Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Shear-Safe Hydraulic Actuator.

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

- *exida* assessed the development process used by KOP Surface Products Singapore Pte Ltd through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team. *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

- *exida* reviewed the manufacturing quality system in use at KOP Surface Products Singapore Pte Ltd.

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* Safety Case tool 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 audited development process as tailored and implemented by the KOP Surface Products Singapore Pte Ltd Shear-Safe Hydraulic Actuator development project, complies with the relevant safety management requirements of IEC 61508 SIL3, SC 3 (SIL 3 Capable).

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Shear-Safe Hydraulic Actuator can be used in a low demand safety related system in a manor where the PFD\(_{avg}\) is within the allowed range for up to SIL2 (HFT = 0) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Shear-Safe Hydraulic Actuator meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

**This means that the Shear-Safe Hydraulic Actuator is capable for use in SIL3 applications in Low DEMAND mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.**

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 and literature used ............................................................................... 6
   2.4 Reference documents ........................................................................................... 6
       2.4.1 Documentation provided by KOP Surface Products Singapore Pte Ltd ...... 6
       2.4.2 Documentation provided by Deep Blue Engineering ................................... 9
       2.4.3 Documentation generated by exida............................................................... 11
   2.5 Assessment Approach ......................................................................................... 11

3 Product Descriptions ............................................................................................... 12
   3.1 Hardware Version Numbers ................................................................................. 12

4 IEC 61508 Functional Safety Assessment Scheme ................................................. 13
   4.1 Methodology ......................................................................................................... 13
   4.2 Assessment level ................................................................................................... 13

5 Results of the IEC 61508 Functional Safety Assessment ...................................... 14
   5.1 Lifecycle Activities and Fault Avoidance Measures ............................................. 14
       5.1.1 Functional Safety Management .................................................................... 14
       5.1.2 Safety Requirements Specification and Architecture Design ....................... 15
       5.1.3 Hardware Design ............................................................................................ 15
       5.1.4 Validation ........................................................................................................ 15
       5.1.5 Verification ....................................................................................................... 16
       5.1.6 Proven In Use .................................................................................................. 16
       5.1.7 Modifications ................................................................................................... 16
       5.1.8 User documentation ....................................................................................... 16
   5.2 Hardware Assessment ........................................................................................... 17

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

7 Status of the Document ........................................................................................... 19
   7.1 Liability .................................................................................................................. 19
   7.2 Releases .................................................................................................................. 19
   7.3 Future Enhancements ............................................................................................ 19
   7.4 Release Signatures .............................................................................................. 19
1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the KOP Surface Products Singapore Pte Ltd Shear-Safe Hydraulic Actuator 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 KOP Surface Products Singapore Pte Ltd.

All assessment steps were continuously documented by exida (see [R1] to [R3]).
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

KOP Surface Products Singapore Pte Ltd  
Manufacturer of the Shear-Safe Hydraulic Actuator

Deep Blue Engineering  
Created design concept and initial design

exida  
Performed the hardware assessment

exida  
Performed the IEC 61508 Functional Safety Assessment

KOP Surface Products Singapore Pte Ltd contracted exida in September 2014 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 KOP Surface Products Singapore Pte Ltd

