Failure Modes, Effects and Diagnostic Analysis

Project:
Pneumatic actuated valves 658 and 660

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

Contract Number: GEMÜ 24/08-201
Report No.: GEMÜ Q24/08-201 R001
Version V0, Revision R1, November 2024
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 Pneumatic actuated valves 658 and 660. 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 Pneumatic actuated valves 658 and 660. 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 Pneumatic actuated valves 658 and 660.

Table 1 Version Overview

Valve 658	2/2-way diaphragm valve with a two-stage actuator for full and partial strokes, stainless steel components, and a spring-to-close function with an adjustable stroke limiter.
Valve 660	2/2-way valve with a stainless steel pneumatic actuator for dosing and filling, with NC and NO control options. It includes stroke limits and an optical position indicator.

The Pneumatic actuated valves 658 and 660 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 Pneumatic actuated valves 658 and 660 can be classified as a 2_H device when the listed failure rates are used. . When 2H 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 (or SIL 3 @ HFT=1) per Route 2H. If Route 2H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1H.

Based on the assumptions listed in 4.3, the failure rates for the Pneumatic actuated valves 658 and 660 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 Pneumatic actuated valves 658 and 660 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 Pneumatic actuated valves 658 and 660. 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 Pneumatic actuated valves 658 and 660
exida	Performed the hardware assessment

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG 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, 6th Edition, 2023	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Sixth Edition, 2023
[N3]	Goble, W.M., 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N4]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N5]	O'Brien, C., Gavin, R., & Bredemeyer, L., 2023	*exida* LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, Second Edition, 2023, ISBN 978-1-934977-24-8
[N6]	Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
[N7]	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

[N8]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	Criteria for the Application of IEC 61508:2010 Route 2H | exida
[N9]	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.

2.4 Reference documents

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

[D1]	4-0005-1227-02~ANTRIEB METALL-FREMD.-KOLBEN~DRW045060~E.pdf	Drawing of the Valve 658, rev. 059632, 13.01.2022
[D2]	Antriebe 658 Strukturstücklisten.xls	BOM of the Valve 658, 07.11.2024
[D3]	db_658_de.pdf	Datasheet of the Valve 658, 07.11.2024
[D4]	660_11T1_4-0005-3010~ANTRIEB METALL-FREMD.-KOLBEN~345776~C.pdf	Drawing of the Valve 660, rev. 059196, 21.10.2021
[D5]	Antriebe 660 Strukturstücklisten.xls	BOM of the Valve 660, 07.11.2024
[D6]	db_660_de.pdf	Datasheet of the Valve 660, 07.11.2024

2.4.2 Documentation generated by *exida*

[R1]	FMEDA GEMU 24-08-201 658 Valve.xlsm	Failure Modes, Effects, and Diagnostic Analysis (internal document)
[R2]	FMEDA GEMU 24-08-201 660 Valve.xlsm	Failure Modes, Effects, and Diagnostic Analysis (internal document)

3 Product Description

The GEMÜ 658 2/2-way diaphragm valve features a two-stage actuator. Two independently operating pistons allow for both full and partial strokes. All actuator components, including closing springs (excluding seals), are made of stainless steel. The control function "spring-to-close" is available. An opening stroke limiter for partial stroke adjustment is integrated as standard.

The GEMÜ 660 2/2-way diaphragm valve features a stainless-steel piston actuator and is pneumatically operated. It is designed for dosing and filling various products. All actuator components (excluding seals) are made of stainless steel. Control options include "spring-to-close (NC)," "spring-to-open (NO)," and "double-acting (DA)." Opening and closing stroke limiters and an optical position indicator are integrated as standard.

Figure 1: The Valve 658 (left) and Valve 660 (right)

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 Pneumatic actuated valves 658 and 660, 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; 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 [N9].

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 ([N6] & [N7]) 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™ 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 Pneumatic actuated valves 658 and 660.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Pneumatic actuated valves 658 and 660, 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.
- In the event of a failure, the device must be completely replaced, as restoration is not feasible.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- 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.
- The valves are generally applied in relatively clean gas or liquid; therefore, no severe service has been considered in the analysis.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- Loss of the Air Pressure supply is not included in these failure rates.
- 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.
- The failure of a Relief Valve not opening to mitigate a system over-pressurization is outside the scope of this report.
- 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 Pneumatic actuated valves 658 and 660.

