Failure Modes, Effects and Diagnostic Analysis

Project:
Pressure, Temperature and Vacuum Switches

Company:
BETA B.V.
Rijswijk
The Netherlands

Contract Number: Beta BV Q21/09-109-C
Report No.: Beta BV Q21/09-109-C R002
Version V1, Revision R1, August 2023
Philipp Hanzik

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 Pressure, Temperature and Vacuum Switches. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the Pressure, Temperature and Vacuum Switches. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the Pressure, Temperature and Vacuum Switches.

Table 1: Version Overview

[C1]	Pressure switches C.-P….- series with air-relay
[C2]	Pressure switches W.-P….- or C.-P….- or B.-P….- series with micro-switch
[C3]	Temperature switches C.-T….- series with air-relay
[C4]	Temperature switches W.-T….- or C.-T….- or B.-T….- series with micro-switch
[C5]	Vacuum switches W.-V….- or C.-V….- or B.-V….- series
[C6]	Differential pressure switches W.-D….- or C.-D….- or G.-D ….- series

The Pressure, Temperature and Vacuum Switches is classified as a device that is part of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

BETA B.V. and *exida* together did a quantitative analysis of the Pressure, Temperature and Vacuum Switches to calculate the failure rates using *exida* 's component database (see [N2]) for the different mechanical components. The failure rates used in this analysis are from the exida Electrical & Mechanical Component Reliability Handbook for Profile 2.

The architectural constraints for the entire final element will need to be evaluated per Route 1_H

Based on the assumptions listed in 4.3, the failure rates for the Pressure, Temperature and Vacuum Switches are listed in section 4.4.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

The failure rates listed in this report are based on over 350 billion-unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 4.2.2.

A user of the Pressure, Temperature and Vacuum Switches can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table of Contents

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 Pressure, Temperature and Vacuum Switches. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

The information in this report can be used to evaluate whether an element 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.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

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

BETA B.V.	Manufacturer of the Pressure, Temperature and Vacuum Switches
exida	Performed the hardware assessment

BETA B.V. contracted *exida* with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Mechanical Component Reliability Handbook, 4th Edition, 2016	*exida* Innovation LLC, Component Reliability Database Handbook, Vol. 2 – Mechanical Components, 4th Edition, 2016
[N3]	Safety Equipment Reliability Handbook, 4th Edition, 2015	*exida* LLC, Safety Equipment Reliability Handbook, Fourth Edition, 2015, ISBN 978-1-934977-13-2
[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]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	O'Brien, C. , Stewart, L., & Bredemeyer, L., 2018	*exida* LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, 2018, ISBN 978-1-934977-18-7

2.4 Reference documents

2.4.1 Documentation provided by BETA B.V.

[D1]	BOEK_August_08_Rev K.pdf	I.O.Manual SP 001 Rev. K of August 2008
[D2]	30_09_29_A (1).pdf	Mechanical drawing "Assembly Pressure & Temperature sensors with C.-enclosure" 30.09.29 Rev. A of 14.11.06
[D3]	32_09_19.pdf	Mechanical drawing "Data differential pressure sensor : D...D" 32.09.19 Rev. 0 of 22.08.97
[D4]	32_09_16.pdf	Mechanical drawing "Data differential pressure sensor D...H" 32.09.16 Rev. 0 of 20.08.97
[D5]	32_09_15.pdf	Mechanical drawing "Data differential pressure sensor D...L" 32.09.15 Rev. 0 of 20.08.97
[D6]	32_09_09.pdf	Mechanical drawing "Data Differential Pressure Sensors, Model: D4..M, D5..M and D6..M" 32.09.09 Rev. B of 20.08.97
[D7]	34_09_02.pdf	Mechanical drawing "Assembly BETAMINI II" 34.09.02 Rev. 0 of 10.08.07
[D8]	30_09_26_B.pdf	Mechanical drawing "Data pressure sensors Models L + M" 30.09.26 Rev. B of 20.08.97
[D9]	30_09_81_E (1).pdf	Mechanical drawing "Assembly Pressure switch series: W.-.....-...-..-.-.-.. For IECEx, CSA & FM" 30.09.81 Rev. E of 31.08.09
[D10]	30_01_15_F (1).pdf	Mechanical drawing "Assembly temperature sensor, model D00" 30.01.15 Rev. F of 17.03.08
[D11]	30_01_16_I (1).pdf	Mechanical drawing "Assembly temperature sensor, model C.." 30.01.16 Rev. I of 11.03.08
[D12]	30_09_96 (1).pdf	Mechanical drawing "Data pressure sensors Models P8..H / P9..H" 30.09.96 Rev. 0 of 26.07.07
[D13]	D14 Switching element type SA_SB in C-encl.pdf	Mechanical drawing "Assembly Air-relay"
[D14]	30_01_07.pdf	Mechanical drawing "Sensor van vacuumschakelaar" 30.01.07 Rev. 0 of 26.09.85

