Failure Modes, Effects and Diagnostic Analysis

Project:
T-Series Trunnion Ball Valve

Company:
MOGAS Industries, Inc.
Houston, TX
USA

Contract Number: Q16/10-021
Report No.: MOG 16-10-021 R002
Version V1, Revision R1, December 20, 2016
Chris O'Brien
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 T-Series Trunnion 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 are determined. The FMEDA that is described in this report concerns only the hardware of the T-Series Trunnion Ball Valve. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Safety Function of the T-Series Trunnion Ball Valve is to Open or Close (Full Stroke, Tight Shut-Off, or Open on Trip) per the final element design within the specified safety time.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the T-Series Trunnion Ball Valve.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Full Stroke, Clean Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 2</td>
<td>Tight Shut-Off, Clean Service</td>
</tr>
<tr>
<td>Option 3</td>
<td>Open on Trip, Clean Service</td>
</tr>
<tr>
<td>Option 4</td>
<td>Full Stroke with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 5</td>
<td>Tight Shut-Off with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 6</td>
<td>Open on Trip with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 7</td>
<td>Full Stroke, Severe Service</td>
</tr>
<tr>
<td>Option 8</td>
<td>Tight Shut-Off, Severe Service</td>
</tr>
<tr>
<td>Option 9</td>
<td>Open on Trip, Severe Service</td>
</tr>
<tr>
<td>Option 10</td>
<td>Full Stroke with PVST, Severe Service</td>
</tr>
<tr>
<td>Option 11</td>
<td>Tight Shut-Off with PVST, Severe Service</td>
</tr>
<tr>
<td>Option 12</td>
<td>Open on Trip with PVST, Severe Service</td>
</tr>
</tbody>
</table>

The T-Series Trunnion Ball Valve is classified as a device that is part of a Type A 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. See Section 5.2. Therefore, the T-Series Trunnion Ball Valve can be classified as a 2 device when the listed failure rates are used. When 2 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 2. If Route 2 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 T-Series Trunnion Ball Valve are listed in section 4.4.

1 Type A element: "Non-Complex" element (using discrete components); for details see 7.4.1.2 of IEC 61508-2, ed2, 2010.
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 250 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 T-Series Trunnion 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).
# Table of Contents

1. Purpose and Scope ........................................................................................................ 5

2. Project Management ...................................................................................................... 6
   2.1 *exida* .................................................................................................................. 6
   2.2 Roles of the parties involved ...................................................................................... 6
   2.3 Standards and literature used ..................................................................................... 6
   2.4 Reference documents ............................................................................................... 7
      2.4.1 Documentation provided by MOGAS Industries, Inc. ......................................... 7
      2.4.2 Documentation generated by *exida* ................................................................. 7

3. Product Description ........................................................................................................ 8

4. Failure Modes, Effects, and Diagnostic Analysis .......................................................... 10
   4.1 Failure categories description ................................................................................... 10
   4.2 Methodology – FMEDA, failure rates ....................................................................... 11
      4.2.1 FMEDA ............................................................................................................. 11
      4.2.2 Failure rates ...................................................................................................... 11
   4.3 Assumptions .............................................................................................................. 11
   4.4 Results ...................................................................................................................... 13

5. Using the FMEDA Results ............................................................................................ 16
   5.1 PFD$_{avg}$ calculation T-Series Trunnion Ball Valve ............................................... 16
   5.2 *exida* Route $2_H$ Criteria ................................................................................... 16

6. Terms and Definitions ................................................................................................... 18

7. Status of the Document ................................................................................................ 20
   7.1 Liability ..................................................................................................................... 20
   7.2 Releases ..................................................................................................................... 20
   7.3 Future enhancements ............................................................................................... 20
   7.4 Release signatures ..................................................................................................... 21

Appendix A  Lifetime of Critical Components ................................................................. 22

Appendix B  Proof Tests to Reveal Dangerous Undetected Faults ................................... 23
   B.1 Suggested Proof Test ............................................................................................... 23
   B.2 Proof Test Coverage ............................................................................................... 23

