



Failure Modes, Effects and Diagnostic Analysis

Project:
Plant-STOP 9475

Company:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 13/04-027
Report No.: STAHL 13/04-027 R024
Version V1, Revision R0; August 2013
Jan Hettenbach

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Plant-STOP 9475 in the version listed in the drawings referenced in section 2.4.1.

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

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

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5 and for a temperature of 75°C multiplied by factor of 4.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

These failure rates are valid for the useful lifetime of the Plant-STOP 9475, see Appendix B.

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

The Plant-STOP 9475 can be classified as a Type A¹ element according to IEC 61508, having a hardware fault tolerance of 0. The failure rates according to IEC 61508:2010 for the Plant-STOP 9475 are listed in the following table.

The Plant-STOP 9475 has two different input types, which are evaluated independent of each other. The types are shown in Table 1. During operation, only one input may be active. A combination of both input types is not allowed and not covered by this report.

There are different variants of the Plant-STOP 9475 available, which differ only in output voltage range or maximum allowable current to match the electrical requirements of the connected components. An overview of all covered types is shown in Table 2.

For safety applications only the described variants were considered. All other possible variants are not covered by this report.

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 1: Input type definition of Plant-STOP 9475

Input type definition	Description
Plant-STOP 9475 I	Input for direct connection of passive contacts
Plant-STOP 9475 II	Input for connection of active signal sources

Table 2: Covered types of Plant-STOP 9475

Type	Description
9475/32-04-12	4 channels / $U_N = 17,9 \text{ V}$ (11,3 V / 40 mA), installation in zone 1
9475/33-04-12	4 channels / $U_N = 17,9 \text{ V}$ (11,3 V / 40 mA), installation in zone 2
9475/32-04-22	4 channels / $U_N = 23,6 \text{ V}$ (12,3 V / 40 mA), installation in zone 1
9475/33-04-22	4 channels / $U_N = 23,6 \text{ V}$ (12,3 V / 40 mA), installation in zone 2
9475/32-04-72	4 channels / $U_N = 13,8 \text{ V}$ (12,3 V / 75 mA), installation in zone 1
9475/33-04-72	4 channels / $U_N = 13,8 \text{ V}$ (12,3 V / 75 mA), installation in zone 2
9475/32-08-52	8 channels / $U_N = 17,5 \text{ V}$ (12,6 V / 30 mA), installation in zone 1
9475/33-08-52	8 channels / $U_N = 17,5 \text{ V}$ (12,6 V / 30 mA), installation in zone 2
9475/32-08-62	8 channels / $U_N = 23,5 \text{ V}$ (17,5 V / 20 mA), installation in zone 1
9475/33-08-62	8 channels / $U_N = 23,5 \text{ V}$ (17,5 V / 20 mA), installation in zone 2

Table 3: Plant-STOP 9475 I according to IEC 61508:2010

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU}) ²	58
Fail Dangerous Detected (λ_{DD}) ³	34
Fail Dangerous Detected (λ_{DD})	34
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Undetected (λ_{AU}) ⁴	37
No effect	101
No part	51
Total failure rate (safety function) ⁵	120
Safe failure fraction (SFF) ⁶	76%
SIL AC ⁷	SIL2

² SU failures are all failures, which are leading to safe state. The Plant- STOP 9475 has two switches to disconnect the output current. Only safe failures of one switch are classified as SU failures.

³ The Plant- STOP 9475 has no real detection circuit, but a redundant switch to disconnect output current. The redundant switch is classified as diagnostic path to consider the redundancy. In a DD condition, a failure in the primary switching path is "detected" by the second switch and a safe state can be reached. Assumed DC = 90% ($\beta = 10\%$)

⁴ The redundant switch is classified as diagnostic circuit. All failures of the redundant switch, which are leading to a safe state, are classified as AU failures.

⁵ The total failure rate includes the input circuit and only one output circuit. Up to 8 output circuits are connected to the input circuit.