Table 2 to Table 9 lists the failure rates for the Pneumatic actuated valves 658 and 660 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). The proof-test coverage is to be found in Chapter B.2.

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

Valve 658	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	494	670	242
Tight Shut-Off, Clean Service	0	0	0	726	438	242
Open on Trip, Clean Service	0	70	0	424	670	242
Full Stroke with PVST, Clean Service	0	0	212	282	670	242
Tight Shut-Off with PVST, Clean Service	0	0	211	515	438	242
Open on Trip with PVST, Clean Service	69	1	212	212	670	242
Full Stroke, Severe Service	0	0	0	920	1219	424
Tight Shut-Off, Severe Service	0	0	0	1385	754	424
Open on Trip, Severe Service	0	140	0	781	1219	424
Full Stroke with PVST, Severe Service	0	0	390	530	1219	424
Tight Shut-Off with PVST, Severe Service	0	0	390	995	754	424
Open on Trip with PVST, Severe Service	139	1	390	391	1219	424

Table 3 Mean time to Failure - Static Applications

Valve 658	MTTF [Years]
Clean Service	81
Severe Service	45

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

Table 4 Failure rates for Static Applications[3] with Good Maintenance Assumptions in FIT @ SSI=2

Valve 660	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	582	719	261
Tight Shut-Off, Clean Service	0	0	0	814	487	261
Open on Trip, Clean Service	0	70	0	512	719	261
Full Stroke with PVST, Clean Service	0	0	257	325	719	261
Tight Shut-Off with PVST, Clean Service	0	0	256	558	487	261
Open on Trip with PVST, Clean Service	69	1	256	256	719	261
Full Stroke, Severe Service	0	0	0	1008	1268	443
Tight Shut-Off, Severe Service	0	0	0	1473	803	443
Open on Trip, Severe Service	0	140	0	868	1268	443
Full Stroke with PVST, Severe Service	0	0	435	573	1268	443
Tight Shut-Off with PVST, Severe Service	0	0	435	1038	803	443
Open on Trip with PVST, Severe Service	139	1	434	434	1268	443

Table 5 Mean time to Failure - Static Applications

Valve 660	MTTF [Years]
Clean Service	73
Severe Service	42

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

Table 6 Failure rates for Dynamic Applications[4] with Good Maintenance Assumptions in FIT @ SSI=2

Valve 658	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	255	703	242
Tight Shut-Off, Clean Service	0	0	0	486	472	242
Open on Trip, Clean Service	0	70	0	185	703	242
Full Stroke with PVST, Clean Service	0	0	68	187	703	242
Tight Shut-Off with PVST, Clean Service	0	0	68	418	472	242
Open on Trip with PVST, Clean Service	69	1	68	117	703	242
Full Stroke, Severe Service	0	0	0	448	1263	425
Tight Shut-Off, Severe Service	0	0	0	911	801	425
Open on Trip, Severe Service	0	141	0	308	1263	425
Full Stroke with PVST, Severe Service	0	0	106	342	1263	425
Tight Shut-Off with PVST, Severe Service	0	0	107	804	801	425
Open on Trip with PVST, Severe Service	140	1	107	201	1263	425

Table 7 Mean time to Failure - Dynamic Applications

Valve 658	MTTF [Years]
Clean Service	95
Severe Service	53

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

Table 8 Failure rates for Dynamic Applications[5] with Good Maintenance Assumptions in FIT @ SSI=2

Valve 660	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	327	771	261
Tight Shut-Off, Clean Service	0	0	0	558	540	261
Open on Trip, Clean Service	0	70	0	257	771	261
Full Stroke with PVST, Clean Service	0	0	103	224	771	261
Tight Shut-Off with PVST, Clean Service	0	0	103	455	540	261
Open on Trip with PVST, Clean Service	69	1	103	154	771	261
Full Stroke, Severe Service	0	0	0	520	1332	444
Tight Shut-Off, Severe Service	0	0	0	983	869	444
Open on Trip, Severe Service	0	141	0	380	1332	444
Full Stroke with PVST, Severe Service	0	0	141	379	1332	444
Tight Shut-Off with PVST, Severe Service	0	0	142	841	869	444
Open on Trip with PVST, Severe Service	140	1	142	238	1332	444

Table 9 Mean time to Failure - Dynamic Applications

Valve 660	MTTF [Years]
Clean Service	84
Severe Service	50

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

$$MTTF = \frac{10^9}{\lambda_{total} \cdot 8760}$$

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

λ_{total} = Total Failure Rate

= No Effect Failures

E = External Leaks

MTTF = Mean time to failure in years

[5] 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 Pneumatic actuated valves 658 and 660 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 Pneumatic actuated valves 658 and 660 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.