Appendix C  *exida* Environmental Profiles ................................................................. 25

Appendix D  Determining Safety Integrity Level ............................................................ 26

Appendix E  Site Safety Index ........................................................................................... 30
   E.1 Site Safety Index Profiles ....................................................................................... 30
   E.2 Site Safety Index Failure Rates – T-Series Trunnion Ball Valve ............................... 31
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 T-Series Trunnion Ball Valve. 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, cybersecurity and availability. 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 system consulting services, safety lifecycle engineering tools, detailed product assurance, cybersecurity and functional safety certification, and a collection of on-line safety and reliability resources. exida maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2  Roles of the parties involved

MOGAS Industries, Inc. Manufacturer of the T-Series Trunnion Ball Valve

exida Performed the hardware assessment

MOGAS Industries, Inc. contracted exida in October 2016 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.

<table>
<thead>
<tr>
<th>N</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

### 2.4 Reference documents

#### 2.4.1 Documentation provided by MOGAS Industries, Inc.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D1]</td>
<td>T Series Valve Components, Rev 2</td>
</tr>
<tr>
<td></td>
<td>Exploded Drawing</td>
</tr>
<tr>
<td>[D2]</td>
<td>ESI-6142, Rev A</td>
</tr>
<tr>
<td></td>
<td>IOM Manual</td>
</tr>
</tbody>
</table>

#### 2.4.2 Documentation generated by exida

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1]</td>
<td>Q16-10-021 W002 V1R1 Mogas C Series.xls, V1R1, 12/16/16</td>
</tr>
<tr>
<td></td>
<td>Failure Modes, Effects, and Diagnostic Analysis – T-Series Trunnion Ball Valve (internal document)</td>
</tr>
<tr>
<td>[R2]</td>
<td>MOG Q16-10-021 R002, V1R1, 20-Dec-16</td>
</tr>
<tr>
<td></td>
<td>FMEDA report, T-Series Trunnion Ball Valve (this report)</td>
</tr>
</tbody>
</table>
3 Product Description

The C-Series valve is an excellent choice in large bore isolation applications. Each ball and seat subassembly is mate-lapped by hand and put through a rigorous testing procedure to ensure its integrity.

The C-Series valve is available in full or reduced bore, ½ inch to 42 inches and in a wide variety of end connections.

Specifications:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valve Sizes:</td>
<td>Valve Sizes 2” through 42”</td>
</tr>
<tr>
<td>Pressure Ratings:</td>
<td>ANSI Class 300 to ANSI Class 2500</td>
</tr>
</tbody>
</table>

Figure 1 Typical T-Series Trunnion Ball Valve covered in this FMEDA,

Table 2 gives an overview of the different versions that were considered in the FMEDA of the T-Series Trunnion Ball Valve.
Table 2 Version Overview

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Full Stroke, Clean Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 2</td>
<td>Tight Shut-Off, Clean Service</td>
</tr>
<tr>
<td>Option 3</td>
<td>Open on Trip, Clean Service</td>
</tr>
<tr>
<td>Option 4</td>
<td>Full Stroke with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 5</td>
<td>Tight Shut-Off with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 6</td>
<td>Open on Trip with PVST, Clean Service</td>
</tr>
<tr>
<td>Option 7</td>
<td>Full Stroke, Severe Service</td>
</tr>
<tr>
<td>Option 8</td>
<td>Tight Shut-Off, Severe Service</td>
</tr>
<tr>
<td>Option 9</td>
<td>Open on Trip, Severe Service</td>
</tr>
<tr>
<td>Option 10</td>
<td>Full Stroke with PVST, Severe Service</td>
</tr>
<tr>
<td>Option 11</td>
<td>Tight Shut-Off with PVST, Severe Service</td>
</tr>
<tr>
<td>Option 12</td>
<td>Open on Trip with PVST, Severe Service</td>
</tr>
</tbody>
</table>

The T-Series Trunnion Ball Valve is classified as a device that is a part of a Type A\(^2\) element according to IEC 61508, having a hardware fault tolerance of 0.