2.4.2 Documentation generated by *exida*

[R1]	C1_FMEDA_V7_Pressure_C-Series_Inc_Setpoint_V1R0.efmx of 06.05.2022
[R2]	C2_FMEDA_V7_Pressure_W-Series_Dec_Setpoint_V1R0.efmx of 06.05.2022
[R3]	C3_FMEDA_V7_Temperature_C-Series_Inc_Setpoint_V1R0.efmx of 06.05.2022
[R4]	C4_FMEDA_V7_Temperature_W-Series_Inc_Setpoint_V1R0.efmx of 06.05.2022
[R5]	C5_FMEDA_V7_Vacuum_W-Series_Inc_Setpoint_V1R0.efmx of 06.05.2022

[R6]	C6_FMEDA_V7_Diff_Pressure_DM_C-Series_Inc_Dec_Setpoint_V1R0.efmx of 06.05.2022
[R7]	FMEDA Report PFDavg Calc_2022.xls of 06.05.2022

3 Product Description

The Pressure, Temperature and Vacuum Switches are considered to be Type A subsystems with a hardware fault tolerance of 0.

The weatherproof C-Series, in cast aluminum or SS316 enclosures. (Optional also Ex ia or ib). Pressure ranges starting from 2 mbar to 540 bar. Vacuum ranges / Differential ranges and Temperature ranges available. Several options and specials possible.

Figure 1: C-Series

The explosion proof (Ex d / Ex tb) W-series, in cast aluminum or SS316 enclosures. Pressure ranges starting from 2 mbar to 540 bar. Vacuum ranges / Differential ranges and Temperature ranges available. Several options and specials possible.

Figure 2: W-Series

The OEM range the BETA MINI switch is anodized aluminum enclosure fixed Hirschmann connector. Pressure ranges starting from 0.3 bar to 540 bar. Fluid power (hydraulic) range up to 540 bar Vacuum ranges and Temperature ranges available. Limited option and specials possible.

Figure 3: B-Series

The Differential Pressure Switch G-Series is an aluminum enclosure for low differential pressure.
The differential range starting from 2 mbar to 15 mbar by a max. static pressure of 10 bar. The Low pressure side is for use of Air or INERT gas. Any fluid can be used on the High pressure side

Figure 4: G-Series

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation listed in section 2.4.1 and is documented in [R1] to [R7].

4.1 Failure categories description

In order to judge the failure behavior of the Pressure, Temperature and Vacuum Switches, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized between contact C and NC (circuit interrupted). This is valid for increasing as well as decreasing set-point.
Fail Safe	Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
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. For the calculation of the SFF it is treated like a safe undetected failure.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress in each application. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category.

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which were derived using over 350 billion-unit operational hours of process industry field failure data from multiple sources and failure data from various databases. The component failure rates are provided for each applicable operational profile and application, see Appendix C. The *exida* profile chosen for this FMEDA was Profile 2 (General Field Equipment) as this was judged to be the best fit for the product and application information submitted by BETA B.V. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. 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. *exida* has detailed models available to make customized failure rate predictions (Contact *exida*).

Accurate plant specific data may be used to check validity of this failure rate data. 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Pressure, Temperature and Vacuum Switches.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Pressure, Temperature and Vacuum Switches, and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- The stress levels are specified in the *exida* Profile used for the analysis limited by the manufacturer's published ratings.
- Materials are compatible with the environmental and process conditions.
- The device is installed and operated per the manufacturer's instructions.
- The micro switch is used to open or to close an electrical circuit (the "safety loop").
- Only the described configurations are used for safety applications.
- All devices are operated in the low demand mode of operation.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the FMEDA analysis of the Pressure, Temperature and Vacuum Switches.

4.4.1 Pressure switches C.-P….- series with air-relay [C1]

The FMEDA carried out on the pressure switches C.-P….- series with air-relay leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 2: FMEDA Results of the pressure switches C.-P….- series

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	**313**
Fail Dangerous Undetected (λ_{DU})	**209**
No effect	147
Total failure rate (safety function)	**522**
SFF	**59%**
MTBF	**171 years**
SIL AC [2]	**SIL1**

[2] 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.

4.4.2 Pressure switches W.-P...- or C.-P ...- or B.-P...- series with micro-switch [C2]

The FMEDA carried out on the pressure switches W.-P….- or C.-P ….- or B.-P….- series with micro-switch leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 3: FMEDA Results of the pressure switches W.-P….- or C.-P ….- or B.-P….- series

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	**190**
Fail Dangerous Undetected (λ_{DU})	**93**
No effect	202
Total failure rate (safety function)	**283**
SFF	**67%**
MTBF	**235 years**
SIL AC [3]	**SIL2**

[3] 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.

