IEC 61508 Functional Safety Assessment

Project:

Tri Lok Triple Offset Butterfly Valves

Customer:

Bray International, Inc.

Houston, Texas

USA

Contract Number: Q07/12-19

Report No.: BRA 07-12-19 R010

Version V2, Revision R1, April 22, 2013

Steven Close

Management summary

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

- Bray Tri Lok Triple Offset Butterfly Valves

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

- *exida* assessed the development process used by Bray International, 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 Bray International, Inc. .

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3 for mechanical components. A full IEC 61508 Safety Case was prepared, using the *exida* SafetyCase 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 Bray International, Inc. Tri Lok Triple Offset Butterfly Valves were found to meet the requirements of IEC 61508 for up to SIL 3 (SIL 3 Capable). The PFD_{AVG} 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

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Bray International, Inc. Tri Lok Triple Offset Butterfly Valves 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 a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Bray International, Inc.	Manufacturer of the Tri Lok Triple Offset Butterfly Valves
exida	Performed the hardware assessment.
exida	Performed the IEC 61508 Functional Safety Assessment and surveillance audit.

Bray International, Inc. contracted *exida* in July 2009 for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

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

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

2.4 Reference documents

2.4.1 Documentation provided by Bray International, Inc.

[D1]	QM, Rev 9; 5/9/2012	Bray Quality System Manual
[D2]	BOP-04-01, Rev 2; 5/8/2010	Design Control
[D3]	BOP-04-02, rev 1; 3/1/2013	Design and Development
[D4]	BOP-04-06; Rev 1; 3/1/2013	Preparation, Control and Issue of Engineering Projects
[D5]	BOP-04-07; Rev 5; 3/1/2013	Preparation, Issue And Control Of Engineering Revision Notices
[D6]	BOP-04-08,rev 1; 3/1/2013	Impact Analysis
[D7]	BOP-08-02, rev 2; 12/30/2011	Traceability Of Products

[D8]	BOP-11-01, rev 2; 2/2/2012	Identification And Registration Of Measuring Equipment
[D9]	BOP-11-02, rev 2; 12/30/2011	Frequency Of Measuring And Test Equipment
[D10]	BOP-11-03, rev 2; 12/30/2011	Out Of Calibration Evaluation
[D11]	BOP-11-04; rev 8; 1/5/2012	Recording Of Calibration Results
[D12]	BOP-13-01; rev 7; 1/9/2012	Identification And Reviewing Of Non-Conforming Products
[D13]	BOP-13-02; rev 5; 8/23/2012	Preparation, Issue And Control Of Product Non - Conformance Reports
[D14]	BOP-13-03; rev 4; 7/26/2010	Handling, Registration Of Return Shipments
[D15]	BOP-13-04; rev 4; 8/23/2012	Registration And Control Of Customer Complaints
[D16]	BOP-14-01, Rev 1, Jan 1997	Preparation Issue And Implementation Of Corrective Action On Nonconformances
[D17]	BOP-14-03; rev 2; 3/5/2012	Preventive Action
[D18]	BOP-18-01, rev 2; 6/6/2012	Training Procedure Technical CV; Training plans & records of individuals
[D19]	BOP-02-01; rev. 1; 12/19/2011	Quality Procedure: Control And Issue Of The Quality Assurance Manual
[D20]	BOP-05-02; rev. 1; 12/19/2011	Quality Procedure: Document And Data Control
[D21]	BOP-01-01; Rev 1; 11/21/2011	Quality Procedure: Management Review
[D22]	BOP-02-02; rev. 1; 11/23/2011	Quality Procedure: Preparation, Control, Issue And Use Of Operating Procedures
[D23]	BOP-02-03; rev. 1; 11/23/2011	Quality Procedure: Preparation, Control, Issue And Use Of Work Instructions
[D24]	BOP-05-01, Rev 0, Aug 1995	Control Of Standards Specifications And Codes
[D25]	BOP-05-04, Rev 0, Feb 1997	Control And Issue Of The Sales And Engineering Manual
[D26]	BOP-06-01; rev 5; 12/28/2011	Preparation And Control Of Approved Suppliers List
[D27]	BOP-11-02, rev 2; 12/30/2011	Frequency Of Measuring And Test Equipment
[D28]	BOP-11-03, rev 2; 12/30/2011	Out Of Calibration Evaluation
[D29]	BOP-11-04; rev 7; 6/13/2002	Recording Of Calibration Results
[D30]	BOP-17-01; rev 3; 6/20/2012	Internal Quality Audits
[D31]	FRM0402A	Design and Development Plan
[D32]	FRM 1801B, Feb 1996	Training Record Form
[D33]	FRM 1801A, Apr 2004	Blank Training From
[D34]	WI-10-01, Rev 2, Aug, 2010	Sample Approval Process
[D35]	Test Standards, Jan 2004	Bray List Of Applicable Test Standards