\(^2\) Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.
4 Failure Modes, Effects, and Diagnostic Analysis

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

4.1 Failure categories description

In order to judge the failure behavior of the T-Series Trunnion Ball Valve, the following definitions for the failure of the device were considered.

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

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

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

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

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

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

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

External Leakage: Failure that causes process fluids, gas, hydraulic fluids or operating media to leak outside of the valve or actuator; External Leakage is not considered part of the safety function and therefore this failure rate is not included in any of the other 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 a given application. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category [N13].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by exida in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which were derived using over 250 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 MOGAS Industries, Inc.. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

The failure rates are predicted for a Site Safety Index of SSI=2 ([N10] & [N11]) as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from exida.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment. exida Environmental Profiles listing expected stress levels can be found in Appendix C. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant. exida has detailed models available to make customized failure rate predictions (Contact exida).

Accurate plant specific data may be used to check validity of this failure rate data. If a user has data collected from a good proof test reporting system such as exida SILStat™ 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 T-Series Trunnion Ball Valve.

- The worst case assumption of a series system is made. Therefore, only a single component failure will fail the entire T-Series Trunnion Ball Valve, therefore 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.

• Failures caused by the operational / maintenance culture are site specific and modeled by the Site Safety index (SSI). Failure rates are presented for an average realistic level (SSI=2) and for comparison purposes at an ideal level, SSI=4.

• The stress levels are specified in the exida Profile used for the analysis are limited by the manufacturer’s published ratings.

• Materials are compatible with the environmental and process conditions.

• The device is installed and operated per the manufacturer’s instructions.

• Valves are installed such that the controlled substance will flow through the valve in the direction indicated by the flow arrow, located on the valve body.

• In order to claim diagnostic coverage for Partial Valve Stroke Testing it is automatically performed at a rate at least ten times faster than the Demand frequency.

• Partial Valve Stroke Testing of the final element includes position detection from actuator top mounted position sensors, typical of quarter turn installations.

• Worst-case internal fault detection time is the PVST test interval time.
4.4 Results

Using reliability data extracted from the exida Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the FMEDA analysis of the T-Series Trunnion Ball Valve.

Table 3 and Table 4 lists the failure rates for the T-Series Trunnion Ball Valve according to IEC 61508 with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix E for an explanation of SSI and the failure rates for SSI of 4 (ideal maintenance practices).

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

<table>
<thead>
<tr>
<th>Application/Device/Configuration</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}$</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>#</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Stroke, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>549</td>
<td>692</td>
<td>487</td>
</tr>
<tr>
<td>Tight Shut-Off, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1118</td>
<td>123</td>
<td>487</td>
</tr>
<tr>
<td>Open on Trip, Clean Service</td>
<td>0</td>
<td>131</td>
<td>0</td>
<td>418</td>
<td>692</td>
<td>487</td>
</tr>
<tr>
<td>Full Stroke with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>236</td>
<td>313</td>
<td>692</td>
<td>487</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>236</td>
<td>882</td>
<td>123</td>
<td>487</td>
</tr>
<tr>
<td>Open on Trip with PVST, Clean Service</td>
<td>130</td>
<td>1</td>
<td>236</td>
<td>182</td>
<td>692</td>
<td>487</td>
</tr>
<tr>
<td>Full Stroke, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>941</td>
<td>1284</td>
<td>532</td>
</tr>
<tr>
<td>Tight Shut-Off, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2012</td>
<td>213</td>
<td>532</td>
</tr>
<tr>
<td>Open on Trip, Severe Service</td>
<td>0</td>
<td>253</td>
<td>0</td>
<td>689</td>
<td>1284</td>
<td>532</td>
</tr>
<tr>
<td>Full Stroke with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>388</td>
<td>554</td>
<td>1284</td>
<td>532</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>388</td>
<td>1625</td>
<td>213</td>
<td>532</td>
</tr>
<tr>
<td>Open on Trip with PVST, Severe Service</td>
<td>250</td>
<td>3</td>
<td>388</td>
<td>301</td>
<td>1284</td>
<td>532</td>
</tr>
</tbody>
</table>

