Failure Modes, Effects and Diagnostic Analysis

Project:
Abc. X Series Ball Valve

Company:
Abc. Inc.
Sellersville, PA
USA

Contract Number: Q11/12-345
Report No.: Abc 11/12-345 R001
Version V1, Revision R2, September 22, 2011

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 Abc. X Series Ball Valve. 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 and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Abc. X Series Ball Valve. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The X Series Ball Valve is a floating ball design. Most X Series Ball Valves utilize swivel flange and half-ring connections. This connection consists of a swivel flange, a nipple or tube with half-ring groove and two half-rings. The nipple-end can be weld-end, male threaded, hub type or other possible end configurations. Seat seals are available in Celon® and PEEK™. Stem material is 17-4PH Stainless Steel. Sizes range from 1" to 10". Pressure classes range from ANSI 1500 to 10000.

The safety function of the Abc. X Series Ball Valve is to move to the designated safe position within the specified safe time.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Abc. X Series Ball Valve.

Table 1 Version Overview

Option 1	Abc. X Series Ball Valve – Clean Service
Option 2	Abc. X Series Ball Valve – Severe Service

The Abc. X Series Ball Valve are classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The complete final element subsystem, of which a X Series Ball Valve is a part of the final control element, will need to be evaluated to determine the Safe Failure Fraction.

Failure rates for Abc. X Series Ball Valve in clean service are listed in Table 2 and in Table 3 for severe service.

[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 2 Failure rates Abc. X Series Ball Valve in clean service

Failure category	Failure rate (FIT)			Failure rate w/PVST (FIT)		
	Close on Trip		Open on Trip	Close on Trip		Open on Trip
	Full Stroke	Tight-Shutoff		Full Stroke	Tight-Shutoff	
Fail Safe Detected	0	0	0	0	0	172
Fail Safe Undetected	0	0	172	0	0	0
Fail Dangerous Detected	0	0	0	149	149	149
Fail Dangerous Undetected	479	1370	307	330	1221	158
Residual	931	40	931	931	40	931

In addition to the failure rates listed above, the external leakage failure rate of the Abc. X Series Ball Valve is 597 FIT in clean service. External leakage failure rates do not directly contribute to the safety integrity of the valve but should be reviewed for secondary safety and environmental issues.

Table 3 Failure rates Abc. X Series Ball Valve in severe service

Failure category	Failure rate (FIT)			Failure rate w/PVST (FIT)		
	Close on Trip		Open on Trip	Close on Trip		Open on Trip
	Full Stroke	Tight-Shutoff		Full Stroke	Tight-Shutoff	
Fail Safe Detected	0	0	0	0	0	317
Fail Safe Undetected	0	0	317	0	0	0
Fail Dangerous Detected	0	0	0	259	259	259
Fail Dangerous Undetected	858	2615	541	599	2356	282
Residual	1797	40	1797	1797	40	1797

In addition to the failure rates listed above, the external leakage failure rate of the X Series Ball Valve is 732 FIT in severe service. External leakage failure rates do not directly contribute to the safety integrity of the valve 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.

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 4.2.2.

Table 4 lists the failure rates for Abc. X Series Ball Valve in clean service according to IEC 61508.

Table 4 Failure rates according to IEC 61508 in clean service (FIT)

Application	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
Full Stroke, Clean Service	0	0	0	479	--
Tight Shut-Off, Clean Service	0	0	0	1370	--
Open on Trip, Clean Service	0	172	0	307	--
Full Stroke with PVST, Clean Service	0	0	149	330	--
Tight Shut-Off with PVST, Clean Service	0	0	149	1221	--
Open on Trip with PVST, Clean Service	172	0	149	158	--

Table 5 lists the failure rates for Abc. X Series Ball Valve in severe service according to IEC 61508.

Table 5 Failure rates according to IEC 61508 in severe service (FIT)

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Full Stroke, Severe Service	0	0	0	858	--
Tight Shut-Off, Severe Service	0	0	0	2615	--
Open on Trip, Severe Service	0	317	0	541	--
Full Stroke with PVST, Severe Service	0	0	259	599	--
Tight Shut-Off with PVST, Severe Service	0	0	259	2356	--
Open on Trip with PVST, Severe Service	317	0	259	282	--

A user of Abc. X Series Ball Valve 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). A full table of failure rates is presented in section 4.4 along with all assumptions.