4.4.3 Temperature switches C.-T….- series with air-relay [C3]

The FMEDA carried out on the temperature switches C.-T….- series with air-relay leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 4: FMEDA Results of the temperature switches C.-T….- series

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	**301**
Fail Dangerous Undetected (λ_{DU})	**196**

No effect	121

Total failure rate (safety function)	**497**
SFF	**60%**
MTBF	**184 years**

SIL AC [4]	**SIL2**

[4] 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.

4.4.4 Temperature switches W.-T...- or C.-T...- or B.-T…- series w micro-switch [C4]

The FMEDA carried out on the temperature switches W.-T….- or C.-T….- or B.-T….- series with micro-switch leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 5: FMEDA Results of the temperature switches W.-T….- or C.-T….- or B.-T….- series

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	**164**
Fail Dangerous Undetected (λ_{DU})	**98**
No effect	177
Total failure rate (safety function)	**262**
SFF	**62%**
MTBF	**242 years**
SIL AC [5]	**SIL2**

[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.

4.4.5 Vacuum switches W.-V….- or C.-V….- or B.-V….- series [C5]

The FMEDA carried out on vacuum switches W.-V….- or C.-V ….- or B.-V….- series leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 6: FMEDA Results of the vacuum switches W.-V….- or C.-V ….- or B.-V….- series

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	**86**
Fail Dangerous Undetected (λ_{DU})	**53**
No effect	130
Total failure rate (safety function)	**139**
SFF	**62%**
MTBF	**423 years**
SIL AC [6]	**SIL2**

[6] 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.

4.4.6 Differential pressure switches W.-D….- or C.-D….- series [C6]

The FMEDA carried out on differential pressure switches W.-D….- or C.-D….- series leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

Table 7: FMEDA Results of the differential pressure switches W.-D….- or C.-D….- series leads

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	**364**
Fail Dangerous Undetected (λ_{DU})	**204**

No effect (#)	411

Total failure rate (safety function)	**568**
SFF	**64%**
MTBF	**116 years**

SIL AC [7]	**SIL2**

Where:

λ_{SU} = Fail Safe Undetected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

These failure rates are valid for the useful lifetime of the product, see Appendix A.

According to IEC 61508-2 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, or the approach according to IEC 61511:2016 which is based on 2_H.

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

The architectural constraint type for the Pressure, Temperature and Vacuum Switches is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

[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.

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation Pressure, Temperature and Vacuum Switches

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for the Pressure, Temperature and Vacuum Switches. considering a proof test coverage of 90% (see Appendix B.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 4.4.

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

Table 8: Pressure, Temperature and Vacuum Switches – PFDAVG values

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
[C1]	PFD_{AVG} = 1.74E-03	PFD_{AVG} = 2.57E-03	PFD_{AVG} = 5.05E-03
[C2]	PFD_{AVG} = 7.75E-04	PFD_{AVG} = 1.14E-03	PFD_{AVG} = 2.24E-03
[C3]	PFD_{AVG} = 1.63E-03	PFD_{AVG} = 2.40E-03	PFD_{AVG} = 4.72E-03
[C4]	PFD_{AVG} = 8.20E-04	PFD_{AVG} = 1.21E-03	PFD_{AVG} = 2.37E-03
[C5]	PFD_{AVG} = 4.43E-04	PFD_{AVG} = 6.52E-04	PFD_{AVG} = 1.28E-03
[C6]	PFD_{AVG} = 1.70E-03	PFD_{AVG} = 2.51E-03	PFD_{AVG} = 4.92E-03

As the Pressure, Temperature and Vacuum Switches is part of an entire safety function it should only consume a certain percentage of the allowed range. Assuming 25% of this range as a reasonable budget it should be better than or equal to 2.50E-03. The calculated PFD_{AVG} values for a proof test interval of 1 year are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 25% of this range, i.e. to be better than or equal to 2.50E-03. Figure 3 shows the time dependent curve of PFD_{AVG} for Pressure, Temperature and Vacuum Switches.