3 Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
4 It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
Table 4 Failure rates for Dynamic Applications with Good Maintenance Assumptions in FIT @ SSI=2

<table>
<thead>
<tr>
<th>Application/Device/Configuration</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}$</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>#</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Stroke, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>333</td>
<td>713</td>
<td>487</td>
</tr>
<tr>
<td>Tight Shut-Off, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>916</td>
<td>130</td>
<td>487</td>
</tr>
<tr>
<td>Open on Trip, Clean Service</td>
<td>0</td>
<td>163</td>
<td>0</td>
<td>170</td>
<td>713</td>
<td>487</td>
</tr>
<tr>
<td>Full Stroke with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>91</td>
<td>242</td>
<td>713</td>
<td>487</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>91</td>
<td>825</td>
<td>130</td>
<td>487</td>
</tr>
<tr>
<td>Open on Trip with PVST, Clean Service</td>
<td>161</td>
<td>2</td>
<td>91</td>
<td>79</td>
<td>713</td>
<td>487</td>
</tr>
<tr>
<td>Full Stroke, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>573</td>
<td>1303</td>
<td>532</td>
</tr>
<tr>
<td>Tight Shut-Off, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1658</td>
<td>219</td>
<td>532</td>
</tr>
<tr>
<td>Open on Trip, Severe Service</td>
<td>0</td>
<td>306</td>
<td>0</td>
<td>268</td>
<td>1303</td>
<td>532</td>
</tr>
<tr>
<td>Full Stroke with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>138</td>
<td>435</td>
<td>1303</td>
<td>532</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>138</td>
<td>1520</td>
<td>219</td>
<td>532</td>
</tr>
<tr>
<td>Open on Trip with PVST, Severe Service</td>
<td>303</td>
<td>3</td>
<td>138</td>
<td>129</td>
<td>1303</td>
<td>532</td>
</tr>
</tbody>
</table>

Where:

$\lambda_{SD}$ = Fail Safe Detected
$\lambda_{SU}$ = Fail Safe Undetected
$\lambda_{DD}$ = Fail Dangerous Detected
$\lambda_{DU}$ = Fail Dangerous Undetected
# = No Effect Failures
E = External Leaks

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.

---

5 Dynamic Application failure rates may be used if the device moves at least once every 200 hours.
6 It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1\text{H} approach according to 7.4.4.2 of IEC 61508 or the 2\text{H} approach according to 7.4.4.3 of IEC 61508, or the approach according to IEC 61511:2016 which is based on 2\text{H} (See Section 5.2).

The 1\text{H} approach involves calculating the Safe Failure Fraction for the entire element.

The 2\text{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 \textit{exida} criteria for Route 2\text{H} which is more stringent than IEC 61508. Therefore, the T-Series Trunnion Ball Valve meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates from Table 3 are used.

If Route 2\text{H} is not applicable for all devices that constitute the entire element, the architectural constraints will need to be evaluated per Route 1\text{H}.

The architectural constraint type for the T-Series Trunnion Ball Valve is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

Table 10 and Table 11 (appendix E) list the failure rates for the T-Series Trunnion Ball Valve according to IEC 61508 with a Site Safety Index (SSI) of 4 (perfect site maintenance practices). This data should not be used for SIL verification and is provided only for comparison with other analysis that has assumed perfect maintenance. See Appendix E for an explanation of SSI.
5 Using the FMEDA Results

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

5.1 PFD\textsubscript{avg} calculation T-Series Trunnion Ball Valve

Using the failure rate data displayed in Table 3, section 4.4, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD\textsubscript{avg}) calculation can be performed for the entire final element.