[2] It is important to realize that the Residual failures are not included in the Safe Undetected failure category according to IEC 61508 ed2, 2010. Note that these failures on their own, will not affect system reliability or safety, and should not be included in spurious trip calculations.

[3] Safe Failure Fraction needs to be calculated on (sub) system level.

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration per IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

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 Piper Valve Systems PB Series Ball Valve. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a final element subsystem meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

2 Project Management

2.1 *exida*

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

2.2 Roles of the parties involved

Abc. Inc.	Manufacturer of Abc. X Series Ball Valve
exida	Performed the hardware assessment according to Option 1 (see Section 1)

Abc. Inc. contracted *exida* in August 2011 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: 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	exida L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. 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. & Bredemeyer, L., 2009	exida L.L.C., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

2.4 *exida* Tools Used

[T1]	V 2.5.1.7	exSILentia

2.5 Reference Documents

2.5.1 Documentation provided by Abc. Inc.

[D1]	BC204-70004-A, Rev 00, 3/11/2011	Bill of Material Drawing
[D2]	N/A	Abc. Inc. Brochure

2.5.2 Documentation generated by *exida*

[R1]	SAMPLE_FMEDA.xls	Failure Modes, Effects, and Diagnostic Analysis – Abc. X Series Ball Valve
[R2]	SAMPLE_FMEDA.doc, 09/22/2011	FMEDA report, Abc. X Series Ball Valve (this report)

3 Product Description

The X Series Ball Valve is a floating ball design. Most X Series Ball Valves utilize swivel flange and half-ring connections. This connection consists of a swivel flange, a nipple or tube with half-ring groove and two half-rings. The nipple-end can be weld-end, male threaded, hub type or other possible end configurations. Seat seals are available in Celon® and PEEK™. Stem material is 17-4PH Stainless Steel. Sizes range from 1" to 10". Pressure classes range from ANSI 1500 to 10000.

The safety function of the Abc. X Series Ball Valve is to move to the designated safe position within the specified safety time.

Figure 1 shows a X Series Ball Valve.

Figure 1 Abc. X Series Ball Valve – Clean Service

Table 6 gives an overview of the different versions that were considered in the FMEDA of the Abc. X Series Ball Valve.

Table 6 Version Overview

Option 1	Abc. X Series Ball Valve – Clean Service
Option 2	Abc. X Series Ball Valve – Severe Service

Abc. X Series Ball Valve are classified as a Type A[4] device according to IEC 61508, having a hardware fault tolerance of 0.

[4] 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 obtained from Abc. Inc. and is documented in [R1].

4.1 Failure Categories description

In order to judge the failure behavior of Abc. X Series Ball Valve, the following definitions for the failure of the devices were considered.

Fail-Safe State	State where the valve performs the safety function to open or close (depending on the application).
Full Stroke	State where the valve is closed.
Tight-Shutoff	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.
Open onTrip	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 Safe Undetected	Failure that is safe and that is not being diagnosed by automatic diagnostics (such as Partial Valve Stroke Testing).
Fail Safe Detected	Failure that is safe and is detected by automatic diagnostics.
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).
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.
Residual	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 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 the Safe Failure Fraction calculation.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation.

External leakage failure rates do not directly contribute the safety integrity of a valve but should be reviewed for secondary safety and environmental issues.

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

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

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the 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, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook which was derived using 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 *exida* Profile 4 for process wetted parts and Profile 3 for all others. 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”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of Abc. X Series Ball Valve.

- Only a single component failure will fail the entire valve
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 4 for process wetted parts and profile 3 for all others with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by any diagnostics
- Materials are compatible with environmental and process conditions
- The device is installed per 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.
- Partial Valve Stroke Testing, when performed, is automatically performed at a rate at least ten times faster than the expected demand rate.
- Partial valve stroke testing of the SIF includes position detection from the valve stem mounted position sensors and a minimum slew rate, typical of quarter turn installations.
- Worst-case internal fault detection time is the PVST test interval time.
- The valves are mated to a ¼ turn actuator for safety applications.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Abc. X Series Ball Valve FMEDA.

Failure rates for Abc, X Series Ball Valve in clean service are listed in Table 7.

