Schaltgeräte GmbH Manufacturer of the Universal Module HART 9469.

exida Performed the hardware assessment.

R. STAHL Schaltgeräte GmbH contracted *exida* in August 2018 with the review of the FMEDA of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	SN 29500-1:01.2004 SN 29500-1 H1:07.2013 SN 29500-2:09.2010 SN 29500-3:06.2009 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 29500-11:07.2013 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Siemens standard with failure rates for components
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N6]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 *exida* tools used

[T1]	SILcal, V9.00.93	<i>exida</i> FMEDA Tool
[T2]	exSILentia, V3.3.0.903	used for PFD _{AVG} calculation

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	9400 0 000 050 0_00.docx	Product and functional safety description, Index 0 of 09.01.2019
[D2]	9469 6 020 010 0_03.pdf	Circuit diagram, Index 3 of 05.06.2018
[D3]	946960310010_00_de_en.pdf	Datasheet V0 of 19.02.2018

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.5.2 Documentation generated by the customer and *exida*

[R1]	FMEDA_Stahl-9469-V1R1.efmx
------	----------------------------

3 Product Description

The Universal Module HART 9469 is universal supply unit for 2-wire or 4-wire signal transformer. It can also be used as supply for output for final elements. It is intended to be used in explosion hazardous areas. Safe state of the Universal Module HART 9469 is to switch-off the supply voltage of the output signals, which is leading to signal loss in case of use as signal transformer or power down in case of use as supply for final elements.

The usecase of the available outputs can be configured by software. The configuration and the controller part of the Universal Module HART 9469 is not part of the safety function, so only the power-down part was considered and thereby, it can be considered to be Type A element with a hardware fault tolerance of 0. Decoupling components are also part of the safety function.

The safety function of the Universal Module HART 9469 is to switch-off the supply voltage of the output signals by using the Plant-STOP function. This function is only available, if the analog or digital output of the Universal Module HART 9469 is used in an application.

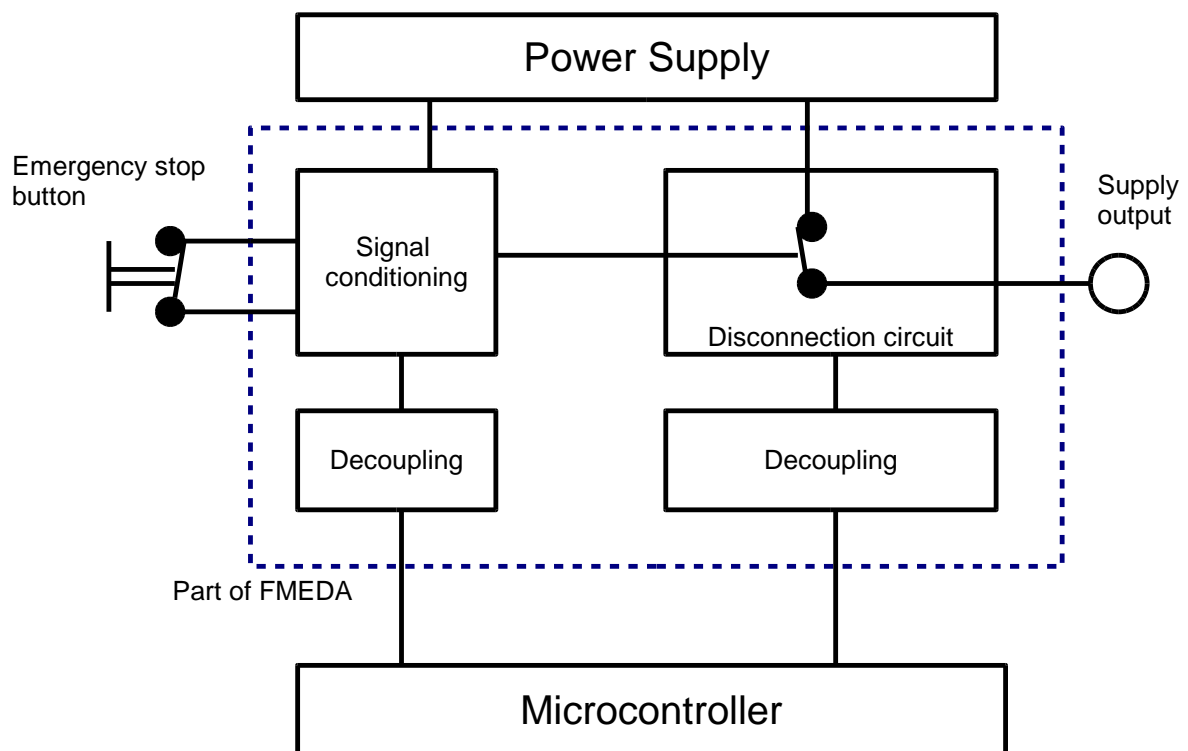


Figure 1: Block diagram of Universal Module HART 9469

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with R. STAHL Schaltgeräte GmbH and is documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the Universal Module HART 9469, the following definitions for the failure of the products were considered.

