Failure Modes, Effects and Diagnostic Analysis

Project:
3/2-Way Pilot Solenoid Valves 032x

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

Contract No.: GEMÜ 13/08-046
Report No.: GEMÜ 13/08-046 R002
Version V0, Revision R1; March 2014

Stephan Aschenbrenner

Management summary

This report summarizes the results of the mechanical assessment carried out on the 3/2-Way Pilot Solenoid Valves 032x in the version listed in the mechanical drawings referenced in section 2.4.1. Table 1 gives an overview of the different variants that belong to the considered 3/2-Way Pilot Solenoid Valves 032x and explains the differences.

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

Table 1: Overview of the considered variants

GEMÜ 0322	Designed for single mounting (straight through design) or for modular battery mounting of up to 12 valves (by using clips).
GEMÜ 0324	Designed for direct mounting (hollow bolt) to pneumatically operated valves or other devices.
GEMÜ 0326	Designed for mounting to a compact aluminum rail as a valve battery for mounting in control cabinets or as a valve manifold near the pneumatic components to be controlled. Battery rail for up to 10 valves.

For safety applications only the described 3/2-Way Pilot Solenoid Valves 032x working as DTT (De-energize To Trip) devices have been considered. GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG calls this configuration “switch position a1”. All other possible variants and configurations are not covered by this report.

exida did a quantitative analysis of the 3/2-Way Pilot Solenoid Valves 032x to calculate the failure rates using *exida*‘s component database (see [N2]) for the different mechanical components.

The 3/2-Way Pilot Solenoid Valves 032x can be considered to be Type A[1] elements with a hardware fault tolerance of 0.

The complete final element, of which the 3/2-Way Pilot Solenoid Valves 032x are an element of the final control element, will need to be evaluated to determine the architectural constraints.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 5.2.2.

The failure rates are valid for the useful life of the considered 3/2-Way Pilot Solenoid Valves 032x (see Appendix 2) when operating as defined in the considered scenarios.

The following tables show how the above stated requirements are fulfilled according to IEC 61508:2010.

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

Table 2: 3/2-Way Pilot Solenoid Valves 032x – Failure rates

Failure category	Failure rates (in FIT), Profile 3 data	
	Close on Trip	
	Without external test	With external test [2]
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**110**	**110**
Dangerous Detected (λ_{DD})	**0**	**93**
Dangerous Undetected (λ_{DU})	**129**	**36**
No Effect	49	49
External leakage	0	0
PTC	93%	74%
Total failure rate (safety function)	**239**	**239**
SFF [3]	**45%**	**84%**
DC	**0%**	**71%**
SIL AC [4]	**SIL1**	**SIL2**
MTBF(in years)	396	396

[2] Full Valve Stroke Testing (FVST) and leakage testing shall be performed at a rate at least ten times faster than the expected demand rate.

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

[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. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD value.

Table 3: 3/2-Way Pilot Solenoid Valves 032x when connected to valve – Failure rates

Failure category	Failure rates (in FIT), Profile 3 data	
	Close on Trip	
	Without external test	With external test [5]
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**110**	**110**
Dangerous Detected (λ_{DD})	**0**	**39**
Dangerous Undetected (λ_{DU})	**39.4**	**0.4**
No Effect	139	139
External leakage	0	0
PTC	99%	0%
Total failure rate (safety function)	**149**	**149**
DC	**0%**	**99%**
MTBF(in years)	396	396

[5] Full Valve Stroke Testing (FVST) and leakage testing shall be performed at a rate at least ten times faster than the expected demand rate.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the Failure Modes, Effects and Diagnostics Analysis (FMEDA) carried out on the described 3/2-Way Pilot Solenoid Valves 032x with hardware version as shown in the referred mechanical drawings (see section 2.4.1).

The FMEDA builds the basis for an evaluation whether an actuator subsystem, including the 3/2-Way Pilot Solenoid Valves 032x meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

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

2.2 Roles of the parties involved

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG	Manufacturer of the 3/2-Way Pilot Solenoid Valves 032x
exida	Performed the mechanical assessment.

GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG contracted *exida* in November 2013 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N3]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions
[N4]	ISA-TR96.05.01-200_; version B of February 2006	Draft technical report "Partial Stroke Testing For Block Valve Actuators in Safety Instrumented Systems Applications"
[N5]	Final Elements Chris O'Brien & Lindsey Bredemeyer, 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC 61511 Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	ba_0322_0324_0326_de_gb.pdf	Installation, Operating and Maintenance Instructions “Pilot Solenoid Valve, Plastic - 3/2 way, electrically controlled” for 0322, 0324, 0326; 11/2013 88333312
[D2]	db_0322_0324_0326_gb.pdf	Technical datasheet “Pilot Solenoid Valve, Plastic” for 0322, 0324, 0326; 04/2011 88332553
[D3]	6-0300-0156_ELEK_-MAG_-VENTIL-SITZ-KUNSTST_334345.PDF	Mechanical drawing “ELEK.-MAG.-VENTIL-SITZ-KUNSTST” 6-0300-0156 version C of 14.10.08
[D4]	Stückliste 0324_88322112.pdf	Parts list for 3/2-Way Pilot Solenoid Valve 0324

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.4.2 Documentation generated by *exida*

[R1]	FMEDA_V8_PilotValve032x_CLOSE-TSO_V0R2.efm of 06.02.14
[R2]	FMEDA_V8_PilotValve032x_CLOSE-TSO_wTest_V0R2.efm of 04.03.14
[R3]	FMEDA_V8_PilotValve032x_CLOSE-TSO_V0R2 – with valve.efm of 06.02.14
[R4]	FMEDA_V8_PilotValve032x_CLOSE-TSO_wTest_V0R2 – with valve.efm of 04.03.14
[R5]	FMEDA_V8_PilotValve032x_CLOSE-TSO_PTC_V0R2.efm of 11.03.14
[R6]	FMEDA_V8_PilotValve032x_CLOSE-TSO_wTest_PTC_V0R2.efm of 11.03.14
[R7]	Summary_V0R1.xlsx of 11.03.14

3 Description of the analyzed elements

The 3/2-Way Pilot Solenoid Valves 032x can be considered to be Type A elements with a hardware fault tolerance of 0.

Table 4 gives an overview of the different variants that belong to the considered 3/2-Way Pilot Solenoid Valves 032x and explains the differences.

Table 4: Overview of the considered variants

GEMÜ 0322	Designed for single mounting (straight through design) or for modular battery mounting of up to 12 valves (by using clips).
GEMÜ 0324	Designed for direct mounting (hollow bolt) to pneumatically operated valves or other devices.
GEMÜ 0326	Designed for mounting to a compact aluminum rail as a valve battery for mounting in control cabinets or as a valve manifold near the pneumatic components to be controlled. Battery rail for up to 10 valves.

Figure 1 shows drawings of the 3/2-Way Pilot Solenoid Valves 032x.

Figure 1: 3/2-Way Pilot Solenoid Valves 032x

4 Description of diagnostic possibilities

4.1 Partial Valve Stroke Testing (PVST)

PVST is the operation of the actuator / valve through a portion of its total stroke range. This short stroke of operation checks that the actuator / valve is not seized in the running position. The limited stroke of the actuator / valve is intended to be short enough so as not to interfere with the operating flow of the system. The purpose of PVST is to provide a diagnostic check of the SIF function. A possible test set-up is shown in Figure 2.

Partial valve stroke testing is performed at a rate at least ten times faster than the expected demand rate. For SIL 2 safety functions the partial valve stroke test is at least SIL 1 compliant.

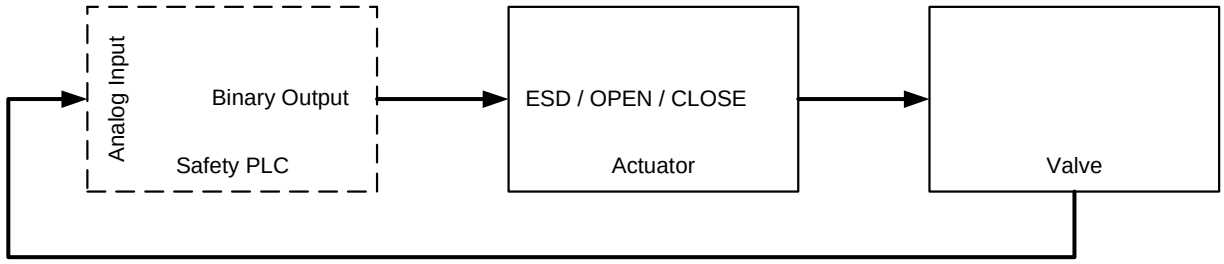

Figure 2: Possible test set-up

Partial stroke testing methods are further described in [N4].

4.2 Full Valve Stroke Testing (FVST)

Full Valve Stroke Testing (FVST) is similar in concept to a PVST, with the variation that the actuator / valve is moved through its full operation stroke during the test. This provides greater diagnostic coverage but typically cannot be performed while the process is running. It is a very effective test that can be automatically executed on batch processes and equipment that periodically shuts down.

5 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by *exida*. The individual results are documented in [R1] to [R7].