Table 7 Failure rates for Abc. X Series Ball Valve in clean service

Failure category	Failure rate (FIT)			Failure rate w/PVST (FIT)		
	Close on Trip		Open on Trip	Close on Trip		Open on Trip
	Full Stroke	Tight-Shutoff		Full Stroke	Tight-Shutoff	
Fail Safe Detected	0	0	0	0	0	172
Fail Safe Undetected	0	0	172	0	0	0
Fail Dangerous Detected	0	0	0	149	149	149
Fail Dangerous Undetected	479	1370	307	330	1221	158
Residual	931	40	931	931	40	931

In addition to the failure rates listed above, the external leakage failure rate of the Abc. X Series Ball Valve is 597 FIT in clean service. External leakage failure rates do not directly contribute to the safety integrity of the valve 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.

Failure rates for Abc. X Series Ball Valve in severe service are listed in Table 8.

Table 8 Failure rates for Abc. X Series Ball Valve in severe service

Failure category	Failure rate (FIT)			Failure rate w/PVST (FIT)		
	Close on Trip		Open on Trip	Close on Trip		Open on Trip
	Full Stroke	Tight-Shutoff		Full Stroke	Tight-Shutoff	
Fail Safe Detected	0	0	0	0	0	317
Fail Safe Undetected	0	0	317	0	0	0
Fail Dangerous Detected	0	0	0	259	259	259
Fail Dangerous Undetected	858	2615	541	599	2356	282
Residual	1797	40	1797	1797	40	1797

In addition to the failure rates listed above, the external leakage failure rate of the Abc. X Series Ball Valve is 732 FIT in severe service. External leakage failure rates do not directly contribute to the safety integrity of the valve 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.

Table 9 and lists the failure rates for Abc. X Series Ball Valve according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the X Series Ball Valve is only one part of a (sub)system, the SFF should be calculated for the entire final element combination. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF: SFF = 1 - $\lambda_{DU} / \lambda_{TOTAL}$

Table 9 Failure rates according to IEC 61508 in clean service (FIT)

Application	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
Full Stroke, Clean Service	0	0	0	479	--
Tight Shut-Off, Clean Service	0	0	0	1370	--
Open on Trip, Clean Service	0	172	0	307	--
Full Stroke with PVST, Clean Service	0	0	149	330	--
Tight Shut-Off with PVST, Clean Service	0	0	149	1221	--
Open on Trip with PVST, Clean Service	172	0	149	158	--

Table 10 Failure rates according to IEC 61508 in severe service (FIT)

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF[6]
Full Stroke, Severe Service	0	0	0	858	--
Tight Shut-Off, Severe Service	0	0	0	2615	--
Open on Trip, Severe Service	0	317	0	541	--
Full Stroke with PVST, Severe Service	0	0	259	599	--
Tight Shut-Off with PVST, Severe Service	0	0	259	2356	--
Open on Trip with PVST, Severe Service	317	0	259	282	--

The architectural constraint type for a X Series Ball Valve is A. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

[5] It is important to realize that the Residual failures are no longer included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own, will not affect system reliability or safety, and should not be included in spurious trip calculations.

[6] Safe Failure Fraction needs to be calculated on (sub) system level.

5 Using the FMEDA Results

5.1 PFD_{AVG} Calculation Abc. X Series Ball Valve

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) X Series Ball Valve with *exida's* exSILentia tool. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years and a Mean Time To Restoration of 96 hours has been assumed. Table 11 lists the proof test coverage (see Appendix B) used for the various configurations as well as the results when the proof test interval equals 1 year.

Table 11 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD_{AVG}	% of SIL 1 Range
Abc. X Series Ball Valve - Full Stroke, Clean Service	48%	1.18E-02	12%
Abc. X Series Ball Valve - Full Stroke, Clean Service – PVST	26%	1.12E-02	11%

The resulting PFD_{AVG} graphs generated from the exSILentia tool for a proof test interval of 1 year are displayed in Figure 2.

