IEC 61508 Functional Safety Assessment

Project:
V316, B316 and C316 Solenoid and Pilot Valve Series

Customer:
Versa Products Company, Inc.
Paramus, NJ
USA

Contract Number: Q12/12-023
Report No.: VER 12/12-023 R004
Version V1, Revision R1, June 25, 2013
Gregory Sauk
Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

- V316 Series Solenoid and Pilot Valves
- B316 Series Solenoid and Pilot Valves
- C316 Series Solenoid and Pilot Valves

The functional safety assessment performed by exida consisted of the following activities:

- exida assessed the development process used by Versa Products Company, Inc. by an on-site audit and creation of a safety case against the requirements of IEC 61508.
- exida performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- exida reviewed field failure data to ensure that the FMEDA analysis was complete.
- exida reviewed the manufacturing quality system in use at Versa Products Company, Inc.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3 for mechanical components. A full IEC 61508 Safety Case was prepared, using the exida SafetyCaseDB™ tool, and used as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized as:

The Versa Products Company, Inc. V316, B316 and C316 Solenoid and Pilot Valve Series were found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable)

The V316, B316 and C316 Solenoid and Pilot Valve Series were found to meet the Random Capability requirements for a Type A device of SIL 2@HFT=0, SIL 3@HFT=1 for all models using Route 2ₕ.

The manufacturer will be entitled to use the following Functional Safety Logos
Table of Contents

Management Summary ........................................................................................................................................... 2
1 Purpose and Scope .............................................................................................................................................. 4
2 Project Management ........................................................................................................................................... 5
   2.1 exida ......................................................................................................................................................... 5
   2.2 Roles of the parties involved ...................................................................................................................... 5
   2.3 Standards and Literature used .................................................................................................................. 5
   2.4 Reference documents ............................................................................................................................... 5
      2.4.1 Documentation provided by Versa Products Company, Inc......................................................... 5
      2.4.2 Documentation generated by exida ................................................................................................. 6
3 Product Description ........................................................................................................................................... 7
   3.1 Versa V316 Series Solenoid and Pilot Valves ....................................................................................... 7
   3.2 Versa B316 Series Solenoid and Pilot Valves ....................................................................................... 7
   3.3 Versa C316 Series Solenoid and Pilot Valves ....................................................................................... 8
4 IEC 61508 Functional Safety Assessment ....................................................................................................... 9
   4.1 Methodology ............................................................................................................................................. 9
   4.2 Assessment level ....................................................................................................................................... 9
5 Results of the IEC 61508 Functional Safety Assessment ................................................................................. 10
   5.1 Lifecycle Activities and Fault Avoidance Measures .............................................................................. 10
      5.1.1 Functional Safety Management .................................................................................................. 10
      5.1.2 Safety Requirements Specification and Architecture Design .................................................. 11
      5.1.3 Hardware Design ......................................................................................................................... 11
      5.1.4 Validation ...................................................................................................................................... 11
      5.1.5 Verification ................................................................................................................................... 11
      5.1.6 Modifications ............................................................................................................................... 11
      5.1.7 User documentation ..................................................................................................................... 11
   5.2 Hardware Assessment ............................................................................................................................ 12
6 Terms and Definitions .................................................................................................................................... 13
7 Status of the Document .................................................................................................................................. 14
   7.1 Liability .................................................................................................................................................... 14
   7.2 Releases ................................................................................................................................................... 14
   7.3 Future Enhancements .............................................................................................................................. 14
   7.4 Release Signatures ................................................................................................................................. 14
1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Versa Products Company, Inc. V316, B316 and C316 Solenoid and Pilot Valve Series by exida according to the requirements of IEC 61508: ed2, 2010.

The results of this 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.
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 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 system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification and a collection of on-line safety and reliability resources. exida maintains the largest process equipment database of failure rates and failure modes with over 60 billion unit operating hours.

2.2 Roles of the parties involved

Versa Products Company, Inc. Manufacturer of the V316, B316 and C316 Solenoid and Pilot Valve Series

exida Performed the hardware assessment

exida Performed the IEC 61508 Functional Safety Assessment

Versa Products Company, Inc. contracted exida in January 2013 for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards and Literature used