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

⁷ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table 4: Plant-STOP 9475 II according to IEC 61508:2010

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU}) ⁸	83
Fail Dangerous Detected (λ_{DD}) ⁹	34
Fail Dangerous Detected (λ_{DD})	34
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Undetected (λ_{AU}) ¹⁰	37
No effect	79
No part	48
Total failure rate (safety function) ¹¹	145
Safe failure fraction (SFF) ¹²	80%
SIL AC ¹³	SIL2

⁸ SU failures are all failures, which are leading to safe state. The Plant- STOP 9475 has two switches to disconnect the output current. Only safe failures of one switch are classified as SU failures.

⁹ The Plant- STOP 9475 has no real detection circuit, but a redundant switch to disconnect output current. The redundant switch is classified as diagnostic path to consider the redundancy. In a DD condition, a failure in the primary switching path is "detected" by the second switch and a safe state can be reached. Assumed DC = 90% ($\beta = 10\%$)

¹⁰ The redundant switch is classified as diagnostic circuit. All failures of the redundant switch, which are leading to a safe state, are classified as AU failures.

¹¹ The total failure rate includes the input circuit and only one output circuit. Up to 8 output circuits are connected to the input circuit.

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

¹³ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table of Contents

Management Summary	2
1 Purpose and Scope.....	7
2 Project Management.....	8
2.1 <i>exida</i>	8
2.2 Roles of the parties involved.....	8
2.3 Standards and Literature used	9
2.4 Reference documents	10
2.4.1 Documentation provided by the customer	10
2.4.2 Documentation generated by <i>exida</i>	10
3 Product Description.....	11
4 Failure Modes, Effects, and Diagnostic Analysis.....	12
4.1 Description of the failure categories	12
4.2 Methodology – FMEDA, Failure Rates	13
4.2.1 FMEDA	13
4.2.2 Failure Rates	13
4.2.3 Assumptions	14
4.3 Results of the assessment	15
4.3.1 Plant-STOP 9475 I.....	16
4.3.2 Plant-STOP 9475 II.....	17
5 Using the FMEDA Results	18
5.1 Example PFD _{AVG} calculation.....	18
6 Terms and Definitions	19
7 Status of the Document.....	20
7.1 Liability.....	20
7.2 Releases.....	20
Appendix A: Possibilities to reveal dangerous undetected faults during the proof test ..	21
Appendix A.1: Possible proof tests to detect dangerous undetected faults	21
Appendix B: Impact of lifetime of critical components on the failure rate	22
Appendix A Appendix C: <i>exida</i> Environmental Profiles	23

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Plant-STOP 9475. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the described Plant-STOP 9475 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project Management

2.1 *exida*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

R. STAHL Schaltgeräte GmbH Manufacturer of the Plant-STOP 9475 and carried out the FMEDA.

exida Reviewed the FMEDAs and issued this report.

R. STAHL Schaltgeräte GmbH contracted *exida* in April 2013 to review the FMEDA and to issue the report.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; 2nd edition
[N2]	SN 29500-1:01.2004 SN 29500-1 H1:12.2005 SN 29500-2:12.2004 SN 29500-3:12.2004 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:08.1990 SN 29500-12:03.1994 SN 29500-13:03.1994 SN 29500-14:03.1994	Siemens standard with failure rates for components
[N3]	Electrical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N4]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	9475 0 000 007 0_02.pdf	Schematic diagram of 14.03.2013
[D2]	9475 0 000 007 4_01.pdf	Parts list of all populated components, index 01 of 15.03.2013
[D3]	9475 0 000 050 0_00.docx	Technical description of safety concept of 26.03.2013
[D4]	9475626310_en.pdf	Operation instructions of 13.03.2013
[D5]	9475 0 000 051 0_00.efm	FMEDA of IS1+ 9475 Plant STOP I of 27.03.2013
[D6]	9475 0 000 052 0_00.efm	FMEDA of IS1+ 9475 Plant STOP II of 27.03.2013

2.4.2 Documentation generated by *exida*

[R1]	Summary FMEDA results Plant-STOP 9475.xls of 04.06.2013
[R2]	PFDavg Calc Plant-STOP 9475.xls of 23.07.2013

3 Product Description

The Plant-STOP 9475 can be classified as a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

The digital output module is used for connecting of up to 8 intrinsically safe hydraulic or solenoid valves to the IS1 remote I/O system. The additional Ex i control input "Plant STOP" is used for safe switching off of all outputs. All channels are individually monitored for wire breakage and short-circuit. The Ex i outputs are short-circuit proof, electrically connected to each other and electrically separated from the system. Some internal circuits are designed redundant for higher reliability.

