



Failure Modes, Effects and Diagnostic Analysis

Project:

Switching Repeater 9170/*1

Customer:

R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 09/03-52

Report No.: STAHL 09/03-52 R019

Version V3, Revision R0; September 2015

Jan Hettenbach

Management summary

This report summarizes the results of the hardware assessment carried out on the switching repeater 9170/*1, Revision E. Table 1 gives an overview of the different configurations that belong to the considered switching repeater 9170/*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.

Table 1: Configuration overview ¹

Switching repeater	Type	9170 /	*a	*b	-	*c	*d	-	*e	*f
Channels	1	1								
	2	2								
Design	U _o 9,6 V, I _o 10 mA	1								
Input	NAMUR	1								
	Enhanced hysteresis	6								
Output	Signal relay: 1 CO per Channel	0								
	Signal relay: single Ch.: 2 CO dual Ch.: 2 NO per Channel	1								
	Power relay: 1 CO per Channel	2								
	Power relay: single Ch.: 2 CO	3								
	Electronic output	4								
Power supply	24 V DC; I.S. version	1								
	120/230 V AC; I.S. version	2								
	24 V DC; non I.S. version	6								
Line fault detection	With	1								
	With, transparent to output	2								
	With, only LED indication	3								

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

¹ The results presented afterwards are also valid for configurations with b = 0, Rev. E as the design is identical.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1. The analysis has been 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. Profile 3 has also similar failure rates since the thermal stress profile is similar for the used hardware components.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed. These failure rates are valid for the useful lifetime of the 9170/*1, see Appendix 2.

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

The switching repeater 9170/*1 is considered to be a Type A² element with a hardware fault tolerance of 0. For Type A elements with a hardware fault tolerance of 0 the SFF has to be > 60% for SIL 2 elements. The following tables show how the above stated requirements are fulfilled.

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

Table 2: Summary for 9170/a1-c2-ef³ – IEC 61508: 2010 failure rates

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	120
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	89
No part	39
Total failure rate (safety function)	201
Safe failure fraction (SFF) ⁴	64%
SIL AC ⁵	SIL2
PFH	7.2E-8 1/h

³ e = 1 or 6.

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

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

Table 3: Summary for 9170/a1-c2-2f / 9170/a1-c3-2f – IEC 61508 failure rates

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	167
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	103
No part	39
Total failure rate (safety function)	248
Safe failure fraction (SFF) ⁶	70%
SIL AC ⁷	SIL2
PFH	7.2E-8 1/h

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

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

Table 4: Summary for 9170/a1-c4-ef⁸ – IEC 61508 failure rates

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	7
Fail Safe Undetected (λ_{SU})	106
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	21
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	125
No part	58
Total failure rate (safety function)	135
Safe failure fraction (SFF)⁹	84%
SIL AC¹⁰	SIL2
PFH	2.1E-8 1/h

⁸ e = 1 or 6.

⁹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁰ 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 5: Summary for 9170/a1-cd-ef¹¹ – IEC 61508 failure rates

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	92
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	81
No part	39
Total failure rate (safety function)	129
Safe failure fraction (SFF)¹²	78%
SIL AC¹³	SIL2
PFH	2.8E-8 1/h

¹¹ d = 0 or 1; e = 1 or 6.

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

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

Table 6: Summary for 9170/a1-cd-2f¹⁴ – IEC 61508 failure rates

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	139
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	28
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	95
No part	40
Total failure rate (safety function)	176
Safe failure fraction (SFF)¹⁵	84%
SIL AC¹⁶	SIL2
PFH	2.8E-8 1/h

¹⁴ d = 0 or 1.

