IEC 61508 Functional Safety Assessment - SIL 3

Project:

Ball Valve

Customer:

Emerson Process Management Virgo Valves SRL

Milano

Italy

Contract No.: Q15/08-044

Report No.: VIR 08-01-53 R003

Version V2, Revision R2, December 9, 2015

Steven Close

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.

Management summary

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

- Ball Valves

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

- exida did the original on-site audit of the design process at Emerson Process Management Virgo Valves SRL, Milan, Italy on May 29, 2008.
- exida performed a detailed FMEDA analysis of each product.
- exida reviewed field failure data to ensure that the FMEDA analysis was complete.
- exida reviewed the design process.
- exida reviewed the manufacturing quality system in use at Emerson Process Management Virgo Valves SRL, Milan, Italy.

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3 for mechanical components. An IEC 61508 Safety Case was prepared and used as the primary audit tool. Hardware process requirements and all associated test report documentation were reviewed.

Some areas of improvement were identified in the design process and the design procedures were upgraded during the project. However because of the low complexity of the products and the proven in use design, Emerson Process Management Virgo Valves SRL was able to demonstrate that the objectives of the standard have been met.

The results of the Functional safety Assessment can be summarized:

The listed products were found to meet the requirements of IEC 61508 for up to SIL 3 (SIL 3 Capable). The PFDavg and Safe Failure Fraction requirements of the standard must be verified for a complete final element design using these final element components.

The manufacturer will be entitled to use the Functional Safety Logo.

Table of Contents

Management summary 2

1 Purpose and Scope 5

1.1 Tools and Methods used for the assessment 5

2 Project management 6

2.1 *exida* 6

2.2 Roles of the parties involved 6

2.3 Standards / Literature used 6

2.4 Reference documents 6

2.4.1 Documentation provided by Emerson Process Management Virgo Valves SRL 6

2.5 Assessment Approach 7

2.5.1 Documentation generated by *exida* 8

3 Product Descriptions 9

4 IEC 61508 Functional Safety Assessment 10

4.1 Methodology 10

4.2 Assessment level 10

5 Results of the IEC 61508 Functional Safety Assessment 11

5.1 Open Issues 11

5.2 Lifecycle Activities and Fault Avoidance Measures 11

5.2.1 Functional Safety Management 11

5.2.2 Safety Requirements Specification and Architecture Design 14

5.2.3 Hardware Design 14

5.2.4 Validation 14

5.2.5 Verification 14

5.2.6 Modifications 14

5.2.7 User documentation 15

5.3 Hardware Assessment 16

6 2015 IEC 61508 Functional Safety Surveillance Audit 17

6.1 Roles of the parties involved 17

6.2 Surveillance Methodology 17

6.3 Surveillance Results 18

6.3.1 Procedure Changes 18

6.3.2 Engineering Changes 18

6.3.3 Impact Analysis 18

6.3.4 Field History 18

6.3.5 Safety Manual 18

6.3.6 FMEDA Update 18
7 Terms and Definitions 19
8 Status of the document 20
8.1 Liability 20
8.2 Releases 20
8.3 Release Signatures 20

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Emerson Process Management Virgo Valves SRL:

- Ball Valves

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

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.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Emerson Process Management Virgo Valves SRL.

All assessment steps were continuously documented by *exida* (see [R1] to [R4])

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 200 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 partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Emerson Process Management Virgo Valves SRL Manufacturer of ball valves

exida Performed the functional safety assessment and surveillance audit in November 2015.

Emerson Process Management Virgo Valves SRL contracted *exida* February 2008 for Certification of several products.

2.3 Standards / Literature used

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

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Emerson Process Management Virgo Valves SRL

[D1]	PO-04, Rev 7, 12 Dec, 2014	Engineering Operating Procedure
[D2]	PO-01, Rev 4, 19 Apr, 2013	PED Valve Directive
[D3]	PO-02, Rev 0, 04 Feb, 2008	Atex Valve Directive
[D4]	QSP-01, Rev 5, 31 Jan, 2013	Control of Documents, data and records
[D5]	PO-21, Rev 5, 31 Jan, 2013	Training of Personnel
[D6]	PO-03, Ed 2, Rev 1, 27 Feb, 2015	Sales Process
[D7]	PO-06, Ed 1, Rev 10, 23 Apr, 2015	Purchasing
[D8]	PO-07, Ed 2, Rev 1, 12 Jan, 2015	Inspection of the Product
[D9]	PO-08, Rev 2, 13 Mar, 2007	Warehouse (Kitting)