Figure 2 shows the connection diagram of the Plant-STOP 9475. Inputs 1-2 are can be connected with emergency stop switches, Inputs 3-4 can be connected to active signal sources. One emergency stop signal input signal can switch up to 8 outputs.



Figure 1: Plant-STOP 9475

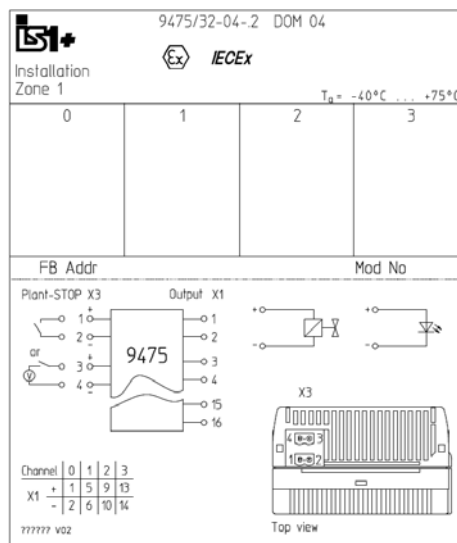


Figure 2: Connection diagram of Plant-STOP 9475

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented [D5] and [D6].

4.1 Description of the failure categories

In order to judge the failure behavior of the Plant-STOP 9475, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the output is de-energized with currents less than 200 μ A.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics or is uncritical because of redundant channels.
Annunciation	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. The Plant-STOP 9475 has no special diagnostic function, but failures of the redundant switch off path are classified as AU failures.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

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

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

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical [N3] and Mechanical [N4] Component Reliability Handbook which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to *exida* Profile 1. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

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

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

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

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Plant-STOP 9475.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- All devices are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described variants are considered.
- Only one output is part of the considered safety function. The other outputs are assumed to be identical.
- Sufficient tests are performed to show the independency between safety functions and the non-safety related parts of the circuit.
- Residual currents less than 200 μ A are low enough to switch off any connected load and rated as noncritical.
- Redundant parts of the circuit are classified as diagnostic circuits which protect the main signal path.

4.3 Results of the assessment

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

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

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

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

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

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-3.

This assessment supports the 1_H approach.

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

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the Plant-STOP 9475 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 Plant-STOP 9475 I

The FMEDA carried out on the Plant-STOP 9475 I for the passive input leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates:

Table 5: Plant-STOP 9475 I according to IEC 61508:2010

	<i>exida</i> Profile 1
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU}) ¹⁴	58
Fail Dangerous Detected (λ_{DD}) ¹⁵	34
Fail Dangerous Detected (λ_{DD})	34
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Undetected (λ_{AU}) ¹⁶	37
No effect	101
No part	51
Total failure rate (safety function) ¹⁷	120
Safe failure fraction (SFF) ¹⁸	76%
SIL AC ¹⁹	SIL2

¹⁴ SU failures are all failures, which are leading to safe state. The Plant- STOP 9475 has two switches to disconnect the output current. Only safe failures of one switch are classified as SU failures.

¹⁵ The Plant- STOP 9475 has no real detection circuit, but a redundant switch to disconnect output current. The redundant switch is classified as diagnostic path to consider the redundancy. In a DD condition, a failure in the primary switching path is "detected" by the second switch and a safe state can be reached. Assumed DC = 90% ($\beta = 10\%$)

¹⁶ The redundant switch is classified as diagnostic circuit. All failures of the redundant switch, which are leading to a safe state, are classified as AU failures.

