Failure Modes, Effects and Diagnostic Analysis

Project:
Butterfly Valve Type R470

Company:
GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG
Niedernhall-Waldzimmern
Germany

Contract Number: Q22/07-012
Report No.: GEMÜ 22/07-012 R006
Version V1, Revision R0, March 2023
Philipp Hanzik

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

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 Butterfly Valve Type R470. 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 Butterfly Valve Type R470. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Butterfly Valve Type R470 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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 5.1. Therefore, the Butterfly Valve Type R470 can be classified as a 2_H device when the listed failure rates are used. When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 per Route 2_H. If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

Based on the assumptions listed in 4.3, the failure rates for the Butterfly Valve Type R470 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 Butterfly Valve Type R470 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 Butterfly Valve Type R470. 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

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG	Manufacturer of the Butterfly Valve Type R470
exida	Performed the hardware assessment

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG contracted *exida* in January 2023 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]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 2 – Mechanical Components	*exida* LLC, Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components ISBN 978-1-934977-09-5
[N3]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 3 – Electrical Sensor Components	*exida* LLC, Component Reliability Database Handbook, 5th Edition, 2021 Vol. 3 – Electrical Sensor Components ISBN 978-1-934977-22-4
[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

[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N9]	Random versus Systematic – Issues and Solutions, September 2016	http://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
[N10]	Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index^{TM}, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
[N11]	Bukowski, J.V. and Stewart, L.L., April 2016	Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	*exida* White Paper, Sellersville, PA www.exida.eu
[N13]	Goble, W.M. and Brombacher, A.C., November 1999, Vol. 66, No. 2	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
[N14]	ISO 13849-1:2016	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

2.4 Reference documents

2.4.1 Documentation provided by GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG

[D1]	db_R470_de.pdf	Data Sheet, Drawing and Bill of Material of 15.02.2023

2.4.2 Documentation generated by *exida*

[R1]	FMEDA_R470.xlsm	Failure Modes, Effects, and Diagnostic Analysis – Butterfly Valve Type R470 (internal document), V1R0 of 03.03.2023

3 Product Description

The GEMÜ R470 Tugela double eccentric butterfly valve made of metal has a free shaft end with head flange according to EN ISO 5211. The butterfly valve is available in nominal sizes DN 50 to 600 and in standardized installation lengths API 609 category A (DIN 3202 K1).

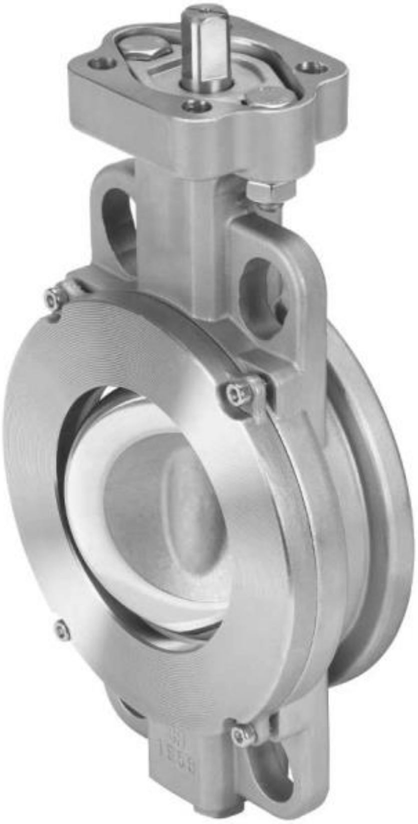

Figure 1 Typical Butterfly Valve Type R470 covered in this FMEDA

The Butterfly Valve Type R470 is classified as a device that is a part of a Type A[2] element according to IEC 61508, having a hardware fault tolerance of 0.

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

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].

4.1 Failure categories description

In order to judge the failure behavior of the Butterfly Valve Type R470, the following definitions for the failure of the device were considered.

Fail-Safe State:

Valve, Full Stroke
State where the valve is closed.

Valve, Tight-Shut-Off
State where the valve is closed and sealed with leakage no greater than the defined leak rate; Tight shut-off requirements shall be specified according to the application, if shut-off requirements allow flow greater than ANSI class V, respectively ANSI class IV, then Full Stroke numbers may be used.