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Safety Case Doc ID</th>
<th>Generic Document Name</th>
<th>Project Document Name and Link</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>D001</td>
<td>Quality Manual</td>
<td>PDC1000048267500004 QUALITY MANUAL - INDONESIA.pdf</td>
<td>Rev 4</td>
<td>22-Sep-14</td>
</tr>
<tr>
<td>D2</td>
<td>D003</td>
<td>Overall Development Process</td>
<td>PDC1000067466700005 ENGINEERING DESIGN.pdf</td>
<td>Rev 5</td>
<td>28-Jan-15</td>
</tr>
<tr>
<td>D3</td>
<td>D004</td>
<td>Configuration Management Process</td>
<td>D004 Configuration Management</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>D4</td>
<td>D004b</td>
<td>Configuration</td>
<td>D004 Configuration</td>
<td>Rev 14</td>
<td>N/A</td>
</tr>
<tr>
<td>Doc ID</td>
<td>Safety Case Doc ID</td>
<td>Generic Document Name</td>
<td>Project Document Name and Link</td>
<td>Version</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>----------------------</td>
<td>--------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management Process - BOM report example</td>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D5]</td>
<td>D005</td>
<td>Field Failure Reporting Procedure</td>
<td>D005 FIELD FAILURE REPORTING PROCEDURE.pdf</td>
<td>Rev 5</td>
<td>29-Apr-14</td>
</tr>
<tr>
<td>[D7]</td>
<td>D007</td>
<td>Manufacturer Qualification Procedure</td>
<td>PDC100002394300004 SUPPLIER APPROVAL PROCEDURE.pdf</td>
<td>Rev 4</td>
<td>4-Jan-12</td>
</tr>
<tr>
<td>[D9]</td>
<td>D007c</td>
<td>Manufacturer Qualification Procedure - qualified supplier list</td>
<td>Manual QSL Update.pdf</td>
<td>N/A</td>
<td>16-Feb-15</td>
</tr>
<tr>
<td>[D16]</td>
<td>D019</td>
<td>Customer Notification Procedure</td>
<td>PDC10002643992 ENGINEERING, SERVICE, HSE BULLETIN CREATION.pdf</td>
<td>Rev 0</td>
<td>12-Dec-14</td>
</tr>
<tr>
<td>Doc ID</td>
<td>Safety Case Doc ID</td>
<td>Generic Document Name</td>
<td>Project Document Name and Link</td>
<td>Version</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>------------------------</td>
<td>--------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>[D18]</td>
<td>D023b</td>
<td>Impact Analysis Template</td>
<td>CRITICALITY RATING</td>
<td>Rev 2</td>
<td>30-Oct-14</td>
</tr>
<tr>
<td>[D19]</td>
<td>D026</td>
<td>FSM Plan or Development Plan</td>
<td>TQP CHECKLIST</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D20]</td>
<td>D032</td>
<td>Job Descriptions and Competency Levels</td>
<td>D032 JOB DESCRIPTIONS AND COMPETENCY LEVELS</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D21]</td>
<td>D033</td>
<td>Training Record</td>
<td>D033 TRAINING RECORD</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D22]</td>
<td>D034</td>
<td>Skills Matrix</td>
<td>Copy of Engineering Dept.pdf</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D24]</td>
<td>D038</td>
<td>List of Design Tools</td>
<td>SolidWorks</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D25]</td>
<td>D040</td>
<td>Safety Requirements Specification</td>
<td>D040 D041 D053</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D26]</td>
<td>D041</td>
<td>Safety Requirements Review</td>
<td>Design Review MOM.pdf</td>
<td>N/A</td>
<td>9-Jan-15</td>
</tr>
<tr>
<td>[D28]</td>
<td>D055</td>
<td>FMEDA Report</td>
<td>KOP 14-06-060 R001 V1R1 FMEDA AM05.pdf</td>
<td>V1R1</td>
<td>16-Dec-14</td>
</tr>
<tr>
<td>[D30]</td>
<td>D069b</td>
<td>Validation Test Plan - PR2 - 5 inch</td>
<td>10002387233.pdf</td>
<td>Rev 0</td>
<td>21-May-14</td>
</tr>
<tr>
<td>[D31]</td>
<td>D069c</td>
<td>Validation Test Plan - FAT</td>
<td>FAT Test</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>[D32]</td>
<td>D070</td>
<td>Validation Test Plan Review Record</td>
<td>FAT Test</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>[D33]</td>
<td>D071</td>
<td>Environmental Test Plan - 3 inch</td>
<td>SP-1-DOC-021 PR2 Qualification Test Procedure 3 1,16-10K Actuator-Rev 4.pdf</td>
<td>Rev 4</td>
<td>10-Jan-11</td>
</tr>
<tr>
<td>[D34]</td>
<td>D071b</td>
<td>Environmental Test Plan - 5 inch</td>
<td>10002387233.pdf</td>
<td>Rev 0</td>
<td>21-May-14</td>
</tr>
</tbody>
</table>
### 2.4.2 Documentation provided by Deep Blue Engineering