[D10]	PO-23, Rev 2, 15 Oct, 2007	Company Processes
[D11]	PO-23 WI-01, Rev 1, 03 Nov, 2010	Work Instructions for Manufacturing Valves
[D12]	SP010, Rev 4, 11/23/2015	Engineering Change Notice
[D13]	PO-12, Rev 3, 13, Sep, 2013	Complaint Process
[D14]	QEMSM Manual E2r3, March 21, 2007	Quality Manual
[D15]	ITP – 17 Dec, 2014	Inspection Test Plan – Sample
[D16]	E20 – Rev 4 MDS ASTM A350 LF2	Material Data Sheet - Sample
[D17]	VPJ-0023: Form	Valve Specification Sheet - Form
[D18]	VEU SM 001, Rev 2, 11/16/2015	Safety Manual (Ball)
[D19]	IAT-xxxx…, Rev 0, 11/23/2015	Impact Analysis Instruction / Form

NOTE: Items in Gray were updated during the recent assessment.

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed upon by Emerson Process Management Virgo Valves SRL.

The following IEC 61508 objectives were subject to detailed auditing at Emerson Process Management Virgo Valves SRL:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
- Hardware-related operation, installation and maintenance requirements

2.5.1 Documentation generated by *exida*

[R1]	IEC 61508 Gap Checklist – Virgo Europe, internal document, July 9, 2008	IEC 61508 Gap Analysis Report SIL 3
[R2]	VIR 08-01-53 R001 V2 R1, August 26, 2015	FMEDA Report, Ball Valve
[R3]	VIR 08-01-53 R002 V1 R1, July 11, 2009	SafetyCase Report, internal document
[R4]	VIR 08-01-53 R003 V2 R2 Assessment Europe Ball Valves, December 9, 2015	IEC 61508 Functional Safety Assessment SIL 3 Report (this report)

3 Product Descriptions

The Ball Valve is a ¼ turn ball valve used to control process fluids. Emerson Process Management Virgo Valves SRL manufactures ball valves from 2” to 72” in size with pressure ratings up to ANSI 2500 or API 15000. Product variations include; Soft Seated, Metal Seated - bolted side entry, welded side entry, bolted top entry, underground, and subsea. The Ball Valve is designed to meet international standards including API 6D, API 6A and API 608 for design/construction including pressure and temperature ratings, shell thickness, and bore diameters. The Ball Valve provides ISO 5211 mounting for simple actuator mounting. The Ball Valve includes double body-gasket sealing and multiple stem seals.

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Emerson Process Management Virgo Valves SRL and is documented in this report.

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software development (if applicable) 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 full Safety Case report, 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 an FMEDA

4.2 Assessment level

The products listed is Section 3 have been assessed per IEC 61508 to the following levels:

- SIL 3 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Emerson Process Management Virgo Valves SRL for this development against the objectives of IEC 61508 parts 1 and 2. The assessment was done on-site at the Milan, Italy facility on May 29, 2008.

5.1 Open Issues

The overall process is strong and is SIL 3 capable. Some areas of improvement were identified in the design process and the design procedures were upgraded during the project. However because of the low complexity of the products and the proven in use design, Emerson Process Management Virgo Valves SRL was able to demonstrate that the objectives of the standard have been met.

5.2 Lifecycle Activities and Fault Avoidance Measures

Emerson Process Management Virgo Valves SRL has a defined product lifecycle process described by PO-23 [D10]. 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 due 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 the original 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 Emerson Process Management Virgo Valves SRL 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 Emerson Process Management Virgo Valves SRL design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.2.1 Functional Safety Management

FSM Planning

Emerson Process Management Virgo Valves SRL has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. This is documented primarily of PO-23 [D10]. Templates and sample documents were reviewed and found to be sufficient. 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

