IEC 61508 Functional Safety Assessment

Project:
MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves

Customer:
MAXON Corporation
Muncie, IN
USA

Contract No.: Q08/09-07
Report No.: MAX 08-09-07 R001 V1 R1 61508 Assessment
Version V1, Revision R1, February 17, 2009
Chris O'Brien

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:

- Series 8000 Air Actuated Valves
- Series MA11, MA12, MA21, and MA 22 Electric Actuated Valves
- Series MM11, MM12, MM21, and MM22 Manual Actuated Valves

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

- exida Certification assessed the development process used by MAXON Corporation by an on-site audit and review of the safety case created for the initial certification. The safety case provides detailed results showing how the product and processes meet the requirements of IEC 61508.

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

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3. A full IEC 61508 Safety Case was prepared, using the exida SafetyCaseDB™ tool, and used as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. The manufacturing quality system was reviewed. Environmental test reports were reviewed. Also the user documentation was reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves were found to meet the requirements of SIL 3.

The manufacturer will be entitled to use the Functional Safety Logo.
# Table of Contents

Management summary .................................................................................................................. 2  

1 Purpose and Scope .................................................................................................................... 4  
   2.1 exida .................................................................................................................................. 5  
   2.2 Roles of the parties involved ............................................................................................. 5  
   2.3 Standards / Literature used ............................................................................................... 5  
   2.4 Reference documents ......................................................................................................... 6  
      2.4.1 Documentation provided by MAXON Corporation ............................................. 6  
      2.4.2 Documentation generated by exida ................................................................... 8  

3 Product Description ................................................................................................................... 9  
   3.1 MAXON Series 8000 Air Actuated Valves ........................................................................ 9  
   3.2 MAXON Series MA11, MA12, MA21, and MA22 Electric Actuated Valves .................. 10  
   3.3 MAXON Series MM11, MM12, MM21, and MM22 Electric Actuated Valves ............... 11  

4 IEC 61508 Functional Safety Assessment ............................................................................. 12  
   4.1 Methodology ...................................................................................................................... 12  
   4.2 Assessment level ................................................................................................................. 12  

5 Results of the IEC 61508 Functional Safety Assessment .................................................... 13  
   5.1 Functional Safety Management ......................................................................................... 13  
   5.2 Safety Requirements Specification and Architecture Design ......................................... 13  
   5.3 Hardware Design .............................................................................................................. 14  
   5.4 Manufacturing .................................................................................................................. 14  
   5.5 Validation ......................................................................................................................... 14  
   5.6 Verification ....................................................................................................................... 14  
   5.7 Modifications .................................................................................................................... 15  
   5.8 User documentation ......................................................................................................... 15  
   5.9 Hardware Assessment ...................................................................................................... 15  

6 Certification Renewal Audit ................................................................................................... 17  

7 Terms and Definitions ............................................................................................................. 18  

8 Status of the document .......................................................................................................... 19  
   8.1 Liability ............................................................................................................................. 19  
   8.2 Releases ............................................................................................................................ 19  
   8.3 Future Enhancements ....................................................................................................... 19  
   8.4 Release Signatures ............................................................................................................ 19
1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

**Option 1: Hardware assessment according to IEC 61508**

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD\textsubscript{AVG}).

This option shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the development process.

**Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511**

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD\textsubscript{AVG}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software including the modification process. This option is useful in combination with end user failure records for doing a prior use justification.

**Option 3: Full assessment according to IEC 61508**

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

**This assessment shall be done according to option 3.**

This document shall describe the results of the IEC 61508 functional safety assessment of the MAXON Corporation MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves. The assessment has been carried out based on the quality procedures and scope definitions of *exida* Certification S.A.
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 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 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

MAXON Corporation manufacture of the MAXON 8000 Series Gas Valves and Gas Electro Mechanical Valves

exida

Provided services to support MAXON Corporation and performed the original functional safety assessment of the MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves.

exida Certification

Performed the IEC 61508 Functional Safety Assessment according to option 3 (see section 1) as an independent organization. The assessment was performed by Chris O’Brien, assessor, who was not involved in the execution of the audited activities.