¹⁷ The total failure rate includes the input circuit and only one output circuit. Up to 8 output circuits are connected to the input circuit.

¹⁸ The complete final element 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 but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

4.3.2 Plant-STOP 9475 II

The FMEDA carried out on the Plant-STOP 9475 II for the active signal input leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates:

Table 6: Plant-STOP 9475 II according to IEC 61508:2010

	<i>exida</i> Profile 1
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU}) ²⁰	83
Fail Dangerous Detected (λ_{DD}) ²¹	34
Fail Dangerous Detected (λ_{DD})	34
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Undetected (λ_{AU}) ²²	37
No effect	79
No part	48
Total failure rate (safety function) ²³	145
Safe failure fraction (SFF) ²⁴	80%
SIL AC ²⁵	SIL2

²⁰ SU failures are all failures, which are leading to safe state. The Plant- STOP 9475 has two switches to disconnect the output current. Only safe failures of one switch are classified as SU failures.

²¹ The Plant- STOP 9475 has no real detection circuit, but a redundant switch to disconnect output current. The redundant switch is classified as diagnostic path to consider the redundancy. In a DD condition, a failure in the primary switching path is "detected" by the second switch and a safe state can be reached. Assumed DC = 90% ($\beta = 10\%$)

²² The redundant switch is classified as diagnostic circuit. All failures of the redundant switch, which are leading to a safe state, are classified as AU failures.

²³ The total failure rate includes the input circuit and only one output circuit. Up to 8 output circuits are connected to the input circuit.

²⁴ The complete final element 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 but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

5 Using the FMEDA Results

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

5.1 Example PFD_{AVG} calculation

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

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

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for Plant-STOP 9475 considering a proof test coverage of 99% (see Appendix A.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in sections [R1]. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 7. Both inputs (input I and input II) have the same PFD_{AVG} values.

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

Table 7: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	T[Proof] = 10 years	T[Proof] = 15 years
$PFD_{AVG} = 2.29E-04$	$PFD_{AVG} = 3.34E-04$	$PFD_{AVG} = 6.62E-04$	$PFD_{AVG} = 1.20E-03$	$PFD_{AVG} = 1.74E-03$

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval considering profile 1 data is approximately equal to 2.29%.

Figure 3 shows the time dependent curve of PFD_{AVG} .

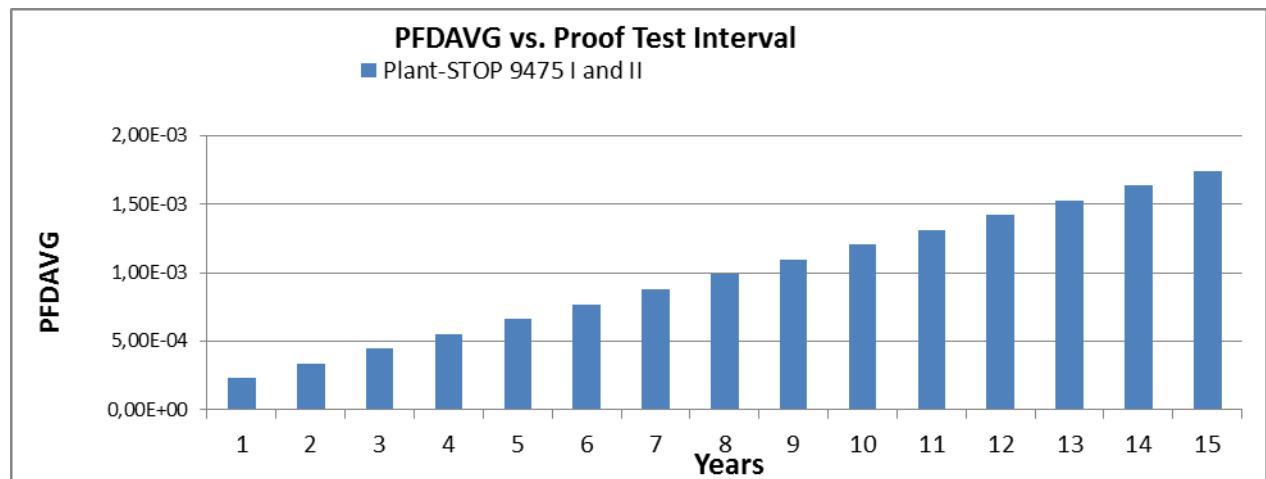


Figure 3: $PFD_{AVG}(t)$ for Plant-STOP I and II

6 Terms and Definitions

FIT	Failure In Time (1x10 ⁻⁹ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
PLC	Programmable Logic Controller
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