Valve, Open-To-Trip
State where the valve is open

Fail Safe
Failure that causes the device to go to the defined fail-safe state without a demand from the process.

Fail Dangerous
Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Valve
Failure that prevents the valve from moving to the defined fail-safe state within the normal time span.

Fail Dangerous Undetected
Failure that is dangerous and that is not being diagnosed by automatic diagnostics, such as Partial Valve Stroke Testing.

Fail Dangerous Detected
Failure that is dangerous but is detected by automatic diagnostics, such as Partial Valve Stroke Testing.

No Effect
Failure of a component that is part of the safety function but that has no effect on the safety function.

External Leakage
Failure that causes process fluids, gas, hydraulic fluids or operating media to leak outside of the valve or actuator; External Leakage is not considered part of the safety function and therefore this failure rate is not included in any of the numbers. External leakage failure rates should be reviewed for secondary safety and environmental issues.

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 [N13].

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 3 (General Field Equipment) and Profile 6 (Process Wetted Parts) for the Valves process wetted parts as this was judged to be the best fit for the product and application information submitted by GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG. 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 failure rates are predicted for a Site Safety Index of SSI=2 ([N10] & [N11]) as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

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^{TM} 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 Butterfly Valve Type R470.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Butterfly Valve Type R470, 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.
- Valves are installed such that the controlled substance will flow through the valve in the direction indicated by the flow arrow, located on the valve body.
- In order to claim diagnostic coverage for Partial Valve Stroke Testing it is automatically performed at a rate at least ten times faster than the Demand frequency.
- Partial Valve Stroke Testing of the Safety Instrumented Function provides a full cycle test of the solenoid/pilot valve. In cases where this is not true, another method must be used to perform a full Valve cycle during automated diagnostics in order to use the PVST numbers.
- Partial Valve Stroke Testing of the final element includes position detection from actuator top mounted position sensors, typical of quarter turn installations.
- Worst-case internal fault detection time is the PVST test interval time.

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 Butterfly Valve Type R470.

Table 1 and Table 2 lists the failure rates for the Butterfly Valve Type R470 according to IEC 61508 with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix D for an explanation of SSI and the failure rates for SSI of 4 (ideal maintenance practices).

Table 1 Failure rates for Static Applications[3] with Good Maintenance Assumptions in FIT @ SSI=2

Butterfly Valve Type R470	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	580	1635	158
Tight Shut-Off, Clean Service	0	0	0	1230	986	158
Open on Trip, Clean Service	0	118	0	462	1635	158
Full Stroke with PVST, Clean Service	0	0	241	339	1635	158
Tight Shut-Off with PVST, Clean Service	0	0	241	989	986	158
Open on Trip with PVST, Clean Service	117	1	241	221	1635	158
Full Stroke, Severe Service	0	0	0	865	2107	279
Tight Shut-Off, Severe Service	0	0	0	1987	986	279
Open on Trip, Severe Service	0	236	0	629	2107	279
Full Stroke with PVST, Severe Service	0	0	309	556	2107	279
Tight Shut-Off with PVST, Severe Service	0	0	309	1678	986	279
Open on Trip with PVST, Severe Service	234	2	309	320	2107	279

[3] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.

Table 2 Failure rates for Dynamic Applications[4] with Good Maintenance Assumptions in FIT @ SSI=2

Butterfly Valve Type R470	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	304	1789	158
Tight Shut-Off, Clean Service	0	0	0	1013	1080	158
Open on Trip, Clean Service	0	118	0	186	1789	158
Full Stroke with PVST, Clean Service	0	0	76	228	1789	158
Tight Shut-Off with PVST, Clean Service	0	0	76	937	1080	158
Open on Trip with PVST, Clean Service	117	1	76	110	1789	158
Full Stroke, Severe Service	0	0	0	512	2261	280
Tight Shut-Off, Severe Service	0	0	0	1693	1080	280
Open on Trip, Severe Service	0	236	0	276	2261	280
Full Stroke with PVST, Severe Service	0	0	98	414	2261	280
Tight Shut-Off with PVST, Severe Service	0	0	98	1595	1080	280
Open on Trip with PVST, Severe Service	234	2	98	178	2261	280