Fail-Safe State	The fail-safe state is defined as the output is switched off.
Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).
Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (DD).
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.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

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

4.2.2 Failure rates

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]). The rates were chosen in a way that is appropriate for safety integrity level verification calculations and the intended applications. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining their applicability to any particular environment. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Universal Module HART 9469.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The Universal Module HART 9469 is installed per the manufacturer's instructions.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. For higher average temperatures, the failure rates should be multiplied with an experience based factor of e.g. 1.5 for 50°C, 2.5 for 60°C and 5 for 80°C.
- Only the described variants can be used for safety applications.
- Only the shut-off path of the Universal Module HART 9469 was considered. The controller part is decoupled from the signal path and thereby not part of the safety function.
- Leakage currents ≤ 1.5 mA and 5.3 V for 4-wire output or ≤ 0.1 mA and 5.3 V for 2-wire output are assumed to be uncritical and thereby safe failures.

4.3 Results

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

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

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

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-2.

This assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the Universal Module HART 9469 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 Failure rates of Universal Module HART 9469, 2- wire output per IEC 61508:2010

The FMEDA carried out on the Universal Module HART 9469 under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.3 leads to the following failure rates:

Table 4: FMEDA results of Universal Module HART 9469 - 2 wire output

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	17
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})¹⁰	10
Fail Annunciation Undetected (λ_{AU}) ¹¹	9
No effect	138
No part	0
Total failure rate (safety function)	27
Safe failure fraction (SFF)¹²	61%
SIL AC¹³	SIL2

¹⁰ λ_{DU} includes 5% common cause failures between redundant components of disconnection circuit.

¹¹ Failures of redundant components of the Plant- STOP function are part of Annunciation Undetected failures.

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 but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD values.

4.3.2 Failure rates of Universal Module HART 9469, 4- wire output per IEC 61508:2010

The FMEDA carried out on the Universal Module HART 9469 under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.3 leads to the following failure rates:

Table 5: FMEDA results of Universal Module HART 9469 - 4 wire output

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	19
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})¹⁴	7
Fail Annunciation Undetected (λ_{AU}) ¹⁵	19
No effect	129
No part	0
Total failure rate (safety function)	26
Safe failure fraction (SFF)¹⁶	73%
SIL AC¹⁷	SIL2

¹⁴ λ_{DU} includes 5% common cause failures between redundant components of disconnection circuit.

¹⁵ Failures of redundant components of the Plant- STOP function are part of Annunciation Undetected failures.

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 but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD values.

5 Using the FMEDA results

Using the failure rate data displayed in section 4.3, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{AVG}) calculation can be performed for the entire safety function.

Probability of Failure on Demand (PFD_{AVG}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{AVG}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{AVG} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{AVG}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix C for a complete description of how to determine the Safety Integrity Level for an entire safety function. The mission time used for the calculation depends on the PFD_{AVG} target and the useful life of the product. The failure rates for all the devices of the safety function and the corresponding proof test coverages are required to perform the PFD_{AVG} calculation. The proof test coverage of the suggested proof test for the Universal Module HART 9469 is listed in Appendix B. This is combined with the dangerous failure rates after proof test for other devices to establish the proof test coverage for the entire safety function.

When performing testing at regular intervals, the Universal Module HART 9469 contribute less to the overall PFD_{AVG} of the Safety Instrumented Function.

The following section gives a simplified example on how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for Universal Module HART 9469. The failure rate data used in this calculation are displayed in sections 4.3.1. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 6 lists the results for different proof test intervals considering an average proof test coverage of 99% (see Appendix B).

Table 6: Universal Module HART 9469 – PFD_{AVG} / PFH values

	T[Proof]			
	1 year	2 years	5 years	10 years
9469, 2 wire output	PFD _{AVG} = 4.98 E-05	PFD _{AVG} = 9.51 E-05	PFD _{AVG} = 2.31 E-4	PFD _{AVG} = 4.58 E-4
9469, 4 wire output	PFD _{AVG} = 3.39 E-05	PFD _{AVG} = 6.47 E-05	PFD _{AVG} = 1.57 E-4	PFD _{AVG} = 3.11 E-4

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02. As the Universal Module HART 9469 is contributing to the 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 1.0E-03. The calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of the allowed range, i.e. to be better than or equal to 1.0E-03.

The resulting PFD_{AVG} graph is generated for a proof test of 1 year are displayed in Figure 2.