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


2.4 Reference documents

2.4.1 Documentation provided by Versa Products Company, Inc.

<p>| [D2] | QP-1, Rev. M, 2/15/13 | Process Control Criteria |
| [D3] | QP-2, Rev. L, 2/15/13 | Quality Procedures and Document Control |
| [D5] | QP-4, Rev. Q, 2/27/13 | Gage and Instrument Control |
| [D7] | QP-6, Rev M, 12/7/12 | Processing of Nonconforming Material |
| [D8] | QP-7, Rev. L, 2/15/13 | Corrective Action |
| [D9] | QP-8, Rev. L, 6/17/12 | Preventive Action |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[D10]</strong></td>
<td>QP-9, Rev. N, 9/25/12</td>
<td>Inspection of Raw Material</td>
</tr>
<tr>
<td><strong>[D11]</strong></td>
<td>QP-10, Rev. N, 2/22/13</td>
<td>Receiving Department Work Instructions</td>
</tr>
<tr>
<td><strong>[D12]</strong></td>
<td>QP-11, Rev. I, 9/28/12</td>
<td>Assembly Test Procedure</td>
</tr>
<tr>
<td><strong>[D13]</strong></td>
<td>Eng- 1, Rev H, 5/13</td>
<td>Engineering Work Request form</td>
</tr>
<tr>
<td><strong>[D14]</strong></td>
<td>Eng. 68, Rev C, 9/09</td>
<td>EWR Impact Analysis Checklist and Design Plan form</td>
</tr>
<tr>
<td><strong>[D15]</strong></td>
<td>Eng. 10, Rev. B</td>
<td>Engineering Lab Test Request Form</td>
</tr>
<tr>
<td><strong>[D16]</strong></td>
<td>Eng. 13, 14, 15, 16, 17, 18, 29, 21, 22, 26, 27, 28, 29, 31</td>
<td>Engineering Laboratory Test Report Templates</td>
</tr>
<tr>
<td><strong>[D17]</strong></td>
<td>Eng- 66, Rev A, 6/26/03</td>
<td>Seal Compound Temperature Chart</td>
</tr>
<tr>
<td><strong>[D18]</strong></td>
<td>ENG-68__EWR-15316.pdf</td>
<td>EWR 15316 and Impact Analysis</td>
</tr>
<tr>
<td><strong>[D19]</strong></td>
<td>ENG-68__EWR-15337.pdf</td>
<td>EWR 15337 and Impact Analysis</td>
</tr>
<tr>
<td><strong>[D20]</strong></td>
<td>Eng- 75, Rev A, 10/09</td>
<td>Safety Manual – Control Valves</td>
</tr>
<tr>
<td><strong>[D21]</strong></td>
<td>Master_Control-Checkout-Checkin-guideline.pdf</td>
<td>Master Control guidelines (Documentation Control System)</td>
</tr>
<tr>
<td><strong>[D22]</strong></td>
<td>VPQP-11, Rev. H</td>
<td>Design Control Procedures</td>
</tr>
<tr>
<td><strong>[D24]</strong></td>
<td>Meeting Minutes, 2/19/13</td>
<td>2012 Management Review Meeting Minutes</td>
</tr>
<tr>
<td><strong>[D25]</strong></td>
<td>Solenoid Chart.xlsx</td>
<td>4 year Shipment History</td>
</tr>
<tr>
<td><strong>[D26]</strong></td>
<td>CC Summary.xls</td>
<td>4 year Customer Complaint History</td>
</tr>
<tr>
<td><strong>[D27]</strong></td>
<td>ENGNPD-1a, Rev B, 6/09</td>
<td>Versa New Product Development Map flowchart</td>
</tr>
</tbody>
</table>

### 2.4.2 Documentation generated by exida

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[R1]</strong></td>
<td>VER 12/12-023 R001 V1 R2, Jun 24, 2013</td>
<td>FMEDA report, V316 Solenoid and Pilot Valve Series</td>
</tr>
<tr>
<td><strong>[R2]</strong></td>
<td>VER 12/12-023 R002 V1 R2, Jun 24, 2013</td>
<td>FMEDA report, B316 Solenoid and Pilot Valve Series</td>
</tr>
<tr>
<td><strong>[R3]</strong></td>
<td>VER 12/12-023 R003 V1 R4, Jun 24, 2013</td>
<td>FMEDA report, C316 Solenoid and Pilot Valve Series</td>
</tr>
<tr>
<td><strong>[R5]</strong></td>
<td>Versa Valves SCDB.esc</td>
<td>IEC 61508 SafetyCaseDB for V316, B316 and C316 Solenoid and Pilot Valve Series</td>
</tr>
<tr>
<td><strong>[R6]</strong></td>
<td>PIU Versa Valves R1.xls, Jun 20, 2013</td>
<td>Proven In Use Analysis for V316, B316, and C316 Series Valves</td>
</tr>
<tr>
<td><strong>[R7]</strong></td>
<td>VER 12-12-023 R004 V1R1 IEC 61508 Assessment.doc, Jun 25, 2013</td>
<td>IEC 61508 Functional Safety Assessment, Versa Products Co., Inc. V316, B316 and C316 Solenoid and Pilot Valve Series (this report)</td>
</tr>
</tbody>
</table>
3 Product Description

Three series of Solenoid and Pilot Valves have been considered in this assessment. For all three series, only valves with 2 discrete valve positions have been considered. These solenoids are intended for use with clean, dry air or inert gas. All three series of valves are classified as Type A\(^1\) devices according to IEC 61508, having a hardware fault tolerance of 0.