Probability of Failure on Demand (PFD\textsubscript{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD\textsubscript{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD\textsubscript{avg} by making many assumptions about the application and operational policies of a site which may be incorrect. Therefore, the use of pre-calculated PFD\textsubscript{avg} numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD\textsubscript{avg}) calculation is best accomplished with exida’s exSILentia tool. See Appendix D for a complete description of how to determine the Safety Integrity Level for the final element. The mission time used for the calculation depends on the PFD\textsubscript{avg} target and the useful life of the product. The failure rates for all the devices in the final element and the proof test coverage for the final element are required to perform the PFD\textsubscript{avg} calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the T-Series Trunnion Ball Valve are listed in Table 7. This is combined with the dangerous failure rates after proof test for other devices in the final element to establish the proof test coverage for the final element.

When performing Partial Valve Stroke Testing at regular intervals, the T-Series Trunnion Ball Valve contributes less to the overall PFD\textsubscript{avg} of the Safety Instrumented Function.

5.2 exida Route 2\textsubscript{H} Criteria

IEC 61508, ed2, 2010 describes the Route 2\textsubscript{H} alternative to Route 1\textsubscript{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 undertake 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\textsubscript{H}, exida has established the following:

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" vs. "systematic" are checked by exida; and
5. every component used in an FMEDA meets the above criteria.

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

Automatic Diagnostics Tests performed online internally by the device or, if specified, externally by another device without manual intervention.

Device A device is something that is part of an element; but, cannot perform an element safety function on its own.

Dynamic Applications The movement interval of the final element device is less than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.

Element A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.

exida criteria A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2nd 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.

PFDavg 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.

Random Capability The SIL limit imposed by the Architectural Constraints for each element.

Severe Service Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.

SFF Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.

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).

SSI  Site Safety Index (See Appendix E)

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

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
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 Releases

Version History:  
V1, R1: Released to MOGAS Industries, Inc.; December 20, 2016
V0, R1: Draft; December 16, 2016

Author(s): Chris O’Brien

Review:  
V0, R1: Greg Sauk (exida); December 16, 2016

Release Status: Released to MOGAS Industries, Inc.

7.3 Future enhancements

At request of client.
7.4 Release signatures

Chris O'Brien, CFSE, Partner

Gregory Sauk, CFSE, Senior Safety Engineer
Appendix A  Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be 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\(_{\text{avg}}\) 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 T-Series Trunnion Ball Valve per manufacturer’s instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 15 years is expected for the T-Series Trunnion Ball Valve.

For high demand mode applications, the useful lifetime is limited by the number of cycles. The useful lifetime of the Valve Seals is \(> 10,000\) full scale cycles or 8 to 10 years, whichever results in the shortest lifetime.

When manufacturer recommendation or plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on manufacturer recommendation or 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 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 5. Refer to the table in B.2 for the Proof Test Coverages.

Table 5 Suggested Proof Test – T-Series Trunnion Ball Valve

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

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 is given in Table 6 and Table 7.

Table 6 Static Proof Test Results – T-Series Trunnion Ball Valve

<table>
<thead>
<tr>
<th>Application</th>
<th>Safety Function</th>
<th>$\lambda_{DUPT}$ (FIT)</th>
<th>Proof Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>No PVST</td>
</tr>
<tr>
<td>Clean Service</td>
<td>Close On Trip – Full Stroke</td>
<td>195</td>
<td>64%</td>
</tr>
<tr>
<td></td>
<td>Close On Trip – Tight Shutoff</td>
<td>765</td>
<td>32%</td>
</tr>
<tr>
<td></td>
<td>Open On Trip</td>
<td>64</td>
<td>85%</td>
</tr>
<tr>
<td>Severe Service</td>
<td>Close On Trip – Full Stroke</td>
<td>360</td>
<td>62%</td>
</tr>
<tr>
<td></td>
<td>Close On Trip – Tight Shutoff</td>
<td>1431</td>
<td>29%</td>
</tr>
<tr>
<td></td>
<td>Open On Trip</td>
<td>107</td>
<td>84%</td>
</tr>
</tbody>
</table>

\( \lambda_{DUPT} = \) Dangerous undetected failure rate after performing the recommended proof test.
Table 7 Dynamic Proof Test Results – T-Series Trunnion Ball Valve