Table 3 Mean Time To Dangerous Failure in years

Butterfly Valve Type R470	Dynamic Application $MTTF_D$
Full Stroke, Clean Service	376
Tight Shut-Off, Clean Service	113
Open on Trip, Clean Service	614
Full Stroke, Severe Service	223
Tight Shut-Off, Severe Service	67
Open on Trip, Severe Service	414

Where:

λ_{SD} = Fail Safe Detected
λ_{SU} = Fail Safe Undetected
λ_{DD} = Fail Dangerous Detected
λ_{DU} = Fail Dangerous Undetected
# = No Effect Failures
E = External Leaks
$MTTF_D$ = Mean Time To Dangerous Failure

[4] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

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 (see Section 5.1).

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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the Butterfly Valve Type R470 meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The architectural constraint type for the Butterfly Valve Type R470 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.

Table 9 and Table 10 lists the failure rates for the Butterfly Valve Type R470 according to IEC 61508 with a Site Safety Index (SSI) of 4 (perfect site maintenance practices). This data should not be used for SIL verification and is provided only for comparison with other analysis than has assumed perfect maintenance. See Appendix D for an explanation of SSI.

5 Using the FMEDA Results

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

5.1 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

> "based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to
>
> - the amount of field feedback; and
> - the exercise of **expert judgment**; and when needed
> - the undertaking of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and

2. a device and all of its components have been installed in the field for one year or more; and

3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and

4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and

5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
Device	A device is something that is part of an element; but, cannot perform an element safety function on its own.
Dynamic Applications	The movement interval of the final element device is less than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
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
High demand Mode	Mode, where the demand interval for operation made on a safety-related system is less than twice the proof test interval.
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
MTTFd	Mean Time To Dangerous Failure in Years
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequently than the proof test; therefore, the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Severe Service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SSI	Site Safety Index (See Appendix D)
Static Applications	The movement interval of the final element device is greater than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
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:	V1R0	Initial Release of 16.03.2023
	V0R1	Initial Draft of 03.03.2023
Authors:	Philipp Hanzik	
Review:	V0R1:	Michael Mütsch, GEMÜ, 08.03.2023
		Stephan Aschenbrenner, *exida*, 15.03.2023

Release Status: Release of 16.03.2023

7.3 Release signatures

B. Eng Philipp Hanzik, Safety Engineer

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

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[5] 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 PFD_{avg} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is the responsibility of the end user to maintain and operate the Butterfly Valve Type R470 per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 15 years is expected for the Butterfly Valve Type R470.

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.

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

Appendix B Proof Tests to 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

The suggested Proof Test consists of a full stroke of the associated device, see Table 4. Refer to the table in B.2 for the Proof Test Coverages.

Table 4 Suggested Proof Test – Butterfly Valve Type R470

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the air supply/input to the Actuator to force the Actuator/Valve assembly to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time. Note:-This tests for all failures that could prevent the functioning of the Control Valve as well as the rest of the final control element.
3.	Inspect the Actuator and Valve for any leaks, visible damage or contamination
4.	Re-store the original air supply/input to the Actuator and confirm that the normal operating state was achieved.
5.	Remove the bypass and otherwise restore normal operation.

For the test to be effective the movement of the Valve must be confirmed. To confirm the effectiveness of the test both the travel of the Valve and slew rate must be monitored and compared to expected results to validate the testing.

B.2 Proof Test Coverage

The Proof Test Coverage for the various device configurations are given in Table 5 and Table 6.