¹⁵ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

¹⁶ 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	10
2 Project management.....	11
2.1 <i>exida</i>	11
2.2 Roles of the parties involved.....	11
2.3 Standards / Literature used.....	11
2.4 Reference documents.....	12
2.4.1 Documentation provided by the customer.....	12
2.4.2 Documentation generated by <i>exida</i>	12
3 Description of the analyzed module	13
3.1 Switching Repeater 9170/*1	13
4 Failure Modes, Effects, and Diagnostic Analysis	14
4.1 Description of the failure categories.....	14
4.2 Methodology – FMEDA, Failure rates	15
4.2.1 FMEDA.....	15
4.2.2 Failure rates	15
4.2.3 Assumptions.....	16
4.3 Results	17
4.3.1 Switching repeater 9170/a1-c2-ef	18
4.3.2 Switching repeater 9170/a1-c2-2f / 9170/a1-c3-2f	19
4.3.3 Switching repeater 9170/a1-c4-ef	20
4.3.4 Switching repeater 9170/a1-cd-ef	21
4.3.5 Switching repeater 9170/a1-cd-2f	22
5 Using the FMEDA results.....	23
6 Terms and Definitions	24
7 Status of the document.....	25
7.1 Liability.....	25
7.2 Releases	25
7.3 Release signatures	25
Appendix 1: Possible proof tests to detect dangerous undetected faults.....	26
Appendix 2: Impact of lifetime of critical components on the failure rate	26
Appendix 3: <i>exida</i> Environmental Profiles.....	27

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 switching repeater 9170/*1.

The FMEDA builds the basis for an evaluation whether a final element subsystem, including the described switching repeater 9170/*1 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 switching repeater 9170/*1.

exida reviewed the FMEDA and issued this report.

R. STAHL Schaltgeräte GmbH contracted *exida* in May 2015 with the update of the FMEDA report 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 61508-2:2000	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]	91 706 03 20 0_05_20150109.pdf	Circuit diagram 91 706 03 20 0 „Switching repeater Type 9170/.1-...“ index 05 of 09.01.15
[D2]	STL 9170_03_090205.xlsx	Parts list for switching repeater 9170/*1
[D3]	B9170_de_en_screen.pdf	Operating instructions S-BA-9170-003-de/en-01/2005
[D4]	B9170_de_en_draft transparent LFD_081007.pdf	Operating instructions B9170 de/en-11/2007
[D5]	9170 Erweiterung _x1 Varianten_C.xlsx of 17.04.09	Configuration overview
[D6]	9170 Varianten ohne Fehlermeldung.docx of 04.01.11	Updated configuration overview
[D7]	Useful lifetime 9170_x1.pdf	Useful lifetime analysis
[D8]	FMEDA V5 9170_a1-c2-11 V1_1.xls of 17.04.09	
[D9]	FMEDA V5 9170_a1-c2-21 V1_1.xls of 17.04.09	
[D10]	FMEDA V5 9170_a1-c4-1f V1_1.xls of 17.04.09	
[D11]	FMEDA V5 9170_a1-cd-11 V1_1.xls of 17.04.09	
[D12]	FMEDA V5 9170_a1-cd-21 V1_1.xls of 17.04.09	

2.4.2 Documentation generated by exida

[R1]	FMEDA V5 9170 complete V1.0.xls of 07.02.06
[R2]	AW 9170 Überarbeitete Version.msg of 17.04.09
[R3]	FMEDA V5 9170_a1-cd-11 V1_3.xls of 27.05.09
[R4]	FMEDA V5 9170_a1-cd-21 V1_3.xls of 27.05.09

3 Description of the analyzed module

3.1 Switching Repeater 9170/*1

Switching repeaters are used for intrinsically safe operation of contacts, proximity switches as defined by EN 60947-5-6 (NAMUR), opto-coupler outputs, etc.

Output variants equipped with signal relays, power relays or opto-couplers meet varying requirements.