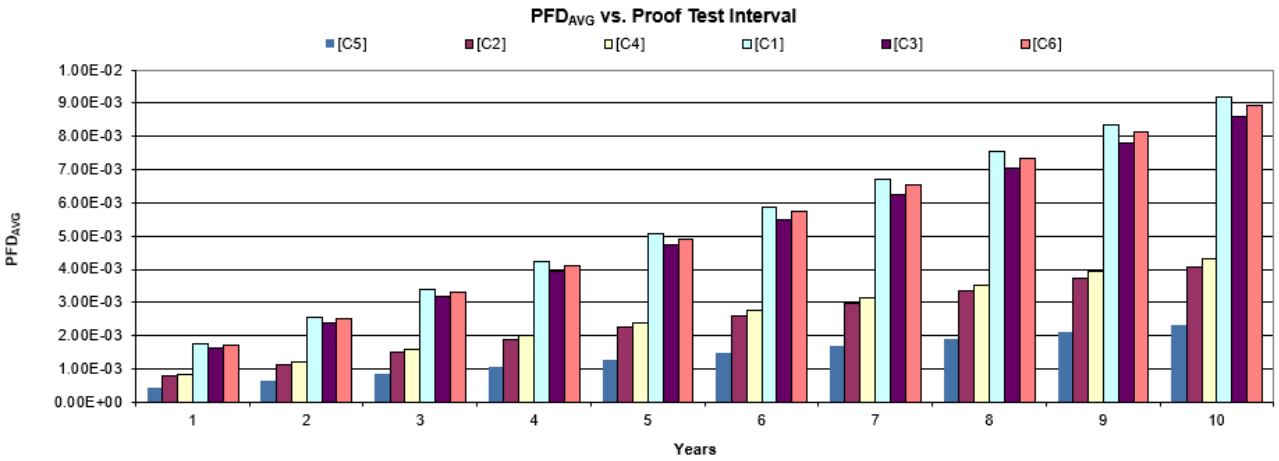


Figure 5: PFDAVG(t)

6 Terms and Definitions

Device	A device is something that is part of an element; but, cannot perform an element safety function on its own.
Element	A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
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 demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIL	Safety Integrity Level
Type A element	“Non-Complex” element (using discrete components); 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 *exida* compiled field failure data and 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, product design changes, 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 model number 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, contact the product vendor to verify the current validity of the results.

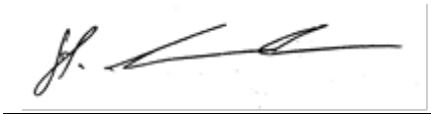
7.2 Version History

Version History

	V1R1:	Product descriptions corrected (Ex), August 11,2023
	V1R0:	Release version; June 26, 2023
	V0R1:	Initial draft version; May 06, 2022

Author:	Philipp Hanzik	
Review:	V0R1:	Stephan Aschenbrenner, *exida*, 26.06.2023
Release status:	V1R0:	Release of 26.06.2023

7.3 Release signatures



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

B. Eng. Philipp Hanzik, Safety Engineer

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 determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the exida FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

It is the responsibility of the end user to maintain and operate the Pressure, Temperature and Vacuum Switches per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

A major factor influencing the useful life is the air quality.

Based on general field failure data a useful life period of approximately 10 years solenoid coil, pilot valve and if applicable main valve) is expected for the Pressure, Temperature and Vacuum Switches.

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

Appendix B Proof Tests to Reveal 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 automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

A suggested proof test consists of the following steps, as described in Table 9. This test will detect 90% of possible DU failures in the Pressure, Temperature and Vacuum Switches when other automated diagnostics are not being performed.

Table 9 Suggested Proof Test – Pressure, Temperature and Vacuum Switches

Step	Action
1	Take appropriate action to avoid a false trip.
2	Inspect the device for any visible damage, corrosion or contamination.
3	Force the switch to reach a defined “MAX” threshold value and verify that the output goes into the safe state.
4	Force the switch to reach a defined “NORMAL” value and verify that the output remains in the normal state.
5	Repeat steps 2 and 3 twice and evaluate average set point value and repeatability.
6	Force the switch to reach a defined “MIN” threshold value and verify that the output goes into the safe state.
7	Force the switch to reach a defined “NORMAL” value and verify that the output remains in the normal state.
8	Repeat steps 2 and 3 twice and evaluate average set point value and repeatability.
9	Restore the loop to full operation.
10	Restore normal operation.

Appendix C *exida* Environmental Profiles

Table 10 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30° C	25° C	25° C	5° C	25° C	25° C
Average Internal Temperature	60° C	30° C	45° C	5° C	45° C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5° C	25° C	25° C	0° C	25° C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5° C	40° C	40° C	2° C	40° C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[8]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[9]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[10]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[11]	G2	G3	G3	G3	G3	Compatible Material
Surge[12]						
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 Susceptibility[13]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[14]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[8] Humidity rating per IEC 60068-2-3
[9] Shock rating per IEC 60068-2-27
[10] Vibration rating per IEC 60068-2-6
[11] Chemical Corrosion rating per ISA 71.04
[12] Surge rating per IEC 61000-4-5
[13] EMI Susceptibility rating per IEC 61000-4-3
[14] ESD (Air) rating per IEC 61000-4-2