<table>
<thead>
<tr>
<th>Doc ID</th>
<th>Safety Case Doc ID</th>
<th>Generic Document Name</th>
<th>Project Document Name and Link</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D44]</td>
<td>D001</td>
<td>Quality Manual</td>
<td>Quality_Manual_1e.pdf</td>
<td>1e</td>
<td>Feb-15</td>
</tr>
<tr>
<td>[D45]</td>
<td>D003</td>
<td>Overall Development Process</td>
<td>SHEAR SAFE DEVELOPMENT PROCESS.pdf</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>[D47]</td>
<td>D026</td>
<td>FSM Plan or Development Plan</td>
<td>SHEAR SAFE DEVELOPMENT PROCESS.pdf</td>
<td>01</td>
<td>N/A</td>
</tr>
<tr>
<td>[D48]</td>
<td>D026b</td>
<td>FSM Plan or Development Plan 1</td>
<td>Shear Safe Actuator project time line Presentation.pptx</td>
<td>N/A</td>
<td>11/29/2014</td>
</tr>
<tr>
<td>[D49]</td>
<td>D026c</td>
<td>FSM Plan or Development Plan 1</td>
<td>Viking Shear Safe Actuator Development.pptx</td>
<td>N/A</td>
<td>3/25/2011</td>
</tr>
<tr>
<td>[D50]</td>
<td>D032</td>
<td>Job Descriptions and Competency Levels</td>
<td>Job Description and Competency Template. Project manager.doc</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D51]</td>
<td>D032b</td>
<td>Job Descriptions and Job Description and</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Doc ID</td>
<td>Safety Case Doc ID</td>
<td>Generic Document Name</td>
<td>Project Document Name and Link</td>
<td>Version</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>--------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>[D52]</td>
<td>D032c</td>
<td>Competency Levels</td>
<td>Competency Template.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D032c</td>
<td>Lead Engineer.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D53]</td>
<td>D034</td>
<td>Skills Matrix</td>
<td>Shear Safe Actuator</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D034</td>
<td>Development Project Skills</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Matrix.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D54]</td>
<td>D038</td>
<td>List of Design Tools</td>
<td>Pro-E, FEA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>D053</td>
<td>MoM March 2012 (2).doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D57]</td>
<td>D059</td>
<td>Fault Injection Test</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D059</td>
<td>Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D58]</td>
<td>D067</td>
<td>Integration Test Plan</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D59]</td>
<td>D068</td>
<td>Integration Test Plan</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D60]</td>
<td>D069</td>
<td>Validation Test Plan</td>
<td>Validation Test Procedure.pdf</td>
<td>0</td>
<td>5/21/2014</td>
</tr>
<tr>
<td>[D61]</td>
<td>D070</td>
<td>Validation Test Plan</td>
<td>Validation Test Procedure.pdf</td>
<td>0</td>
<td>5/21/2014</td>
</tr>
<tr>
<td>[D62]</td>
<td>D074</td>
<td>Validation Test Results</td>
<td>Pressure Test Report &amp; Certification.pdf</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D63]</td>
<td>D074b</td>
<td>Validation Test Failure Report Galling</td>
<td>Galling Failure Report.pdf</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D64]</td>
<td>D074c</td>
<td>Validation Test Failure Report 6 3/8</td>
<td>6.375 Actuator PR2 Test Failure Report - formatted 20082013 (1).pdf</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D65]</td>
<td>D074d</td>
<td>Validation Test Certificate</td>
<td>PR2 Test Qualification Certificate 353041-0001.pdf</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>[D66]</td>
<td>D077</td>
<td>Fault Injection Test</td>
<td>Validation Test Results</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D077</td>
<td>Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D67]</td>
<td>D081</td>
<td>Engineering Change</td>
<td>Background to the change of P40625.docx</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D081</td>
<td>Documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[D68]</td>
<td>D069</td>
<td>Validation Test Plan</td>
<td>Validation Test Procedure.pdf</td>
<td>0</td>
<td>5/21/2014</td>
</tr>
<tr>
<td>[D69]</td>
<td>D070</td>
<td>Validation Test Plan</td>
<td>Validation Test Procedure.pdf</td>
<td>0</td>
<td>5/21/2014</td>
</tr>
</tbody>
</table>
2.4.3 Documentation generated by \textit{exida}