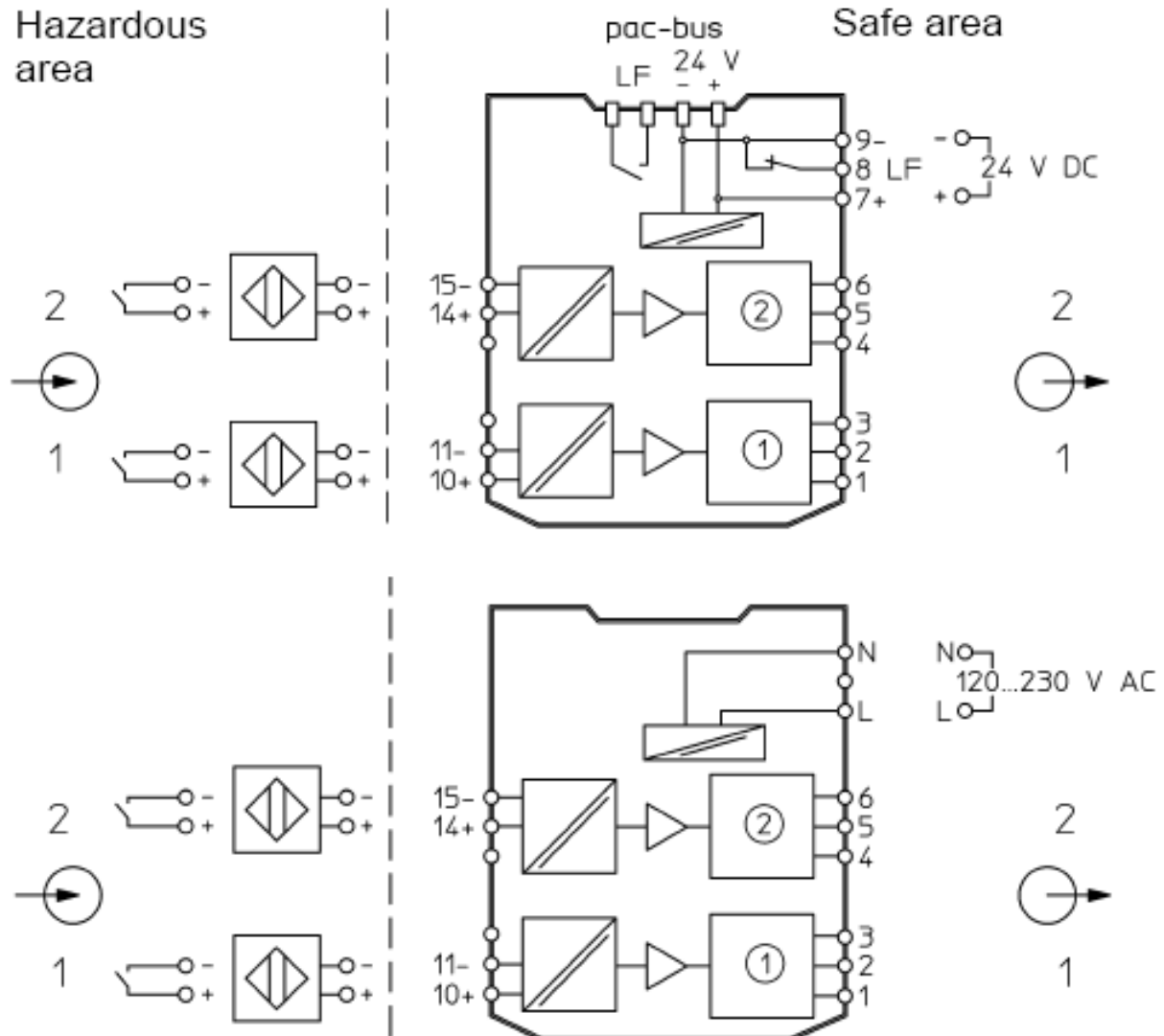


Figure 1: Block diagrams of the switching repeaters 9170/*1-1*-11 and 9170/*1-1*-21

The switching repeater 9170/*1 is considered to be a Type A¹⁷ element with a hardware fault tolerance of 0.

¹⁷ Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented in [D8] to [D10] and [R3] to [R4].

4.1 Description of the failure categories

In order to judge the failure behavior of the switching repeater 9170/*1, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: <ul style="list-style-type: none">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: <ul style="list-style-type: none">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 (DU).
Fail Dangerous Detected	Failure that is dangerous but is detected by internal or external 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.
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 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.

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 switching repeater 9170/*1.

- 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.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- 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.
- All modules are operated in the low demand mode of operation.
- 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.
- For safety applications only the described outputs are considered.
- Only one input and one output are part of the considered safety function.
- The power relay outputs (d = 2 and 3 according to Table 1) are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- The signal relay outputs (d = 0 and 1 according to Table 1) are only connected to resistive load and to maximum 100mA.
- Short circuit and lead breakage detection are activated.