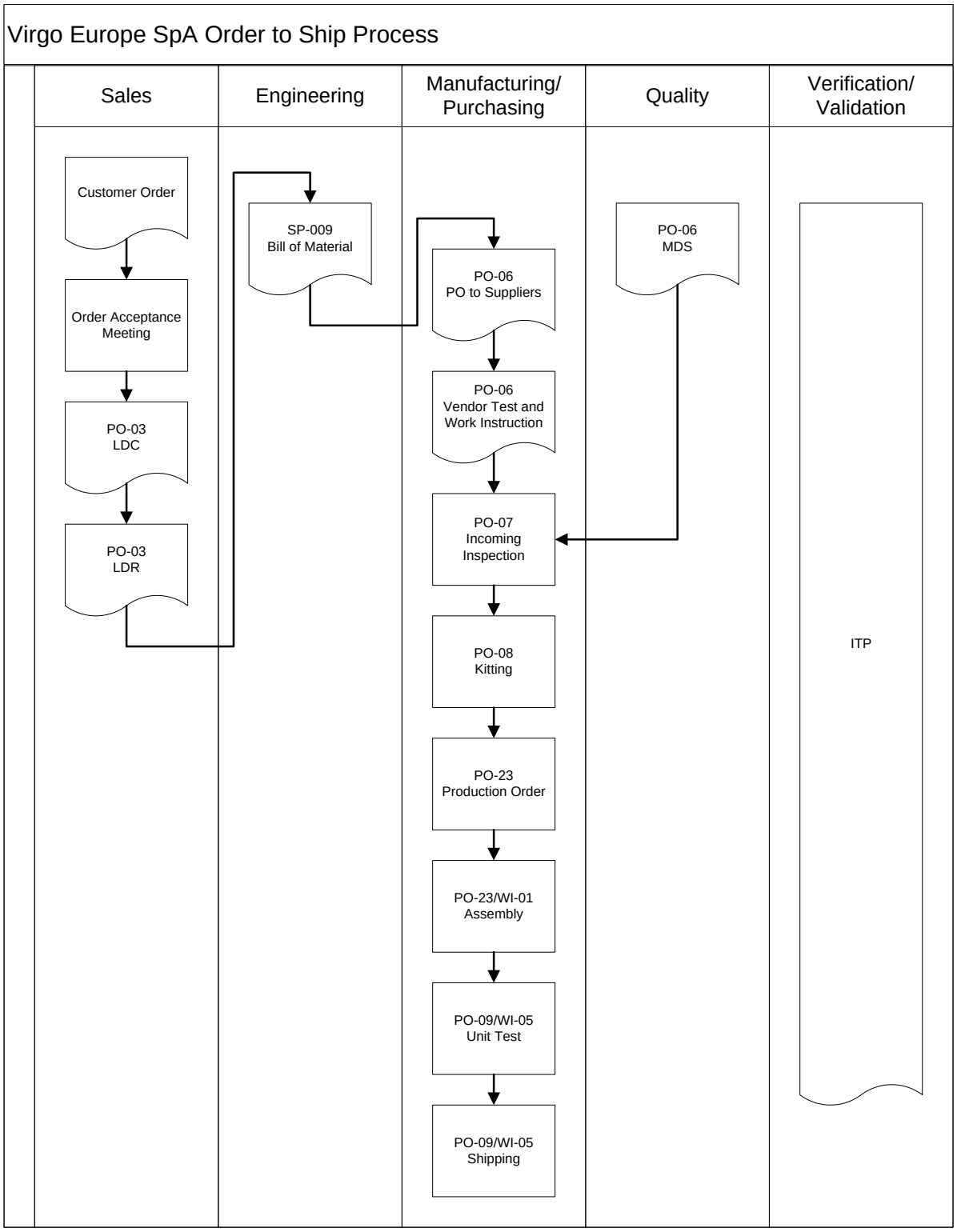
QSP-01 [D4] requires that all documents be archived under document control. Document revisions were evident during the audit.

Training, Competency recording

Personnel training records are kept per standard quality procedures as documented in PO-21 [D5]. A competency evaluation for critical jobs including IEC 61508 design and testing is required. Emerson Process Management Virgo Valves SRL hired exida Consulting to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

The valves manufactured at this facility are very large and are not built for inventory. These valves are built-to-order. The basic design in standardized, but each order can have variations. Due to the specialized nature of each valve, documentation that defines any unique requirements is generated for every order. Figure 1 shows the graphical representation of the Order-to-Ship procedures.