Many variations of solenoid actuators are available for ordinary general use, hazardous areas, different levels of environmental protection, and various agency approvals. The standard Versa choices for Solenoid availability have been considered for this project and are listed in the respective FMEDA reports.

Refer to the FMEDA reports and/or the certificates for a list which versions and sizes of valves were analyzed in this project.

3.1 Versa V316 Series Solenoid and Pilot Valves

The V316 series of Valves are high flow, 3 or 5 port Solenoid/Pilot spool valves. These Valves can be used to pilot large actuators to provide quick closing of large valves. The solenoid valves are available in a variety of sizes and configurations to meet many application needs.

The configurations that are covered by this assessment consist of a 3-way or 4-way valve body, and an active or passive actuator assembly on each end. The valve body can have port sizes of \(\frac{1}{4}\)" NPT, \(\frac{3}{8}\)" NPT, or \(\frac{1}{2}\)" NPT. 3-way 1" NPT sizes were also included in this analysis. The active actuator(s) can be either a Solenoid-pilot (with or without a manual override) or a Pressure-pilot. The only passive actuator covered in this report is a spring return. Latching options on spring return units -3358 series and -181series were also considered for up to \(\frac{1}{2}\)" valve sizes. Refer to Section 4.1 of the FMEDA report for a more complete definition of how DTT (De-energize To Trip), ETT (Energize To Trip), N.C. (Normally Closed) and N.O. (Normally Open) are defined for the use of these valves in Safety Functions. Only valves with 2 discrete valve positions have been considered in this assessment. Also included are 3 and 4-way valves up to \(\frac{1}{2}\)" with redundant solenoids, options –RS and –SOV. Note that due to the high Safe failure rate of the –SOV option, those devices have not been grouped together with any other types in the version table or in the combined worst case results tables in the FMEDA.

Some valves may include a latching option (models with -3358 series or -181 series suffixes). These are valves where once tripped (or due to a loss of signal) shift and return to the normal (safe) position and latch. When the signal is restored, the valve remains in the tripped position until the valve is manually unlatched. Valves may also have a push button that may be used to provide a momentary manual override. Note: the SIF designer is responsible for determining if the latching function is suitable for the application and the end user is responsible for determining if it is safe to manually unlatch or override the valve position.

3.2 Versa B316 Series Solenoid and Pilot Valves

The B316 Series is a complete line of compact, rugged Three-Way (3/2), side-ported valves, constructed of 316 stainless steel (conforms to NACE standard MR-01-75). They are designed for use particularly in corrosive environments and to control a variety of aggressive media as well as

---

\(^1\) Type A element: “Non-Complex” element (using discrete components) for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010
air. O ring packed poppets provide bubbletight sealing throughout the operating pressure range 
and when used to operate small volume appliances this feature conserves valuable instrument air.

Actuations include solenoid/pilot (including those suitable for Ordinary, Hazardous or Low-Watt 
service), remote pressure pilot, manual, and mechanical. Many combination actuators and special 
function types can also be provided.

The configurations that are covered by this assessment consist of a 3-way valve body, and an 
active or passive actuator assembly on each end. The active actuator(s) can be either a Solenoid- 
pilot or a Pressure-pilot. The passive actuators covered in this assessment are spring return and 
mechanically actuated. Latching options on spring return units -159 series and -301 series were 
also considered. DTT (De-energize To Trip) and ETT (Energize To Trip) applications were 
considered. Some valves may also have an air pilot latch or are latching manual reset valves 
(models with -356*). These are valves where a loss of the electrical or pilot signal causes the valve 
to shift and return to the DTT (safe) position and latch. When the signal is restored, the valve 
remains in the DTT position until the valve is manually unlatched. Note: the SIF designer is 
responsible for determining if the latching function is suitable for the application and the end user is 
responsible for determining if it is safe to manually unlatch or override the valve position.