<table>
<thead>
<tr>
<th>Application</th>
<th>Safety Function</th>
<th>$\lambda_{DU}^{PT}$ (FIT)</th>
<th>Proof Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>No PVST</td>
</tr>
<tr>
<td>Clean Service</td>
<td>Close On Trip – Full Stroke</td>
<td>197</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td>Close On Trip – Tight Shutoff</td>
<td>780</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>Open On Trip</td>
<td>34</td>
<td>80%</td>
</tr>
<tr>
<td>Severe Service</td>
<td>Close On Trip – Full Stroke</td>
<td>366</td>
<td>36%</td>
</tr>
<tr>
<td></td>
<td>Close On Trip – Tight Shutoff</td>
<td>1451</td>
<td>12%</td>
</tr>
<tr>
<td></td>
<td>Open On Trip</td>
<td>60</td>
<td>78%</td>
</tr>
</tbody>
</table>

$\lambda_{DU}^{PT}$ = Dangerous undetected failure rate after performing the recommended proof test.
## Appendix C  *exida* Environmental Profiles

### Table 8 *exida* Environmental Profiles

<table>
<thead>
<tr>
<th><em>exida</em> Profile</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description (Electrical)</strong></td>
<td>Cabinet mounted/Climate Controlled</td>
<td>Low Power Field Mounted no self-heating</td>
<td>General Field Mounted self-heating</td>
<td>Subsea</td>
<td>Offshore</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Description (Mechanical)</strong></td>
<td>Cabinet mounted/Climate Controlled</td>
<td>General Field Mounted</td>
<td>General Field Mounted</td>
<td>Subsea</td>
<td>Offshore</td>
<td>Process Wetted</td>
</tr>
<tr>
<td><strong>IEC 60654-1 Profile</strong></td>
<td>B2</td>
<td>C3 applicable for D1</td>
<td>C3 applicable for D1</td>
<td>N/A</td>
<td>C3 applicable for D1</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Average Ambient Temperature</strong></td>
<td>30 C</td>
<td>25 C</td>
<td>25 C</td>
<td>5 C</td>
<td>25 C</td>
<td>25 C</td>
</tr>
<tr>
<td><strong>Average Internal Temperature</strong></td>
<td>60 C</td>
<td>30 C</td>
<td>45 C</td>
<td>5 C</td>
<td>45 C</td>
<td>Process Fluid Temp.</td>
</tr>
<tr>
<td><strong>Daily Temperature Excursion (pk-pk)</strong></td>
<td>5 C</td>
<td>25 C</td>
<td>25 C</td>
<td>0 C</td>
<td>25 C</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Seasonal Temperature Excursion (winter average vs. summer average)</strong></td>
<td>5 C</td>
<td>40 C</td>
<td>40 C</td>
<td>2 C</td>
<td>40 C</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Exposed to Elements / Weather Conditions</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Humidity</strong>&lt;sup&gt;10&lt;/sup&gt;</td>
<td>0-95% Non-Condensing</td>
<td>0-100% Condensing</td>
<td>0-100% Condensing</td>
<td>0-100% Condensing</td>
<td>0-100% Condensing</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Shock</strong>&lt;sup&gt;11&lt;/sup&gt;</td>
<td>10 g</td>
<td>15 g</td>
<td>15 g</td>
<td>15 g</td>
<td>15 g</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Vibration</strong>&lt;sup&gt;12&lt;/sup&gt;</td>
<td>2 g</td>
<td>3 g</td>
<td>3 g</td>
<td>3 g</td>
<td>3 g</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Chemical Corrosion</strong>&lt;sup&gt;13&lt;/sup&gt;</td>
<td>G2</td>
<td>G3</td>
<td>G3</td>
<td>G3</td>
<td>G3</td>
<td>Compatible Material</td>
</tr>
<tr>
<td><strong>Surge</strong>&lt;sup&gt;14&lt;/sup&gt;</td>
<td>Line-Line 0.5 kV</td>
<td>1 kV</td>
<td>0.5 kV</td>
<td>0.5 kV</td>
<td>0.5 kV</td>
<td>0.5 kV</td>
</tr>
<tr>
<td><strong>EMI Susceptibility</strong>&lt;sup&gt;15&lt;/sup&gt;</td>
<td>Line-Ground 1 kV</td>
<td>1 kV</td>
<td>1 kV</td>
<td>1 kV</td>
<td>1 kV</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>ESD (Air)</strong>&lt;sup&gt;16&lt;/sup&gt;</td>
<td>80 MHz to 1.4 GHz 10 V/m</td>
<td>10 V/m</td>
<td>10 V/m</td>
<td>10 V/m</td>
<td>10 V/m</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>ESD (Air)</strong>&lt;sup&gt;16&lt;/sup&gt;</td>
<td>1.4 GHz to 2.0 GHz 3 V/m</td>
<td>3 V/m</td>
<td>3 V/m</td>
<td>3 V/m</td>
<td>3 V/m</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>ESD (Air)</strong>&lt;sup&gt;16&lt;/sup&gt;</td>
<td>2.0 GHz to 2.7 GHz 1 V/m</td>
<td>1 V/m</td>
<td>1 V/m</td>
<td>1 V/m</td>
<td>1 V/m</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>ESD (Air)</strong>&lt;sup&gt;16&lt;/sup&gt;</td>
<td>6 kV</td>
<td>6 kV</td>
<td>6 kV</td>
<td>6 kV</td>
<td>6 kV</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<sup>10</sup> Humidity rating per IEC 60068-2-3  
<sup>11</sup> Shock rating per IEC 60068-2-27  
<sup>12</sup> Vibration rating per IEC 60068-2-6  
<sup>13</sup> Chemical Corrosion rating per ISA 71.04  
<sup>14</sup> Surge rating per IEC 61000-4-5  
<sup>15</sup> EMI Susceptibility rating per IEC 61000-4-3  
<sup>16</sup> ESD (Air) rating per IEC 61000-4-2
Appendix D  Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). The numbers used in the examples are not for the product described in this report.