[D36]	Inspection Report, Oct 2009	Sample Inspection Report
[D37]	Bray NCR, Jan 2010	Ncr Screen Shot
[D38]	13 August 2009	Lloyd's Register Certificate Of Conformity
[D39]	14 May, 2010	Lloyd's Assessment Report
[D40]	June 2010	Stem Retention Verification Report
[D41]	June 2010	Wall Thickness Verification Report
[D42]	Various 2010 Dates	Production Test Reports
[D43]	March 2010	Fire Report Test 3", Class 150
[D44]	79665, Jan 20, 2010	Ta-Luft Test Report
[D45]	Feb, 1020	API 598 Seal Test Report
[D46]	R1,	Safety Manual
[D47]	R1	Safety Requirements Specification

2.4.2 Documentation generated by *exida*

[R1]	BRA 07-12-19-R002, V2R1, April 3, 2013	FMEDA report, Bray Tri Lok Triple Offset Butterfly Valves
[R2]	BRA 07/12-19 R001, V1R1, Oct 29, 2009	IEC 61508 Process Gap Analysis Report, Bray International, Inc.
[R3]	Bray_ SafetyCaseDB IEC 61508R2.esc, April 2013	IEC 61508 SafetyCaseDB for Tri Lok Triple Offset Butterfly Valves
[R4]	BRA 07-12-19 R010 V2R1 TriLok IEC 61508 Assessment.doc, April 22, 2013	IEC 61508 Functional Safety Assessment, Bray International, Inc. Tri Lok Triple Offset Butterfly Valves (this report)

3 Product Descriptions

The Tri Lok is a high performance quarter-turn triple offset butterfly valve used to control process fluids. It is offered in a standard version, and in a fire-safe version. The standard version is available in sizes from 3" through 60" in ASME pressure classes 150 and 300.

The valve is inherently firesafe, and is certified to API 607, fifth edition and ISO 10497 in all materials listed in ASME B16.34, as well as in non-ferrous nickel-aluminum bronze.

Tri Lok is offered in wafer, lug body, double-flange, and gate face-to-face configuration. It is designed in accordance with ASME standard B16.34, which meets international standards for pressure and temperature ratings, shell thickness, and bore diameters.

Installation details conform to the international flange standards ASME B16.5 and B16.47, ISO 7005, JIS B2238, and others. Tri Lok is provided with actuator/operator mounting details which conform to ISO 5211 standard.

The main components of the Tri Lok triple offset butterfly valve are the body, disc, stem, and seat. The assembly includes the disc seal, disc seal retainer, stem journals, stem packing set, packing gland, stem anti-blowout clips, and bottom body plug. The assembly is complemented with necessary gaskets, and fastener hardware.

The design is similar between the various body offerings and valve series. All of these valves are classified as Type A[1] devices according to IEC 61508, having a hardware fault tolerance of 0.

This report is applicable to the valves series listed in Table 1.

Table 1 Bray Tri Lok Triple Offset Butterfly Valves Descriptions

Valve Series	Description
Series F0	150# Double Flanged Butterfly Valve
Series F1	300# Double Flanged Butterfly Valve
Series L0	150# Lug Series Butterfly Valve
Series L1	300# Lug Series Butterfly Valve
Series G0	150# Gate Series Butterfly Valve
Series G1	300# Gate Series Butterfly Valve
Series W0	150# Wafer Series Butterfly Valve
Series W1	300# Wafer Series Butterfly Valve

[1] Type A device: "Non-Complex" subsystem (using discrete elements) for details see 7.4.3.1.2 of IEC 61508-2

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Bray International, Inc. and is documented in this report.

A surveillance audit was conducted in April of 2013. This report was revised to reflect the results of the surveillance audit. In Summary the surveillance audit did not reveal any non-conformances.

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 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 a FMEDA

The review of the development procedures is described in section 5. The review of the product design is described in section 5.3.

4.2 Assessment level

The Tri Lok Triple Offset Butterfly Valves 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 Bray International, Inc. for these products against the objectives of IEC 61508 parts 1 and 2. The assessment was done on-site at the Bray International, Inc. facility on October 27, 2009 and documented in the SafetyCase [R3].