5.1 Description of the failure categories

In order to judge the failure behavior of the 3/2-Way Pilot Solenoid Valves 032x, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the state where the solenoid is de-energized and the valve is returned to the CLOSE position (DTT). At GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG this configuration is called “switch position a1”.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed.
Dangerous Detected	Failure that is dangerous but is detected by external testing.
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.
External Leakage	Failure that causes process fluids to leak outside of the valve; External leakage is not considered part of the safety function. External leakage failure rates do not directly contribute the reliability of a valve but should be reviewed for secondary safety and environmental issues.

5.2 Methodology – FMEDA, Failure rates

5.2.1 FMEDA

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

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

5.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from a proprietary mechanical component failure rate database derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to *exida* Profile 3. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

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

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

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

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

5.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 3/2-Way Pilot Solenoid Valves 032x.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The system is installed per the manufacturer's instructions.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Materials are compatible with process conditions and process fluids.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- Only the described variants are used for safety applications.
- Only "switch position a1" is used for safety applications.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- All devices are operated in the low demand mode of operation.
- Full valve stroke testing is performed at a rate at least ten times faster than the expected demand rate.
- For the calculations in section 6.1 the time to detect a dangerous failure by full valve stroke testing is 730 hours.
- For SIL x safety functions the partial valve stroke test is at least SIL (x-1) compliant. If for example the safety function needs to fulfill SIL3 then the partial valve stroke test should be at least SIL2 compliant.
- Failures caused by maintenance capability are site specific and therefore cannot be included.
- The stress levels are average for an industrial outdoor environment and can be compared to *exida* Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.

5.4 Results

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

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

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

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

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

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

This assessment supports the 1_H approach.

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

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

As the 3/2-Way Pilot Solenoid Valves 032x are only one part of a final element, the architectural constraints should be determined for the entire final element.

5.4.1 Air quality failures

The product failure rates that are displayed in this section are failure rates that reflect the situation where the device is used with clean filtered air. Additionally, contamination from poor control air quality may affect the function or air flow in the device. For applications where these assumptions do not apply, the user must estimate the failure rates due to contaminated air and add this failure rate to the product failure rates.

5.4.2 3/2-Way Pilot Solenoid Valves 032x

The FMEDA carried out on the 3/2-Way Pilot Solenoid Valves 032x leads under the assumptions described in sections 5.3 and 5.4 and the definitions given in section 5.1 to the following failure rates according to IEC 61508:2010:

Failure category	Failure rates (in FIT), Profile 3 data	
	Close on Trip	
	Without external test	With external test [6]
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**110**	**110**
Dangerous Detected (λ_{DD})	**0**	**93**
Dangerous Undetected (λ_{DU})	**129**	**36**
No Effect	49	49
External leakage	0	0
PTC	93%	74%
Total failure rate (safety function)	**239**	**239**
SFF [7]	**45%**	**84%**
DC	**0%**	**71%**
SIL AC [8]	**SIL1**	**SIL2**
MTBF(in years)	396	396

[6] Full Valve Stroke Testing (FVST) and leakage testing shall be performed at a rate at least ten times faster than the expected demand rate.

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

[8] 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. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD value.

5.4.3 3/2-Way Pilot Solenoid Valves 032x connected to a process valve

The FMEDA carried out on the 3/2-Way Pilot Solenoid Valves 032x when connected to a process valve leads under the assumptions described in sections 5.3 and 5.4 and the definitions given in section 5.1 to the following failure rates according to IEC 61508:2010:

Failure category	Failure rates (in FIT), Profile 3 data	
	Close on Trip	
	Without external test	With external test [9]
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**110**	**110**
Dangerous Detected (λ_{DD})	**0**	**39**
Dangerous Undetected (λ_{DU})	**39.4**	**0.4**
No Effect	139	139
External leakage	0	0
PTC	99%	0%
Total failure rate (safety function)	**149**	**149**
DC	**0%**	**99%**
MTBF(in years)	396	396

[9] Full Valve Stroke Testing (FVST) and leakage testing shall be performed at a rate at least ten times faster than the expected demand rate.

6 Using the FMEDA results

The following section describes how to apply the results of the FMEDA. It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

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

6.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 3/2-Way Pilot Solenoid Valve 032x with external testing considering additional proof test coverage as indicated in Appendix 1.2. A mission time of 10 years has been assumed, an average Mean Time To Restoration of 389 hours and a maintenance capability of 100%. The failure rate data used in this calculation are displayed in section 5.4.2. The resulting PFD_{AVG} (for a variety of proof test intervals) values are displayed in Table 5.