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.
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.
PFD_{avg}	Average Probability of Failure on Demand
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.
SIF	Safety Instrumented Function
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
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.

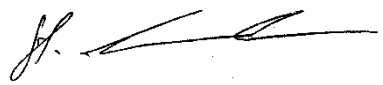
Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, contact the product vendor to verify the current validity of the results.

7.2 Version History

Version History:	V1R0: Review comments; 26. November 2024 V0R1: Initial version; 07. November 2024
Authors:	Philipp Hanzik
Review:	V0R1: Stephan Aschenbrenner, *exida,* 26. November 2024 Philipp Göker, GEMÜ, 21. November 2024
Release Status:	Release to GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG

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[6] 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 Pneumatic actuated valves 658 and 660 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 used.

Based on general field failure data a useful life period of approximately 15 years (actuators, valves, actuator-valve combinations) is expected for the Pneumatic actuated valves 658 and 660.

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

[6] 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 10. Refer to the table in B.2 for the Proof Test Coverages.

Table 10 Suggested Proof Test – Pneumatic actuated valves 658 and 660

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Inspect the device for any visible damage, corrosion or contamination.
3.	Force the valve to go to the Fail-Safe sate and confirm that the safe state has been achieved and within the correct time.
4.	*Optional: Carry out a leak detection test to increase the proof test coverage.*
5.	Remove the bypass and otherwise restore normal operation
6.	Record any failures in your company's SIF inspection database

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 11 to Table 8.

Table 11 Proof Test Results – Valve 658 – Static Application

Application	Safety Function	$\lambda_{DU}PT$[7] (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	176	64%	38%
	Close On Trip – Tight Shutoff	409	44%	21%
	Open On Trip	107	75%	50%
Severe Service	Close On Trip – Full Stroke	335	64%	37%
	Close On Trip – Tight Shutoff	800	42%	20%
	Open On Trip	196	75%	50%

Table 12 Proof Test Results – Valve 658 – Static Application

Application	Safety Function	$\lambda_{DU}PT$[8] (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	197	66%	39%
	Close On Trip – Tight Shutoff	430	47%	23%
	Open On Trip	128	75%	50%
Severe Service	Close On Trip – Full Stroke	356	65%	38%
	Close On Trip – Tight Shutoff	821	44%	21%
	Open On Trip	217	75%	50%

[7] $\lambda_{DU}PT$ = Dangerous undetected failure rate after performing the recommended proof test.

[8] $\lambda_{DU}PT$ = Dangerous undetected failure rate after performing the recommended proof test.

Table 13 Proof Test Results – Valve 660 – Dynamic Application

Application	Safety Function	λ_{DU}PT (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	153	40%	18%
	Close On Trip – Tight Shutoff	384	21%	8%
	Open On Trip	83	55%	29%
Severe Service	Close On Trip – Full Stroke	289	35%	15%
	Close On Trip – Tight Shutoff	751	18%	7%
	Open On Trip	148	52%	26%

Table 14 Proof Test Results – Valve 660 - Dynamic Application

Application	Safety Function	λ_{DU}PT (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	172	47%	23%
	Close On Trip – Tight Shutoff	404	28%	11%
	Open On Trip	102	60%	34%
Severe Service	Close On Trip – Full Stroke	308	41%	19%
	Close On Trip – Tight Shutoff	771	22%	8%
	Open On Trip	168	56%	29%

Appendix C *exida* Environmental Profiles

Table 15 *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[9]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[10]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[11]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[12]	G2	G3	G3	G3	G3	Compatible Material
Surge[13]						
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[14]						
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)[15]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[9] Humidity rating per IEC 60068-2-3
[10] Shock rating per IEC 60068-2-27
[11] Vibration rating per IEC 60068-2-6
[12] Chemical Corrosion rating per ISA 71.04
[13] Surge rating per IEC 61000-4-5
[14] EMI Susceptibility rating per IEC 61000-4-3
[15] 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 16 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 16 *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.