5.1 Open Issues

The overall process is strong and the designs have extensive proven field experience, sufficient for SIL 3 capability. Some areas of improvement were identified in the design process and some of the design procedures and forms were upgraded during the project. All of the improvements were evaluated and included in the final version of the SafetyCase.

5.2 Lifecycle Activities and Fault Avoidance Measures

Bray International, Inc. has a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D2] and various Quality Procedures [D2-D28]. A documented modification process is also covered in the Quality Manual and BOP-05-02. 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 the 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 Bray International, 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 Bray International, Inc. design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.2.1 Functional Safety Management

FSM Planning

Bray International, 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 of their Quality System Manual [D2] and in greater detail in procedures BOP-01-01 to BOP-14-01. Templates and sample documents were reviewed and found to be sufficient. The modification process is covered by BOP-04-07. This process and the procedures referenced therein 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

BOP-05-02 specifies what documents must be under document control and lists the applicable BOP procedures to be followed. Use of this to control revisions was evident during the audit.

Training, Competency recording

BOP-18-01 requires that each department retain on file training records and / or training attendance lists. Filing shall be done as described in BOP-16-01. It is the responsibility of the department managers to establish the training needs of individuals and a training record for individuals who perform activities that could affect quality within their department. The procedures and forms were examined and found up-to-date and sufficient. A sample of a training attendance record was placed in evidence in the SafetyCase.

Bray International, Inc. hired *exida* Consulting to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

5.2.2 Safety Requirements Specification and Architecture Design

A Safety Requirements Specification (SRS) for the Bray International Tri Lok Triple Offset Butterfly Valves, was submitted as evidence in the SafetyCase. The SRS must be formatted and controlled per BOP-05-02 prior to certification renewal. As the Bray Tri Lok Triple Offset Butterfly 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.

5.2.3 Hardware Design

The design process is documented in Section 7.1 through 7.3 of [D2]. Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards, (EU Directives, API, EN29001) 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.

5.2.4 Validation

As the Bray International Tri Lok Triple Offset Butterfly Valves are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The Bray Tri Lok Triple Offset Butterfly Valves perform only 1 Safety Function, which is extensively tested under various conditions during validation testing. Validation testing is conducted on 100% of production for both pressure and torque.

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 Section 7.3 of [D2]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.2.6 Proven In Use

A Proven in Use evaluation was not carried out on the Bray International, Inc. Bray Tri Lok Triple Offset Butterfly Valves during the initial assessment. Since the valve was a relatively new design and there was not enough field operating hours to satisfy the criteria of >100 million operating hours that must be demonstrated for a Proven in Use analysis to be valid.

The shipping and field return information for the Tri Lok Butterfly Valves was analyzed during the surveillance audit. The hours in use are approximately 20 million and the actual field failure rate was determined to be in line with the FMEDA results.

5.2.7 Modifications

Modifications are initiated per BOP-04-07 [D5] Preparation, Issue and Control of Engineering Revision Notices. Engineering Revision Notices are controlled through an engineering data base. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process. This meets SIL 3.

5.2.8 User documentation

Bray International, 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 Safety Manual references the FMEDA reports which are available and contain the 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 (Bray International Tri Lok Triple Offset Butterfly 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.

5.3 Hardware Assessment

To evaluate the hardware design of the Tri Lok Triple Offset Butterfly Valves a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida*. This is documented in [R1].

An 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 report [R1]. Tables in the FMEDA report list these failure rates for the Bray Tri Lok Triple Offset Butterfly Valves under a variety of applications. The failure rates listed are valid for the useful life of the devices.

Note, as the Bray International Tri Lok Triple Offset Butterfly Valves are only one part of a (sub)system, the SFF should be calculated for the entire final element combination.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The architectural constraints requirements of IEC 61508-2, also need to be evaluated for each final element application. 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 analysis shows that the design of the Bray International Tri Lok Triple Offset Butterfly Valves can meet the hardware requirements of IEC 61508, SIL 3. The Hardware Fault Tolerance, PFD_{AVG}, and Safe Failure Fraction requirements of IEC 61508 must be verified for each specific design.

6 Terms and Definitions

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
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.
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:	V2	
Revision:	R1	
Version History:	V2, R1:	Surveillance audit update, S. Close, April 3, 2013
	V1, R1:	Released to Bray, November 9, 2010
	V0, R1:	Draft; July 13, 2010
Authors:	Steven Close	
Review:	V2, R1:	William Goble, exida, April 19, 2013
	V1, R1:	William Goble
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Steven F. Close, Safety Engineer

Dr. William M. Goble, Principal Partner