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N4] and [N7].

These are:
A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;
B. Architecture Constraints (minimum redundancy requirements) are met; and
C. a PFD$_{avg}$ calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N8].

C. Probability of Failure on Demand (PFD$_{avg}$) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD$_{avg}$) must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the exida FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD$_{avg}$ for any given set of variables.
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore, idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSiLentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03 (Figure 2).

![Figure 2: exSiLentia results for idealistic variables.](image)
If the Proof Test Internal for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

![Figure 3: PFDavg versus Proof Test Interval](image)

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD\textsubscript{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD\textsubscript{avg} contributions are Sensor PFD\textsubscript{avg} = 2.77E-03, Logic Solver PFD\textsubscript{avg} = 1.14E-05, and Final Element PFD\textsubscript{avg} = 5.49E-02 (Figure 4).
It is clear that $PFD_{avg}$ results can change an entire SIL level or more when all critical variables are not used.
Appendix E  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.

E.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 9 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 9 exida Site Safety Index Profiles

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSI 4</td>
<td>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. <strong>Note</strong>: This level is generally considered not possible but retained in the model for comparison purposes.</td>
</tr>
<tr>
<td>SSI 3</td>
<td>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.</td>
</tr>
<tr>
<td>SSI 2</td>
<td>Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.</td>
</tr>
<tr>
<td>SSI 1</td>
<td>Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.</td>
</tr>
<tr>
<td>SSI 0</td>
<td>None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.</td>
</tr>
</tbody>
</table>
### E.2 Site Safety Index Failure Rates – T-Series Trunnion Ball Valve

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

Table 10 and Table 11 lists the failure rates for the T-Series Trunnion Ball Valve according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

