IEC 61508 Functional Safety Assessment

Project:
Series 92/93 Rack & Pinion Actuators

Customer:
Bray International, Inc.
Houston, Texas
USA

Contract Number: Q07/12-19
Report No.: BRA 07-12-19 R006
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 Series 92/93 Rack & Pinion Actuators

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

- **exida** Certification 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. Series 92/93 Rack & Pinion Actuators 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

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 / Literature used ....................................................................................... 5
   2.4 Reference documents ................................................................................................. 5
      2.4.1 Documentation provided by Bray International, Inc. .................................................. 5
      2.4.2 Documentation generated by exida ........................................................................ 7

3 Product Descriptions ..................................................................................................... 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 Open Issues ................................................................................................................ 10
   5.2 Lifecycle Activities and Fault Avoidance Measures .................................................. 10
      5.2.1 Functional Safety Management ............................................................................ 10
      5.2.2 Safety Requirements Specification and Architecture Design ............................... 11
      5.2.3 Hardware Design ................................................................................................. 11
      5.2.4 Validation ............................................................................................................ 11
      5.2.5 Verification .......................................................................................................... 11
      5.2.6 Proven In Use ...................................................................................................... 12
      5.2.7 Modifications ....................................................................................................... 12
      5.2.8 User documentation ............................................................................................. 12
   5.3 Hardware Assessment ............................................................................................... 12

6 Terms and Definitions .................................................................................................... 14

7 Status of the Document ................................................................................................ 14
   7.1 Liability ..................................................................................................................... 15
   7.2 Releases ..................................................................................................................... 15
   7.3 Future Enhancements ............................................................................................... 15
   7.4 Release Signatures ................................................................................................... 15
1 Purpose and Scope


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 Series 92/93 Rack & Pinion Actuators
exida Performed the hardware assessment.
exida Performed the IEC 61508 Functional Safety Assessment and Surveillance audit.


2.3 Standards / 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 Bray International, Inc.

<p>| [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 |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Reference</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D8]</td>
<td>BOP-11-01, rev 2; 2/2/2012</td>
<td>Identification And Registration Of Measuring Equipment</td>
<td></td>
</tr>
<tr>
<td>[D9]</td>
<td>BOP-11-02, rev 2; 12/30/2011</td>
<td>Frequency Of Measuring And Test Equipment</td>
<td></td>
</tr>
<tr>
<td>[D11]</td>
<td>BOP-11-04; rev 8; 1/5/2012</td>
<td>Recording Of Calibration Results</td>
<td></td>
</tr>
<tr>
<td>[D12]</td>
<td>BOP-13-01; rev 7; 1/9/2012</td>
<td>Identification And Reviewing Of Non-Conforming Products</td>
<td></td>
</tr>
<tr>
<td>[D13]</td>
<td>BOP-13-02; rev 5; 8/23/2012</td>
<td>Preparation, Issue And Control Of Product Non-Conformance Reports</td>
<td></td>
</tr>
<tr>
<td>[D14]</td>
<td>BOP-13-03; rev 4; 7/26/2010</td>
<td>Handling, Registration Of Return Shipments</td>
<td></td>
</tr>
<tr>
<td>[D15]</td>
<td>BOP-13-04; rev 4; 8/23/2012</td>
<td>Registration And Control Of Customer Complaints</td>
<td></td>
</tr>
<tr>
<td>[D16]</td>
<td>BOP-14-01, Rev 1, Jan 1997</td>
<td>Preparation Issue And Implementation Of Corrective Action On Nonconformances</td>
<td></td>
</tr>
<tr>
<td>[D17]</td>
<td>BOP-14-03; rev 2; 3/5/2012</td>
<td>Preventive Action</td>
<td></td>
</tr>
<tr>
<td>[D18]</td>
<td>BOP-18-01, rev 2; 6/6/2012</td>
<td>Training Procedure Technical CV; Training plans &amp; records of individuals</td>
<td></td>
</tr>
<tr>
<td>[D20]</td>
<td>BOP-05-02; rev. 1; 12/19/2011</td>
<td>Quality Procedure: Document And Data Control</td>
<td></td>
</tr>
<tr>
<td>[D22]</td>
<td>BOP-02-02; rev. 1; 11/23/2011</td>
<td>Quality Procedure: Preparation, Control, Issue And Use Of Operating Procedures</td>
<td></td>
</tr>
<tr>
<td>[D23]</td>
<td>BOP-02-03; rev. 1; 11/23/2011</td>
<td>Quality Procedure: Preparation, Control, Issue And Use Of Work Instructions</td>
<td></td>
</tr>
<tr>
<td>[D24]</td>
<td>BOP-05-01, Rev 0, Aug 1995</td>
<td>Control Of Standards Specifications And Codes</td>
<td></td>
</tr>
<tr>
<td>[D26]</td>
<td>BOP-06-01; rev 5; 12/28/2011</td>
<td>Preparation And Control Of Approved Suppliers List</td>
<td></td>
</tr>
<tr>
<td>[D27]</td>
<td>BOP-11-02, rev 2; 12/30/2011</td>
<td>Frequency Of Measuring And Test Equipment</td>
<td></td>
</tr>
<tr>
<td>[D29]</td>
<td>BOP-11-04; rev 7; 6/13/2002</td>
<td>Recording Of Calibration Results</td>
<td></td>
</tr>
<tr>
<td>[D30]</td>
<td>BOP-17-01; rev 3; 6/20/2012</td>
<td>Internal Quality Audits</td>
<td></td>
</tr>
<tr>
<td>[D31]</td>
<td>FRM0402A</td>
<td>Design and Development Plan</td>
<td></td>
</tr>
<tr>
<td>[D32]</td>
<td>WI-10-01, Rev 2, Jul 2008</td>
<td>Sample Approval Process</td>
<td></td>
</tr>
<tr>
<td>[D33]</td>
<td>SRS, Feb 2007</td>
<td>Safety Requirements Specification 92/93 Actuators</td>
<td></td>
</tr>
<tr>
<td>[D34]</td>
<td>Test Standards, Jan 2004</td>
<td>Bray List Of Applicable Test Standards</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D37]</td>
<td>Bray NCR, Jan 2010</td>
<td>NCR Screen Shot</td>
<td></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>BRA 07-12-19-R001, V2R1, April 3, 2013</td>
</tr>
</tbody>
</table>
3 Product Descriptions