MAXON Corporation contracted exida in December 2008 with 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.

### 2.4 Reference documents

#### 2.4.1 Documentation provided by MAXON Corporation

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D3] MAXON Category Certification, 2002</td>
<td>Test lab CSA certification certificate</td>
<td></td>
</tr>
<tr>
<td>[D5] ModelNo, 10/1/2005</td>
<td>Valve Model Number Description</td>
<td></td>
</tr>
<tr>
<td>[D10] OP-0057, Rev B; 6/19/2008</td>
<td>Development Plan</td>
<td></td>
</tr>
<tr>
<td>[D13] PR-6102</td>
<td>Test Plan for CSA 6.5-2000 2.7.3 - maximum input current at 110% voltage test</td>
<td></td>
</tr>
<tr>
<td>[D14] PR-6103</td>
<td>Test plan for CSA 6.5-2000 overvoltage</td>
<td></td>
</tr>
<tr>
<td>[D15] PR-6104</td>
<td>Test plan for CSA 6.5-2000 2.7.1 undervoltage</td>
<td></td>
</tr>
<tr>
<td>[D16] PR-6105</td>
<td>Test plan for CSA 6.5-2000 temperature test</td>
<td></td>
</tr>
<tr>
<td>[D17] PR-6107</td>
<td>Test plan for CSA 6.5-2000 2.4.1, external leakage</td>
<td></td>
</tr>
<tr>
<td>[D18] PR-6108</td>
<td>Test plan for CSA 6.5-2000 2.4.2 seat leakage</td>
<td></td>
</tr>
<tr>
<td>[D19] PR-6109, 2/10/2003</td>
<td>Valve Closure on Gas Pressure Surge Test plan and test report</td>
<td></td>
</tr>
<tr>
<td>[D20] PR-6112</td>
<td>Test plan for dielectric withstand voltage</td>
<td></td>
</tr>
<tr>
<td>[D21] PR-6114, 2/10/2003</td>
<td>Test plan and test report for UL-429 Paragraph 37 - hosedown test</td>
<td></td>
</tr>
<tr>
<td>[D22] PR-6115, 2/10/2003</td>
<td>Test plan and test report for CSA 6.5-2000 2.7.4 overvoltage test</td>
<td></td>
</tr>
<tr>
<td>[D23] PR-6116</td>
<td>Test plan for CSA 6.5-2000 4.4 closing time of the valve</td>
<td></td>
</tr>
<tr>
<td>[D24] PR-6120, 11/8/2002</td>
<td>Environmental Test Data, Test plan and test results</td>
<td></td>
</tr>
<tr>
<td>[D25] Calibration, Rev B; 5/9/2003</td>
<td>WI checking and calibrating pressure gauges, and other docs, including sample calibration results.</td>
<td></td>
</tr>
<tr>
<td>[D26] RFA R&amp;D 2000-2, 10/3/2000</td>
<td>Product Specifications within the Request For Authorization (RFA) document; Example RFA containing all specifications including safety requirements</td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[D27]</td>
<td>Rev 0; 10/24/2005</td>
<td>IEC 61508 addition to instructions (Safety Manual)</td>
</tr>
<tr>
<td>[D28]</td>
<td>SMTT Rev 4; 6/26/2001</td>
<td>SmarTeam testing, test review checklist of all tests done and versions of all tools used.</td>
</tr>
<tr>
<td>[D29]</td>
<td>SMTT SE, Rev 4; 6/20/2001</td>
<td>SmarTeam Solid Edge Integration</td>
</tr>
<tr>
<td>[D30]</td>
<td>Database print-out, 9/1/2005</td>
<td>Valve returns and customer complaint records</td>
</tr>
</tbody>
</table>
### 2.4.2 Documentation generated by exida