4.3 Results

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

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

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

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

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

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

This assessment supports the 1_H approach.

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

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the switching repeater 9170/*1 is only one part of an element, the architectural constraints should be determined for the entire sensor element

4.3.1 Switching repeater 9170/a1-c2-ef ¹⁸

The FMEDA carried out on the switching repeater 9170/a1-c2-ef leads under the assumptions described in section 4.2.3 to the following failure rates:

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	120
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	89
No part	39

Total failure rate (safety function)	201
Safe failure fraction (SFF) ¹⁹	64%

SIL AC ²⁰	SIL2
PFH	7.2E-8 1/h

¹⁸ e = 1 or 6.

¹⁹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²⁰ 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 Switching repeater 9170/a1-c2-2f / 9170/a1-c3-2f

The FMEDA carried out on the switching repeater 9170/a1-c2-2f leads under the assumptions described in section 4.2.3 to the following failure rates:

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	167
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72
Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	103
No part	39
Total failure rate (safety function)	248
Safe failure fraction (SFF) ²¹	70%
SIL AC ²²	SIL2
PFH	7.2E-8 1/h

²¹ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²² SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

4.3.3 Switching repeater 9170/a1-c4-ef ²³

The FMEDA carried out on the switching repeater 9170/a1-c4-ef leads under the assumptions described in section 4.2.3 to the following failure rates:

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	7
Fail Safe Undetected (λ_{SU})	106
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	21

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	125
No part	58

Total failure rate (safety function)	135
Safe failure fraction (SFF) ²⁴	84%

SIL AC ²⁵	SIL2
PFH	2.1E-8 1/h

²³ e = 1 or 6.

²⁴ The complete sensor 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

4.3.4 Switching repeater 9170/a1-cd-ef ²⁶

The FMEDA carried out on the switching repeater 9170/a1-cd-1f leads under the assumptions described in section 4.2.3 to the following failure rates:

<i>exida</i> Profile 1	
Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	8
Fail Safe Undetected (λ_{SU})	92
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	28

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	81
No part	39

Total failure rate (safety function)	129
Safe failure fraction (SFF) ²⁷	78%

SIL AC ²⁸	SIL2
PFH	2.8E-8 1/h

²⁶ d = 0 or 1; e = 1 or 6.

²⁷ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

²⁸ . 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

4.3.5 Switching repeater 9170/a1-cd-2f ²⁹

The FMEDA carried out on the switching repeater 9170/a1-cd-2f leads under the assumptions described in section 4.2.3 to the following failure rates:

Failure category	<i>exida</i> Profile 1	
	Failure rates (in FIT)	
Fail Safe Detected (λ_{SD})		8
Fail Safe Undetected (λ_{SU})		139
Fail Dangerous Detected (λ_{DD})		1
Fail Dangerous Undetected (λ_{DU})		28

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	12
No effect	95
No part	40

Total failure rate (safety function)	176
Safe failure fraction (SFF) ³⁰	84%

SIL AC ³¹	SIL2
PFH	2.8E-8 1/h

²⁹ d = 0 or 1.

³⁰ The complete sensor 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 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

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 9170 considering a proof test coverage of 99% (see Appendix 1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 4.3.1 to 4.3.5. 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

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
9170/a1-c2/3-ef	$PFD_{AVG} = 3.44E-04$	$PFD_{AVG} = 6.56E-04$	$PFD_{AVG} = 1.59E-03$
9170/a1-c4-ef	$PFD_{AVG} = 1.00E-04$	$PFD_{AVG} = 1.91E-04$	$PFD_{AVG} = 4.65E-04$
9170/a1-c0/1-ef	$PFD_{AVG} = 1.34E-04$	$PFD_{AVG} = 2.55E-04$	$PFD_{AVG} = 6.19E-04$