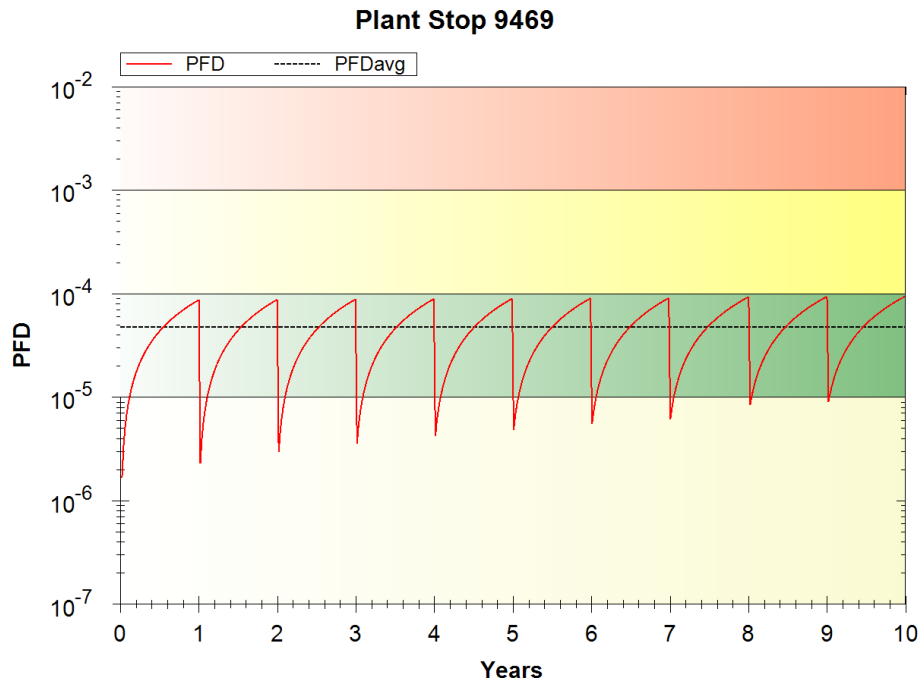


Figure 2: PFD_{AVG}(t) of 2- wire output

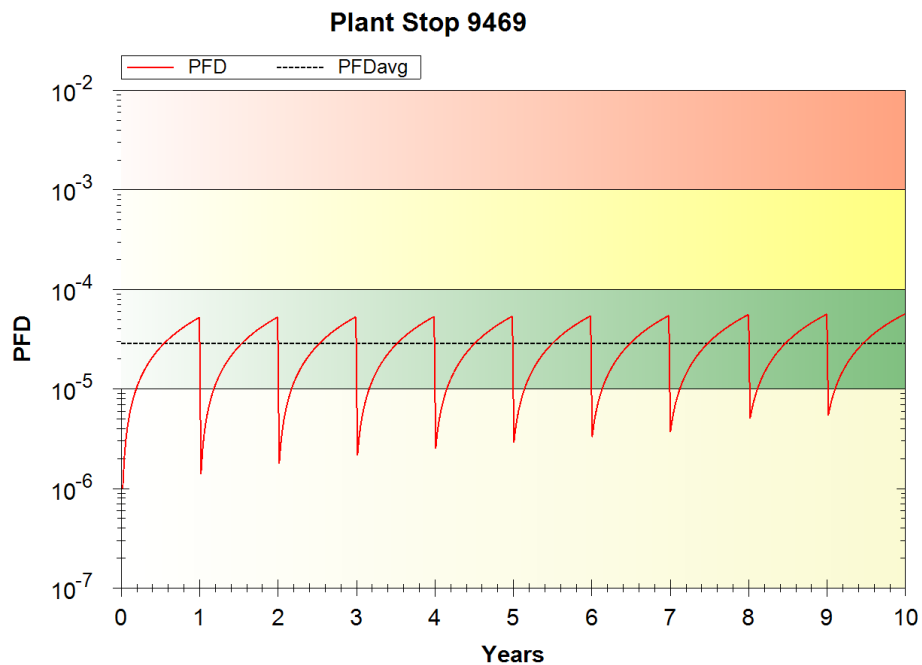


Figure 3: PFD_{AVG}(t) of 4- wire output

6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
DC	Diagnostic Coverage of dangerous failures ($DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$)
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTBF	Mean Time Between Failures
MTTF _d	Mean Time To dangerous Failure
MTTR	Mean Time To Restoration
PFD _{AVG}	Average Probability of Failure on Demand
SIF	Safety Instrumented Function
SIL	Safety Integrity Level IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

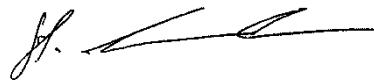
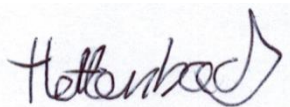
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

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

7.2 Releases

Version History: V1R1: Results updated; February 11, 2019
V1R0: Review comments included; February 5, 2019
V0R1: Initial version; December 20, 2018
Author: Jan Hettenbach
Review: V0R1: Andreas Bagusch (R. STAHL Schaltgeräte GmbH), Stephan Aschenbrenner (*exida*)
Release status: V1R0: Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures



Dipl.-Ing. (Univ.) Jan Hettenbach

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

Appendix A: Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime¹⁸ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

There are no components with reduced life-time within the considered safety function.

¹⁸ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B: Proof tests to detect dangerous undetected faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

A suggested proof test consists of the following steps, as described Table 7.

Table 7 Steps for Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Force the Universal Module HART 9469 to go to the safe state and verify that the safe state is reached.
3.	Measure the output current of each channel if it is less than 1.5 mA and 5.3 V for 4-wire output and less than 0.1 mA and 5.3 V for 2-wire output
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect 99% of possible “du” failures.