Figure 1: Emerson Process Management Virgo Valves SRL Order to Ship Process



5.2.2 Safety Requirements Specification and Architecture Design

For the existing products, the simple safety functionality is the primary functionality of the product (Close / Open Valve). Therefore no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the actuator and valve 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 referenced in PO-04 [D1], PO-01 [D2], PO-02 [D3], and ITP [D17]. This meets SIL 3.

5.2.3 Hardware Design

The design process is documented in PO-04 [D1] and PO-23 [D10]. Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards (PED, ATEX), project management, documentation (design outputs are documented per PO-23 [D10]), structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 3.

5.2.4 Validation

Validation Testing is documented in ITP [D15] and includes testing per all standard and customer performance requirements. As the products are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The products 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.

5.2.5 Verification

The development and verification activities are defined in ITP [D17]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.2.6 Modifications

Modifications are initiated per PO-04 [D1]. When approved, the normal design process is used. The Engineering Change Notice [D12] triggers an impact analysis which is documented on [D19].

This meets SIL 3.

5.2.7 User documentation

Emerson Process Management Virgo Valves SRL has created a Safety Manual which was inspected during the assessment. It contained all required information given the simplicity of the products. The FMEDA reports are available and they contain failure rate, failure mode, 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 (the products 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.

5.3 Hardware Assessment

To evaluate the hardware design of the products, Failure Modes, Effects, and Diagnostic Analysis's were performed by exida. This is documented in [R2].

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.

The analysis shows that design of the products can meet the hardware requirements of IEC 61508, SIL 3 depending on the complete final element design. The PFDavg and Safe Failure Fraction requirements of the IEC 61508 must be verified for each specific design.

6 2015 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Emerson Process Management Virgo Valves SRL	Manufacturer of ball valves
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Emerson Process Management Virgo Valves SRL contracted *exida* in August 2015 to perform the surveillance audit for the above Ball Valves. The surveillance audit was conducted remotely.

6.2 Surveillance Methodology

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

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if an of the changes could affect the safety function of the Ball Valves.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.3 Surveillance Results

6.3.1 Procedure Changes

The Operating Procedures and Forms highlighted in Section 2.4.1 were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

Engineering changes during the past 3 years were reviewed and were found to be conducted in accordance to the previously assessed engineering change procedure.

6.3.3 Impact Analysis

Since the exida certificate for the Ball Valves expired in August 2011 impact analyses for Functional Safety were not performed on the changes to the Ball Valve Designs. The revised Engineering Change Notice form SP-10 [D12] includes a requirement to perform a functional safety impact analysis on SIL certified products. The impact analysis is documented on the Impact Analysis Form [D19].

6.3.4 Field History

Shipping and field return information from 2009 to 2015 was reviewed as part of the surveillance audit. A Proven-in-Use evaluation was carried out on the Emerson Process Management Virgo Valves SRL Ball Valves. Shipment records were used to determine that the Ball Valves have >30 million hours in use and they have demonstrated a field failure rate less than the failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 3.

6.3.5 Safety Manual

The latest version of the safety manual [D18] was reviewed and was found to include the requirements of IEC 61508 for a safety manual.

6.3.6 FMEDA Update

The FMEDA for the Ball Valves was updated per the 2010 Version of IEC 61508. The update was documented in the FMEDA report [R2].

7 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
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).
SRS	Safety Requirements Specification

8 Status of the document

8.1 Liability

exida accepts no liability whatsoever for the use of this report.

8.2 Releases

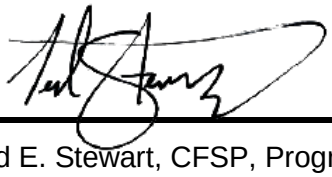
Version History: V2, R2: Revised company name, product description, December 8, 2015
V2, R1: Revised per surveillance audit, Q15/08-044, S. Close November 30, 2013
V1, R2: Update, July 25, 2008: product description update.
V1, R1: Released, July 11, 2008: edits and corrections.
V0, R1: Draft; July 9, 2008

Author: Steven Close
Review: V0, R1: William Goble
Review: V2, R1: Ted Stewart
Release status: Released

Future Enhancements
At request of client.

8.3 Release Signatures

Steven Close, Senior Safety Engineer



Ted E. Stewart, CFSP, Program Development & Compliance Manager