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

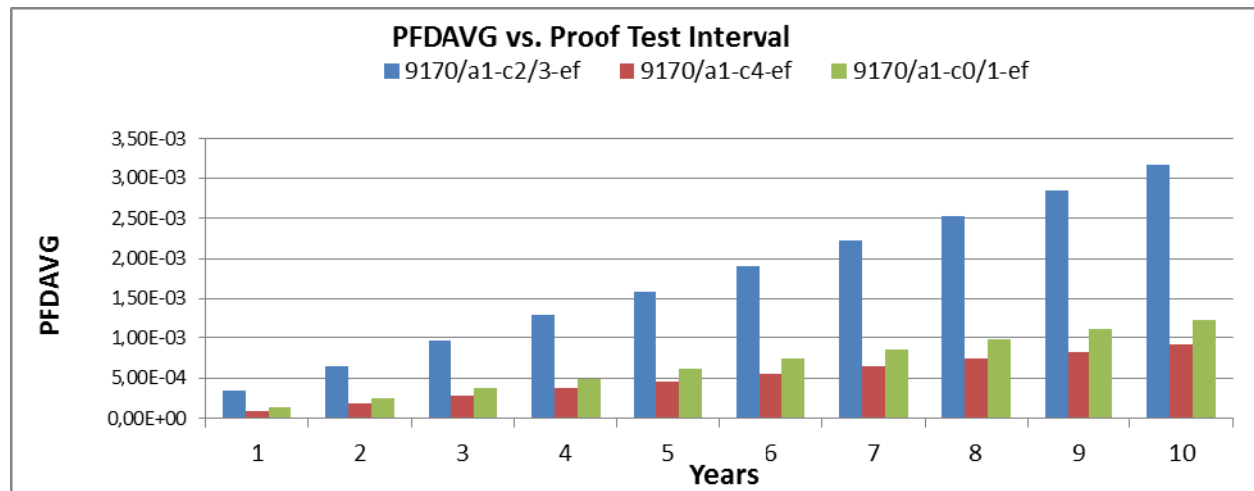


Figure 2: $PFD_{AVG}(t)$

6 Terms and Definitions

DC _S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
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.
PDF _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A element	"Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
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

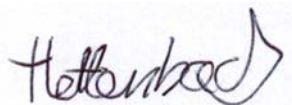
Version History: V3R0: Editorial Changes after review; September 29, 2015
V2R4: Editorial changes, including new variants; July 8, 2015
V2R3: Editorial changes; March 9, 2011
V2R2: Configurations extended; February 7, 2011
V2R1: Editorial changes; February 7, 2011
V2R0: Additional variants added; February 4, 2011
V1R0: Review comments incorporated; June 11, 2009
V0R1: Initial version; May 19, 2009

Authors: Jan Hettenbach

Review: V2R4: J. Hochhaus (*exida*), M. Fleisch (R. STAHL Schaltgeräte GmbH)

Release status: Released to R. STAHL Schaltgeräte GmbH

7.3 Release signatures



Dipl. -Ing. (Univ.) Jan Hettenbach

Dipl.-Ing. Jürgen Hochhaus

Appendix 1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 8.

Table 8 Steps for Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2	Force the switching repeater 9170/*1 to go to the safe state and verify that the safe state is reached.
3	Restore the loop to full operation.
4	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect more than 99% of possible “du” failures in the switching repeater 9170/*1.

Appendix 2: 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 lifetime³² 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
Relay	K81A, K82A	100.000 switching cycles

The relays are the only limiting factor with regard to the useful lifetime of the system.

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

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

³² 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 3: *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
Humidity³³	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock³⁴	10 g	15 g	15 g	15 g	15 g	N/A
Vibration³⁵	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion³⁶	G2	G3	G3	G3	G3	Compatible Material
Surge³⁷						
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 Susceptibility³⁸						
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)³⁹	6kV	6kV	6kV	6kV	6kV	N/A

³³ Humidity rating per IEC 60068-2-3

³⁴ Shock rating per IEC 60068-2-6

³⁵ Vibration rating per IEC 60770-1

³⁶ Chemical Corrosion rating per ISA 71.04

³⁷ Surge rating per IEC 61000-4-5

³⁸ EMI Susceptibility rating per IEC 6100-4-3

³⁹ ESD (Air) rating per IEC 61000-4-2