<table>
<thead>
<tr>
<th></th>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1]</td>
<td>KOP 14-06-060 R001 V1R1 FMEDA AM05, December 16, 2014</td>
<td>FMEDA report, Shear-Safe Hydraulic Actuators</td>
</tr>
<tr>
<td>[R2]</td>
<td>KOP Q14-06-060 V1.1 KOP SafetyCase, June 8, 2015</td>
<td>IEC 61508 SafetyCase for Shear-Safe Hydraulic Actuator</td>
</tr>
</tbody>
</table>

2.5 Assessment Approach

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

The assessment was planned by \textit{exida} and agreed upon by KOP Surface Products Singapore Pte Ltd.

The following IEC 61508 objectives were subject to detailed auditing at KOP Surface Products Singapore Pte Ltd:

- 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 architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware-related operation, installation and maintenance requirements
3 Product Descriptions

Shear-Safe Hydraulic Actuator is a hydraulic piston/cylinder arrangement that drives the valve to the open position, via the stem, when hydraulic control pressure is supplied to the cylinder. A return spring drives the cylinder, stem and valve gate back to the closed position when hydraulic fluid is vented from the cylinder. Inside the Shear-Safe actuator, a mechanical transmission system applies a managed level of compression to the return spring during the extending/opening stroke, so that a controlled force is applied during the closing stroke, with higher force where it is needed.

The safety state of the Shear-Safe Hydraulic Actuator is to retract the stem of the actuator with the spring pack extended.

3.1 Hardware Version Numbers

This assessment is applicable to the following hardware versions of Shear-Safe Hydraulic Actuator:

<table>
<thead>
<tr>
<th>Smallest Size</th>
<th>Largest Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 1/16 inch</td>
<td>5 inch</td>
</tr>
</tbody>
</table>
4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by KOP Surface Products Singapore Pte Ltd for this development project against the objectives of the exida certification scheme which includes subsets of IEC 61508 -1 to 3. The results of the assessment are documented in [R2] and [R3].

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 5.2.

4.2 Assessment level

The Shear-Safe Hydraulic Actuator has 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 Deep Blue Engineering and KOP Surface Products Singapore Pte Ltd for these products against the objectives of IEC 61508 parts 1 - 7. The assessment for KOP Surface Products Singapore Pte Ltd was done on-site at the Singapore facility on March 9-10, 2015 and documented in the SafetyCase [R2]. The assessment for Deep Blue Engineering was done on-site at the Deep Blue Engineering facility on February 4 & 5, 2015 and is documented in SafetyCase [R3].

5.1 Lifecycle Activities and Fault Avoidance Measures

KOP Surface Products Singapore Pte Ltd has a defined product lifecycle process in place. This is documented in the Quality Manual [D1] and various Quality Procedures [D2-D18]. Every customer job goes through the complete design process. A documented modification process is also covered in the Engineering Change Management [D17]. 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 KOP Surface Products Singapore Pte Ltd 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 KOP Surface Products Singapore Pte Ltd design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

The actuators manufactured by KOP Surface Products Singapore Pte Ltd are not built for inventory. These actuators are built-to-order. The basic designs are standardized, but each order can have materials variations or specific customer requested proof tests. Due to the specialized nature of each actuator, documentation that defines all of the requirements is generated for every order as part of the process.