**Table 10 Failure rates for Static Applications**\(^{17}\) with Ideal Maintenance Assumption in FIT @ SSI=4

<table>
<thead>
<tr>
<th>Application/Device/Configuration</th>
<th>(\lambda_{SD})</th>
<th>(\lambda_{SU}) (^{18})</th>
<th>(\lambda_{DD})</th>
<th>(\lambda_{DU})</th>
<th>#</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Stroke, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>275</td>
<td>415</td>
<td>292</td>
</tr>
<tr>
<td>Tight Shut-Off, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>559</td>
<td>74</td>
<td>292</td>
</tr>
<tr>
<td>Open on Trip, Clean Service</td>
<td>0</td>
<td>79</td>
<td>0</td>
<td>209</td>
<td>415</td>
<td>292</td>
</tr>
<tr>
<td>Full Stroke with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>118</td>
<td>157</td>
<td>415</td>
<td>292</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>118</td>
<td>441</td>
<td>74</td>
<td>292</td>
</tr>
<tr>
<td>Open on Trip with PVST, Clean Service</td>
<td>78</td>
<td>1</td>
<td>118</td>
<td>91</td>
<td>415</td>
<td>292</td>
</tr>
<tr>
<td>Full Stroke, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>471</td>
<td>770</td>
<td>319</td>
</tr>
<tr>
<td>Tight Shut-Off, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1006</td>
<td>128</td>
<td>319</td>
</tr>
<tr>
<td>Open on Trip, Severe Service</td>
<td>0</td>
<td>152</td>
<td>0</td>
<td>345</td>
<td>770</td>
<td>319</td>
</tr>
<tr>
<td>Full Stroke with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>194</td>
<td>277</td>
<td>770</td>
<td>319</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>194</td>
<td>813</td>
<td>128</td>
<td>319</td>
</tr>
<tr>
<td>Open on Trip with PVST, Severe Service</td>
<td>150</td>
<td>2</td>
<td>194</td>
<td>151</td>
<td>770</td>
<td>319</td>
</tr>
</tbody>
</table>

\(^{17}\) Static Application failure rates are applicable if the device is static for a period of more than 200 hours.

\(^{18}\) It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
Table 11 Failure rates for Dynamic Applications\textsuperscript{19} with Ideal Maintenance Assumption in FIT @ SSI=4

<table>
<thead>
<tr>
<th>Application/Device/Configuration</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}$\textsuperscript{20}</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>#</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Stroke, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>167</td>
<td>428</td>
<td>292</td>
</tr>
<tr>
<td>Tight Shut-Off, Clean Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>458</td>
<td>78</td>
<td>292</td>
</tr>
<tr>
<td>Open on Trip, Clean Service</td>
<td>0</td>
<td>98</td>
<td>0</td>
<td>85</td>
<td>428</td>
<td>292</td>
</tr>
<tr>
<td>Full Stroke with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>121</td>
<td>428</td>
<td>292</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Clean Service</td>
<td>0</td>
<td>0</td>
<td>46</td>
<td>413</td>
<td>78</td>
<td>292</td>
</tr>
<tr>
<td>Open on Trip with PVST, Clean Service</td>
<td>97</td>
<td>1</td>
<td>46</td>
<td>40</td>
<td>428</td>
<td>292</td>
</tr>
<tr>
<td>Full Stroke, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>287</td>
<td>782</td>
<td>319</td>
</tr>
<tr>
<td>Tight Shut-Off, Severe Service</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>829</td>
<td>131</td>
<td>319</td>
</tr>
<tr>
<td>Open on Trip, Severe Service</td>
<td>0</td>
<td>184</td>
<td>0</td>
<td>134</td>
<td>782</td>
<td>319</td>
</tr>
<tr>
<td>Full Stroke with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>69</td>
<td>218</td>
<td>782</td>
<td>319</td>
</tr>
<tr>
<td>Tight Shut-Off with PVST, Severe Service</td>
<td>0</td>
<td>0</td>
<td>69</td>
<td>760</td>
<td>131</td>
<td>319</td>
</tr>
<tr>
<td>Open on Trip with PVST, Severe Service</td>
<td>182</td>
<td>2</td>
<td>69</td>
<td>65</td>
<td>782</td>
<td>319</td>
</tr>
</tbody>
</table>

\textsuperscript{19} Dynamic Application failure rates may be used if the device moves at least once every 200 hours.
\textsuperscript{20} It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.