7 Status of the Document

7.1 Liability

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

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

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

7.2 Releases

Version History: V1R0: Editorial changes, August 26, 2013

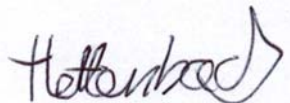
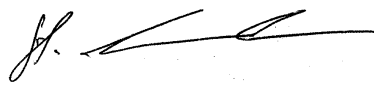
V0R1: Initial draft; July 17, 2013

Author: Jan Hettenbach

Review: Stephan Aschenbrenner (*exida*), Andreas Bagusch (R. STAHL Schaltgeräte GmbH)

Release Status: V1R0 Released to R. STAHL Schaltgeräte GmbH

7.3 Release Signatures

Handwritten signature of Jan Hettenbach in black ink.Handwritten signature of Stephan Aschenbrenner in black ink.

Dipl. -Ing. (Univ.) Jan Hettenbach

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

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

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

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

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

A suggested proof test consists of the following steps, as described in Table 8. It is assumed that this test will detect 99% of possible dangerous failures.

Table 8: Steps for proof test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Force the Plant-STOP 9475 to go to the safe state and verify that the safe state is reached.
3.	Measure the output current if it is less than 200 μ A in safe state.
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or otherwise restore normal operation.

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime²⁶ of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

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

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

Table 9 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 9: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life
Opto-coupler - With bipolar output	O402, O403	More than 15 years

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

²⁶ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix C: *exida* Environmental Profiles

Table 10 *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted	General Field Mounted	Subsea	Offshore	N/A
		no self-heating	self-heating			
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3	C3	N/A	C3	N/A
		also applicable for D1	also applicable for D1		also applicable for D1	
Average Ambient Temperature	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity²⁷	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock²⁸	10 g	15 g	15 g	15 g	15 g	N/A
Vibration²⁹	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion³⁰	G2	G3	G3	G3	G3	Compatible Material
Surge³¹						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility³²						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)³³	6kV	6kV	6kV	6kV	6kV	N/A

²⁷ Humidity rating per IEC 60068-2-3

²⁸ Shock rating per IEC 60068-2-6

²⁹ Vibration rating per IEC 60770-1

³⁰ Chemical Corrosion rating per ISA 71.04

³¹ Surge rating per IEC 61000-4-5

³² EMI Susceptibility rating per IEC 6100-4-3

³³ ESD (Air) rating per IEC 61000-4-2

Appendix D: FMEDA results according to IEC 61508:2000

Table 11: Plant-STOP 9475 I according to IEC 61508:2000

	<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})	101
Fail safe undetected	0
No effect	101
Fail Dangerous Detected (λ_{DD})	31
Fail detected (detected by internal diagnostics)	31
Fail Dangerous Undetected (λ_{DU})	65
Fail dangerous undetected	28
Annunciation undetected	37
No part	51

Total failure rate (safety function)	197
Safe failure fraction (SFF)	88%
DC_D	53%
SIL AC	SIL2

Table 12: Plant-STOP 9475 II according to IEC 61508:2000

<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})	79
Fail safe undetected	0
No effect	79
Fail Dangerous Detected (λ_{DD})	31
Fail detected (detected by internal diagnostics)	31
Fail Dangerous Undetected (λ_{DU})	65
Fail dangerous undetected	28
Annunciation undetected	37
No part	48

Total failure rate (safety function)	175
Safe failure fraction (SFF)	88%
DC_D	53%

SIL AC	SIL2
---------------	-------------