Bray pneumatic actuators are rack and pinion, opposed piston actuators available in two versions: double acting and spring return. Series 92/93 actuators feature two independently adjustable travel stop screws and a cam on the output shaft to permit precise bidirectional adjustments movement in both the open and closed positions for quarter turn valves. Either spring return or double acting configurations may be used in functional safety applications. All of these actuators are classified as Type A\(^1\) devices according to IEC 61508, having a hardware fault tolerance of 0.

The Series 92/93 Actuators are available in two basic versions:

<table>
<thead>
<tr>
<th>Version 1</th>
<th>Series 93 – Spring Return</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 2</td>
<td>Series 92 – Double Acting</td>
</tr>
</tbody>
</table>

Each version is available in a variety of sizes to accommodate a wide range of torque requirements.

\(^1\) 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 Series 92/93 Rack & Pinion Actuators 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. The Safety Requirements Specification and Safety Manual for the Series 92/93 Actuators are not in a final Bray format. This will be required for recertification.

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. 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 Series 92/93 Actuators, 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 Series 92/93 Rack & Pinion Actuators 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 Series 92/93 Actuators are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The Bray Series 92/93 Rack & Pinion Actuators 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 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

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the Bray International, Inc. Bray Series 92/93 Rack & Pinion Actuators during the surveillance activities in April 2013. Shipment records were used to determine that the actuators have >600 million operating hours 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.

5.2.7 Modifications

Modifications are initiated per BOP-04-07 [D4] 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 Series 92/93 Actuators 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 Series 92/93 Rack & Pinion Actuators 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 International Series 92/93 Actuators under a variety of applications. The failure rates listed are valid for the useful life of the devices.

Note, as the Bray International Series 92/93 Actuators are only one part of an element, 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, Table 2 also need to be evaluated for each final element application. It is the end user's 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 Series 92/93 Actuators 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)
FMEFA             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 2013
- V1,R2: Revised Report Number to R006
- V1, R1: Released to Bray International, Inc.
- V0, R1: Draft; March 25, 2010

Authors: Steven Close

Review:
- V2, R1: William Goble, exida, April 19, 2013
- V0, R1: William Goble

Release status: Release to Bray

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Steven F. Close, Safety Engineer

Dr. William M. Goble, Principal Partner