Table 5 Proof Test Results – Butterfly Valve Type R470 – Static Application

Application	**Safety Function**	**λ_{DU}PT**[6] **(FIT)**	**Proof Test Coverage**	
			No PVST	**with PVST**
Clean Service	Close On Trip – Full Stroke	218	62%	36%
	Close On Trip – Tight Shutoff	868	29%	12%
	Open On Trip	100	78%	55%
Severe Service	Close On Trip – Full Stroke	401	54%	28%
	Close On Trip – Tight Shutoff	1523	23%	9%
	Open On Trip	165	74%	48%

Table 6 Proof Test Results – Butterfly Valve Type R470 – Dynamic Application

Application	**Safety Function**	**λ_{DU}PT**[7] **(FIT)**	**Proof Test Coverage**	
			No PVST	**with PVST**
Clean Service	Close On Trip – Full Stroke	190	38%	17%
	Close On Trip – Tight Shutoff	899	11%	4%
	Open On Trip	72	61%	35%
Severe Service	Close On Trip – Full Stroke	365	29%	12%
	Close On Trip – Tight Shutoff	1546	9%	3%
	Open On Trip	129	53%	28%

[6] **λ_{DU}PT** = Dangerous undetected failure rate after performing the recommended proof test.

[7] **λ_{DU}PT** = Dangerous undetected failure rate after performing the recommended proof test.

Appendix C *exida* Environmental Profiles

Table 7 *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

Appendix D Site Safety Index

Numerous field failure studies have shown that the failure rate for a specific device (same Manufacturer and Model number) will vary from site to site. The Site Safety Index (SSI) was created to account for these failure rates differences as well as other variables. The information in this appendix is intended to provide an overview of the Site Safety Index (SSI) model used by *exida* to compensate for site variables including device failure rates.

D.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 8 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.

Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:

Commission Test
Safety Validation Test
Proof Test Procedures
Proof Test Documentation
Failure Diagnostic and Repair Procedures
Device Useful Life Tracking and Replacement Process
SIS Modification Procedures
SIS Decommissioning Procedures
and others

Table 8 *exida* Site Safety Index Profiles

Level	Description
SSI 4	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, equipment is always replaced before end of useful life, equipment is always selected according to the specified environmental limits and process compatible materials. Electrical power supplies are clean of transients and isolated, pneumatic supplies and hydraulic fluids are always kept clean, etc. **Note:** This level is generally considered not possible but retained in the model for comparison purposes.
SSI 3	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials. Electrical power supplies are normally clean of transients and isolated, pneumatic supplies and hydraulic fluids are mostly kept clean, etc. Equipment is replaced before end of useful life, etc.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
SSI 1	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
SSI 0	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.

D.2 Site Safety Index Failure Rates – Butterfly Valve Type R470

Failure rates of each individual device in the SIF are increased or decreased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less than ideal end-user practices than are sensors or logic solvers. By increasing or decreasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance.

Table 9 and Table 10 lists the failure rates for the Butterfly Valve Type R470 according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 9 Failure rates for Static Applications[15] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	290	981	95
Tight Shut-Off, Clean Service	0	0	0	615	591	95
Open on Trip, Clean Service	0	71	0	231	981	95
Full Stroke with PVST, Clean Service	0	0	121	169	981	95
Tight Shut-Off with PVST, Clean Service	0	0	121	494	591	95
Open on Trip with PVST, Clean Service	70	1	121	110	981	95
Full Stroke, Severe Service	0	0	0	432	1264	167
Tight Shut-Off, Severe Service	0	0	0	993	591	167
Open on Trip, Severe Service	0	142	0	314	1264	167
Full Stroke with PVST, Severe Service	0	0	154	278	1264	167
Tight Shut-Off with PVST, Severe Service	0	0	154	839	591	167
Open on Trip with PVST, Severe Service	141	1	154	160	1264	167

Table 10 Failure rates for Dynamic Applications[16] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	152	1073	95

[15] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[16] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Tight Shut-Off, Clean Service	0	0	0	506	648	95
Open on Trip, Clean Service	0	71	0	93	1073	95
Full Stroke with PVST, Clean Service	0	0	38	114	1073	95
Tight Shut-Off with PVST, Clean Service	0	0	38	468	648	95
Open on Trip with PVST, Clean Service	70	1	38	55	1073	95
Full Stroke, Severe Service	0	0	0	256	1356	168
Tight Shut-Off, Severe Service	0	0	0	846	648	168
Open on Trip, Severe Service	0	142	0	138	1356	168
Full Stroke with PVST, Severe Service	0	0	49	207	1356	168
Tight Shut-Off with PVST, Severe Service	0	0	49	797	648	168
Open on Trip with PVST, Severe Service	141	1	49	89	1356	168