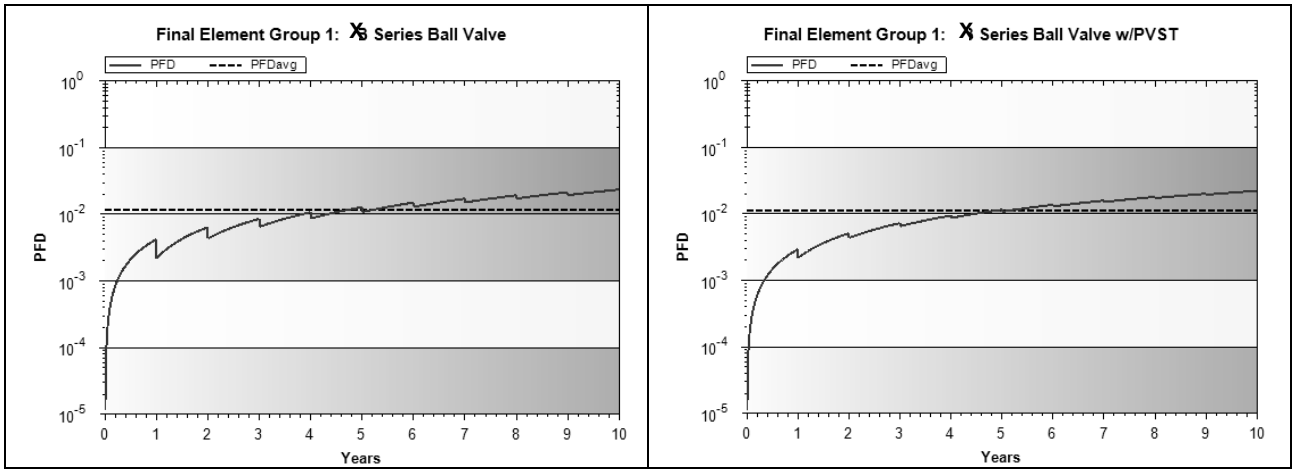


Figure 2 PFDavg value for a single, Abc X Series Ball Valve with proof test intervals of 1 year.

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. For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of Abc. X Series Ball Valve is approximately equal to 11% of the range without PVST.

When performing partial valve stroke testing at regular intervals, a X Series Ball Valve contributes less to the overall PFD_{AVG} of the Safety Instrumented Function. These 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 Terms and Definitions

FIT	Failure In Time (1x10-9 failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval and is equal to or greater than one year.
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 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.
Proof Test	Periodic test performed manually to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
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).
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
Severe service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.

7 Status of the Document

7.1 Liability

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

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

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

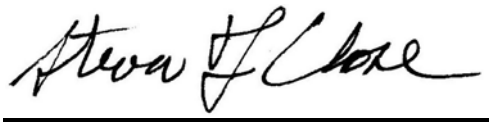
7.2 Releases

Version:	V1	
Revision:	R2	
Version History:	V1, R2:	Revised Low Demand Mode definition, September 22, 2011
	V1, R1:	Released to Abc. Inc, September 20, 2011
	V0, R1:	Draft; September 20, 2011
Author(s):		
Review:	V0, R1:	Reviewed September 20, 2011
Release Status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Steven Close, Safety Engineer

Dr. William M. Goble, Principal Partner

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 assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[7] 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 X Series Ball Valve per the manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

A useful life period of 10 to 15 years or 10,000 cycles is expected for the Abc. X Series Ball Valve. Based on general field failure data a product life period of approximately 30 years is expected for the Abc. X Series Ball Valve if the lower level components are renewed before the end of their useful life and the device is maintained per manufacturer's instructions.

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

[7] 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 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 actuator and/or valve, see Table 12.

Table 12 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the signal/supply to the actuator to force the actuator and valve to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time.
3.	Re-store the supply/signal to the actuator and inspect for any visible damage or contamination and confirm that the normal operating state was achieved.
4.	Inspect the valve for any leaks, visible damage or contamination.
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 product configurations is given in Table 13.

Table 13 Proof Test Coverage – Abc. X Series Ball Valve

Device	Application	No PVST	PVST
Abc. X Series Ball Valve – Clean Service	Close On Trip – Full Stroke	48%	25%
	Close On Trip – Tight Shutoff	17%	7%
	Open On Trip	75%	51%
Abc. X Series Ball Valve – Severe Service	Close On Trip – Full Stroke	46%	23%
	Close On Trip – Tight Shutoff	15%	6%
	Open On Trip	73%	48%