3.3 Versa C316 Series Solenoid and Pilot Valves

The Versa C-316 Series stainless steel body-ported valve is a high flow, 3 or 5-port, solenoid/pilot 
valve. The sealing design is that of Versa’s proven elastomer packed plunger producing bubble-
tight performance along with long trouble-free product life. This seal design also yields the highest 
flow available in the smallest package.

The C-316 Series utilizes stainless steel bodies, actuating caps and internal parts making this 
series of valves ideal for use in the most aggressive environments. Seals are FKM (fluorocarbon). 
Solenoid materials are a function of area classification rating.

The C-316 Series is available as either a 4-way, for double acting devices or a 3-way, for spring 
return devices. The 3-way function can be specified as either normally closed or opened. All 
solenoid actuators are solenoid/pilot type, which allows the use of the smallest solenoids available 
resulting in low power consumption. This design also assures a positive shifting force which makes 
certain the valve shifts when energized and reduces the chance of coil burnout.

Single solenoid spring return models utilize an air assisted spring return feature assuring a positive 
return. Double solenoid models are equipped with a detent that maintains the valve in the last 
shifted position, even in high vibration environments. A complete selection of electrical 
connections, power requirements and area classifications, makes Versa’s C-316 the valve of 
choice for demanding applications.

Latching manual reset valves (models with -356*) are valves where a loss of the electrical or pilot 
signal causes the valve to shift and return to the normally closed (safe) position and latches. When 
the signal is restored, the valve remains in the closed position until the valve is manually unlatched. 
Valves may also have a palm button that may be used to provide a momentary manual override. 
To manually override, the operator must first unlatch, then pull on the palm button. Once the palm 
button is released, the valve will automatically shift back and again latch to the normally closed 
position. Note: the SIF designer is responsible for determining if the latching function is suitable for 
the application and the end user is responsible for determining if it is safe to manually unlatch or 
override the valve position.
4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Versa Products Company, Inc. and is documented in the SafetyCase [R5].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the SafetyCase, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
  - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
  - Specification process, techniques and documentation
  - Design process, techniques and documentation, including tools used
  - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
  - Verification activities and documentation
  - Modification process and documentation
  - Installation, operation, and maintenance requirements, including user documentation
  - Manufacturing Quality System
- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA

The review of the development procedures is described in section 5. The review of the product design is described in section 5.2.

4.2 Assessment level

The V316, B316 and C316 Solenoid and Pilot Valve Series have been assessed per IEC 61508 to the following levels:

- Systematic Capability SC3 (SIL 3 capability) as the development procedures were assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.
- Architecture Constraint limitations of SIL 2 for a single device (using Route 2ₐ) and SIL 3 for a single device where the SFF for the complete final element is >90% (if using Route 1ₐ).
5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Versa Products Company, Inc. for this development against the objectives of IEC 61508 parts 1 and 2. The assessment was done on-site at the Paramus, N.J. facility and documented in the SafetyCase [R5].

5.1 Lifecycle Activities and Fault Avoidance Measures

Versa Products Company, Inc. has a defined product lifecycle process in place. This is documented in the Quality Manual [D1] and various Quality Procedures [D2-D12]. The same process is used for modifications. No software is part of the design and therefore any requirements specific from IEC 61508 to software and software development do not apply.

The assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for product design and development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The defined product lifecycle process was modified as a result of a previous audit which showed some areas for improvement. However, given the simple nature of the safety function and the extensive proven field experience for existing products Versa Products Company, Inc. was able to demonstrate that the objectives of the standard have been met. The result of the assessment can be summarized by the following observations:

The audited Versa Products Company, Inc. design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

Versa Products Company, Inc. has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. This is primarily documented in section 7.3 of their Quality Manual [D1]. Templates, forms and sample documents are provided. The same process is used for modifications. This process and procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well defined safety functionality.

Version Control

VPQP-11 requires that all documents be under document control. Master Control is used to check drawings in and out and to guarantee that only the current version of a drawing or document is used. Use of this to control revisions was evident during the audit.

Training, Competency recording

Human Resources maintain appropriate records of education, experience, training and qualifications for all personnel. Department managers are responsible for identifying and providing the training needs for their department and for maintaining records of in-process training. The procedures and records were examined and found up-to-date and sufficient. Versa Products Company, Inc. hired exida Consulting to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.
5.1.2 Safety Requirements Specification and Architecture Design

For the V316, B316, and C316 Series Valves, the simple primary functionality of the control valve is the same as the safety functionality of the product (Valve changes position, Close / Open). Therefore no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the Solenoid Valves designs are simple and are based upon standard designs with extensive field history, no semi-formal methods are needed. General Design and testing methodology is documented and required as part of the design process. This meets SIL 3.