<table>
<thead>
<tr>
<th></th>
<th>MAX 08-09-07 R001 V1 R1 IEC 61508 Assessment, 2/17/2009</th>
<th>IEC 61508 Functional Safety Assessment, Flowserve MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves (this report)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R2]</td>
<td>MAX 08-09-07 R002 V1 R1 – Series 8000 FMEDA Report, 02/17/2009</td>
<td>FMEDA report MAXON Series 8000 Air Actuated Valves</td>
</tr>
<tr>
<td>[R3]</td>
<td>MAX 08-09-07 R003 V1 R1 – Series MA Electric Actuated FMEDA Report, 02/17/2009</td>
<td>FMEDA MAXON Series MA11, MA12, MA21, and MA22 Electric Actuated Valves</td>
</tr>
<tr>
<td>[R6]</td>
<td>MAX 04-11-10 R005 V1 R1 IEC 61508 Assessment.doc, 1/10/2006</td>
<td>IEC 61508 Assessment, MAXON Series 5000, Series 8000 and Series 808 Valves</td>
</tr>
</tbody>
</table>
3 Product Description

3.1 MAXON Series 8000 Air Actuated Valves

MAXON Series 8000 Air Actuated Valves are used as shut-off and vent valves, primarily in burner management systems. They are pneumatically operated gate valves, operated by a patented solenoid and quick exhaust assembly that controls the air supply. The solenoid and quick exhaust assembly utilizes an additional ball check valve which maximizes the fail-safe operation. The solenoid and quick exhaust assembly is directly wired into the control system.

Integrated SPDT (Single Pole/Double Throw) valve position switches are offered in. Standard packages include a Valve Close Switch, actuated at the end of the closing stroke and one Valve Open Switch, actuated at the end of the opening stroke. The valve close switch is classified as a “proof of closure switch with valve seal over travel” by third party approval agencies. These position switches are not included as part of the safety functionality of the valves and have not been included in the assessment.

The MAXON Series 8000 Air Actuated Valves are FM and CSA approved as safety shut-off valves for fuel gas service. Models are available for hazardous location service for Class 1 Divisions 1 & 2 and Zones 0 & 2. The actuator is rated for IP65 and NEMA 1, 3, 3S, 4 and NEMA 4X. The valves meet FCI 70-2 control valve standard for Class VI seat leakage.

Table 1 gives an overview of the different versions that were considered in the assessment of the Series 8000 Air Actuated Valves. The first option considers the situation where the valve needs to achieve fully closed position and its design shut-off criteria, i.e. meets the requirements of FCI 70-2 Class VI Seat Leakage. The second option considers the situation where the valve needs to achieve the fully-closed position to meet FCI Class III. This means that in the second situation, the application can tolerate minor leakage.

Table 1 Version overview Series 8000 Air Actuated Valves

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-D/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 8000 Air actuator, spring-return – Design Sealing performance</td>
</tr>
<tr>
<td>FC-F/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 8000 Air actuator, spring-return – Full stroke performance</td>
</tr>
<tr>
<td>FO-F/SR</td>
<td>Normally-Open Vent Valve configuration with Series 8000 Air actuator, spring-return</td>
</tr>
</tbody>
</table>

The MAXON Series 8000 Air Actuated Valves are classified as a Type A\(^1\) devices according to IEC 61508. The hardware fault tolerance of the devices is 0.

\(^1\) Type A component: “Non-Complex” component with well-defined failure modes, for details see 7.4.3.1.3 of IEC 61508-2.
3.2 MAXON Series MA11, MA12, MA21, and MA22 Electric Actuated Valves

The MAXON Series MA11, MA12, MA21, and MA22 Electric Actuated Valves are used as shut-off and vent valves, primarily in burner management systems. They are electric operated gate valves, operated by electric release snap action valves. The solenoid is directly wired into the control system. The solenoid holds with power on, permits trip on power loss. Spring return function functionality is designed into the valve function. The valve has an automatic electric motor reset.