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

Table 5: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years
PFD_{AVG} = 5.34E-04	PFD_{AVG} = 6.52E-04

As the 3/2-Way Pilot Solenoid Valves 032x are part of an entire safety function they should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget they should be better than or equal to 1.00E-03 for SIL2. The calculated PFD_{AVG} values for a 1 year proof test interval are within the allowed range for SIL2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of the allowed range.

The resulting PFD_{AVG} graph generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 3.

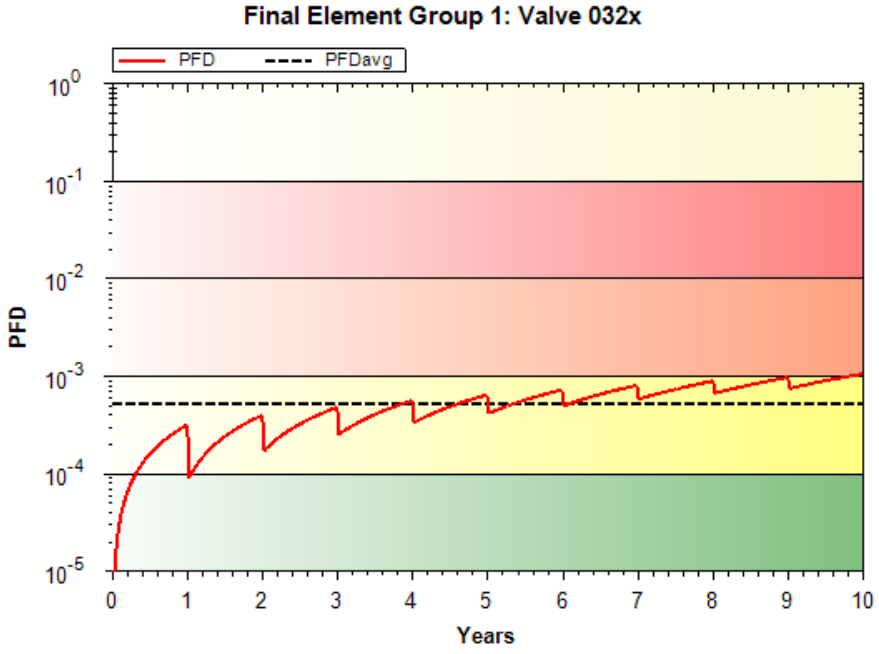

Figure 3: PFD_{AVG} (t) value for 3/2-Way Pilot Solenoid Valves 032x

7 Terms and Definitions

DC	Diagnostic Coverage of dangerous failures (DC = λ_{dd} / (λ_{dd} + λ_{du}))
FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test
	It is assumed that the Partial Stroke Testing, when performed, is performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Stroke Testing also has an impact on the Safe Failure Fraction.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

8 Status of the document

8.1 Liability

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

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

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

8.2 Releases

Version History:	V0R1: Initial version; March 11, 2014
Authors:	Stephan Aschenbrenner
Review:	Not reviewed yet
Release status:	Released to GEMÜ Gebr. Müller Apparatebau GmbH & Co. KG. for review, only

Appendix 1: Possibilities to reveal dangerous faults during the proof test

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

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

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 6.

Table 6: Steps for a suggested proof test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Send a signal to the solenoid valve to perform a full stroke and verify that this is achieved and within the appropriate time.
3	Inspect the solenoid valve for any visible damage or contamination.
4	Remove the bypass and otherwise restore normal operation.

Appendix 1.2: Proof test coverage

The proof test coverage is given in Table 7.

Table 7: Proof test coverage 3/2-Way Pilot Solenoid Valves 032x

CLOSE			
standalone		**connected to process valve**	
without test	**with test**	**without test**	**with test**
93%	74%	99%	0%

The implementer of the SIF needs to confirm the effectiveness of any proof test.

Appendix 2: Impact of lifetime of critical components on the failure rate

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 5.3) this only applies provided that the useful lifetime[10] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions.

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

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

Table 8 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 8: Useful lifetime of components with reduced useful lifetime contributing to λ_{du}

Type	Useful life
Mechanical parts	Approximately 10 years

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

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

Appendix 3: *exida* Environmental Profiles

***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	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[11]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[12]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[13]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[14]	G2	G3	G3	G3	G3	Compatible Material
Surge[15]						
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[16]						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)[17]	6kV	6kV	6kV	6kV	6kV	N/A

[11] Humidity rating per IEC 60068-2-3
[12] Shock rating per IEC 60068-2-6
[13] Vibration rating per IEC 60770-1
[14] Chemical Corrosion rating per ISA 71.04
[15] Surge rating per IEC 61000-4-5
[16] EMI Susceptibility rating per IEC 6100-4-3
[17] ESD (Air) rating per IEC 61000-4-2