FSM Planning

KOP Surface Products Singapore Pte Ltd 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 5 of their Quality Manual [D1] and in greater detail in Engineering Design Procedure [D2]. Templates and sample documents were reviewed and found to be sufficient. The modification process is covered by Engineering Change Management [D17]. 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

Document Control and Document Management Procedure [D4] requires that all documents be under document control. Use of this to control revisions was evident during the audit.
Training, Competency recording
Section 3.2 of Quality Manual [D1] requires the Human Resource department to maintain training records of education, experience, training and qualifications for all personnel. Department heads are responsible for identifying and providing the training needs for their department as well as proficiency evaluations. The procedures and records were examined and found up-to-date and sufficient. KOP Surface Products Singapore Pte Ltd hired *exida* 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 Shear-Safe Hydraulic Actuator, the simple primary functionality of the actuator is the same as the safety functionality of the product (Actuator retracts the stem of the actuator with the spring pack extended). Therefore no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the Shear-Safe Hydraulic Actuator 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 hardware design of the Shear-Safe Hydraulic Actuator was performed by Deep Blue Engineering. The development team consisted of 3 primary members of Deep Blue Engineering and a coordinator from KOP Surface Products Singapore Pte Ltd. Deep Blue Engineering followed sound engineering practices in the design, verification and validation of the Shear-Safe Hydraulic Actuator. Design reviews were held with KOP Surface Products Singapore Pte Ltd at critical stages of the design [D56].

The design process is documented in Section 5.4 of [D2]. Items from IEC 61508-2, Table B.2 include observance of guidelines and standards such as API, 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 was conducted per API 6A PR2 by an independent test facility. Internal validation testing is documented on form [D31] which is created for each order. The test plan includes testing per all standard and customer performance requirements. As the Shear-Safe Hydraulic Actuator are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The Shear-Safe Hydraulic Actuator 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
Verification activities performed during the development of the Shear-Safe Hydraulic Actuator were carried out by Deep Blue Engineering. The records of the verification calculations were documented in a design file.

Continued development and verification activities are the responsibility of KOP Surface Products Singapore Pte Ltd and are defined in Section 5 of [D2]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.1.6 Proven In Use
Proven In Use is not applicable to KOP Surface Products Singapore Pte Ltd Shear-Safe Hydraulic Actuator.

5.1.7 Modifications
Modifications are initiated per Section 3.13 of [D2] Engineering Design procedure. 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.

The modification process has been successfully assessed and audited, so KOP Surface Products Singapore Pte Ltd may make modifications to this product as needed.

- As part of the exida scheme a surveillance audit is conducted every 3 years. The modification documentation listed below is submitted as part of the surveillance audit. exida will review the decisions made by the competent person in respect to the modifications made.
  - List of all anomalies reported
  - List of all modifications completed
  - Safety impact analysis which shall indicate with respect to the modification:
    - The initiating problem (e.g. results of root cause analysis)
    - The effect on the product / system
    - The elements/components that are subject to the modification
    - The extent of any re-testing
  - List of modified documentation
  - Regression test plans

This meets SIL 3.

5.1.8 User documentation
KOP Surface Products Singapore Pte Ltd creates the following user documentation: product catalogs, Operations And Maintenance Manual [D39] and a Safety Manual [D40]. 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 (Shear-Safe Hydraulic Actuator 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 Shear-Safe Hydraulic Actuator Failure Modes, Effects, and Diagnostic Analysis’s were performed by exida. These are 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 report [R1]. Tables in the FMEDA report list these failure rates for the Shear-Safe Hydraulic Actuator under a variety of applications. The failure rates listed are valid for the useful life of the actuators.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the exida criteria for Route 2_H. Therefore the Shear-Safe Hydraulic Actuator can be classified as a 2_H device. When 2_H data is used for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H.

If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

Note, as the Shear-Safe Hydraulic Actuator 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, Table 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 Shear-Safe Hydraulic Actuator can meet the hardware requirements of IEC 61508, SIL 3 and SIL 2 for the Shear-Safe Hydraulic Actuators depending on the complete final element design. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.
6 Terms and Definitions

Architectural Constraint The SIL limit imposed by the combination of SFF and HFT for Route 1H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2H

exida criteria A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2H 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 PFD_{avg} 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).

Systematic Capability The SIL limit imposed by the capability of the products manufacturer.

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, July 2, 2015  
V0, R1: Draft; June 4, 2015  
Authors: Jack Gao  
Review: V0, R1: Steven Close; June 8, 2015  
Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Steven Close, Senior Safety Engineer

Jack Gao, CFSE, Senior Safety Engineer

Loren Stewart, CFSP, Safety Engineer