5.1.3 Hardware Design

The design process is documented in Section 7.3 of [D1]. Items from IEC 61508-2, Table B.2 include observance of guidelines and standards, (PED, ATEX, NACE) project management, documentation (design outputs are documented per quality procedures), structured design, modularization, use of well-tried components / materials, and computer-aided design tools. This meets SIL 3.

5.1.4 Validation

Validation Testing is done via a documented plan created with the products specifications and includes compliance testing per application and agency standards. As the V316, B316, and C316 Series Valves are purely electro-mechanical devices with a simple safety function, there is no separate integration testing necessary. The Solenoid Valves perform only 1 Safety Function, which is extensively tested under various conditions during validation testing.

Items from IEC 61508-2, Table B.3 include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). Field experience and statistical testing via regression testing are not applicable. This meets SIL 3.

Items from IEC 61508-2, Table B.5 included functional testing and functional testing under environmental conditions, project management, documentation, failure analysis (analysis on products that failed), expanded functional testing, black-box testing, and fault insertion testing. This meets SIL 3.

5.1.5 Verification

The development and verification activities are defined in Section 7.3 of [D1]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.1.6 Modifications

Modifications are initiated with an Engineering Work Request [D13]. All changes are first reviewed and if approved, the work follows the normal design process. This meets SIL 3.

5.1.7 User documentation

Versa Products Company, Inc. creates the following user documentation: product catalogs and a Safety Manual. The Safety Manual was found to contain all of the required information given the simplicity of the products. The FMEDA reports are referenced, available and they contain required failure rates, failure modes, useful life, and suggested proof test information.
Items from IEC 61508-2, Table B.4 include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (V316, B316, and C316 Series Valves perform well-defined actions) and operation only by skilled operators (operators familiar with type of valve, although this is partly the responsibility of the end-user). This meets SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the V316, B316 and C316 Solenoid and Pilot Valve Series Failure Modes, Effects, and Diagnostic Analysis’s were performed by exida. This is documented in [R1].

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. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA, failure rates are derived for each important failure category. All failure rate analysis results and useful life limitations are listed in the FMEDA reports [R1] to [R3]. Tables in the FMEDA report list these failure rates for the V316, B316, and C316 Series Valves under a variety of configurations and applications. The failure rates listed are valid for the useful life of the devices. Based on general field failure data a useful life period of approximately 3 to 10 years is expected for the Solenoid Valves. This is listed in the FMEDA report. However, when plant experience indicates a shorter useful lifetime than indicated in the FMEDA report, the number based on plant experience should be used. All other assumptions are also listed in the reports.

For SIL 2 applications, single use, the PFD\text{AVG} value of the Safety Instrumented Function needs to be $\geq 10^{-3}$ and $< 10^{-2}$. The FMEDA reports list the percentage that some typical V316, B316, and C316 Series Valves use of this budget. The Valve will contribute less to the overall PFD\text{AVG} of the Safety Instrumented Function when Partial Valve Stroke Testing is automatically performed.

Note, if the Solenoid Valves is only one part of a final element, the SFF must be calculated for the entire final element combination if following the Route 1\text{H} hardware architectural constraints. It is the end users responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

The failure rate data used for this analysis meets the exida criteria for Route 2\text{H}. Therefore all of the reviewed V316, B316, and C316 Series Valves meet the Route 2\text{H} hardware architectural constraints for up to SIL 2 at HFT=0 when the listed failure rates are used, and SIL 3 applications with a HFT=1.

The analysis shows that the design of the V316, B316, and C316 Series Valves can meet the hardware requirements of IEC 61508, SIL 3 depending on the complete final element design. The Hardware Fault Tolerance, PFD\text{AVG}, and Safe Failure Fraction (when not following Route 2\text{H}) requirements of the IEC 61508 must be verified for each specific design.
6 Terms and Definitions

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

exida criteria: A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the $2_H$ Route in IEC 61508-2.

Fault tolerance: Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)

FIT: Failure In Time ($1 \times 10^{-9}$ 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.

PFD$_{AVG}$: Average Probability of Failure on Demand

PVST: Partial Valve Stroke Test

It is assumed that the Partial 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 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.

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
7 Status of the Document

7.1 Liability

exida prepares reports based on methods advocated in International standards. exida accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version: V1
Revision: R1

Version History:
V1, R1: Released, June 25, 2013
V0, R1: Draft; June 20, 2013

Authors: Gregory Sauk

Review:
V0, R1: Steven Close; June 21, 2013

Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Gregory Sauk, CFSE, Senior Safety Engineer

Dr. William M. Goble, Principal Partner