Valve position switches are offered in SPDT (Single Pole/Double Throw). Standard packages include a Valve Close Switch, actuated at the end of the closing stroke and one Valve Open Switch, actuated at the end of the opening stroke. The valve close switch is classified as a “proof of closure switch with valve seal over travel” by third party approval agencies. The position switches are not included as part of the safety functionality of the valves and have not been included in the assessment.

The MAXON Series MA valves are FM and CSA approved as safety shut-off valves for fuel gas service. Models are available for hazardous location service for Class 1 Division 2. The actuator is rated for NEMA 1, 3, 3S, 4, 12 and NEMA 4X. The valves meet FCI 70-2 control valve standard for Class VI seat leakage.

Table 2 gives an overview of the different versions that were considered in the assessment of the Series MA11, MA12, MA21, and MA22 Electric Actuated Valves. The first option considers the situation where the valve needs to achieve fully closed position and its design shut-off criteria, i.e. meets the requirements of FCI 70-2 Class VI Seat Leakage. The second option considers the situation where the valve needs to achieve the fully-closed position to meet FCI Class III. This means that in the second situation, the application can tolerate minor leakage.

Table 2 Version overview Series MA11, MA12, MA21, and MA22 Electric Actuated Valves

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-D/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 5000 and 5000NI Electric actuator, spring-return – Design Sealing performance</td>
</tr>
<tr>
<td>FC-F/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 5000 and 5000NI Electric actuator, spring-return – Full stroke performance</td>
</tr>
<tr>
<td>FO-F/SR</td>
<td>Normally-Open Vent Valve configuration with Series STOA and STOA-NI Electric actuator, spring-return</td>
</tr>
</tbody>
</table>

The MAXON Series MA11, MA12, MA21, and MA22 Electric Actuated Valves are classified as a Type A devices according to IEC 61508. The hardware fault tolerance of the devices is 0.
3.3 MAXON Series MM11, MM12, MM21, and MM22 Electric Actuated Valves

MAXON Series MM11, MM12, MM21, and MM22 Electric Actuated Valves are used as shut-off and vent valves, primarily in burner management systems. They are electric operated gate valves, operated by electric release snap action valves. The solenoid valve is directly wired into the control system. The solenoid holds with power on, permits trip on power loss. Spring return function functionality is designed into the valve function. The valve has a manual reset.

Integrated SPDT (Single Pole/Double Throw) valve position switches are offered. Standard packages include a Valve Close Switch, actuated at the end of the closing stroke and one Valve Open Switch, actuated at the end of the opening stroke. The valve close switch is classified as a “proof of closure switch with valve seal over travel” by third party approval agencies. The position switches are not included as part of the safety functionality of the valves and have not been included in the assessment.

The MAXON Series MM Electric Actuated Valves are FM and CSA approved as safety shut-off valves for fuel gas service. Models are available for hazardous location service for Class 1 Divisions 2. The actuator is rated for NEMA 1, 3, 3S, 4, 12 and NEMA 4X. The valves meet FCI 70-2 control valve standard for Class VI seat leakage.

Table 3 gives an overview of the different versions that were considered in the assessment of the Series MM11, MM12, MM21, and MM22 Electric Actuated Valves. The first option considers the situation where the valve needs to achieve fully closed position and its design shut-off criteria, i.e. meets the requirements of FCI 70-2 Class VI Seat Leakage. The second option considers the situation where the valve needs to achieve the fully-closed position to meet FCI Class III. This means that in the second situation, the application can tolerate minor leakage.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-D/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 808 and 808NI Electric actuator, spring-return – Design Sealing performance</td>
</tr>
<tr>
<td>FC-F/SR</td>
<td>Normally-Close Shut-Off Valve configuration with Series 808 and 808NI Electric actuator, spring-return – Full stroke performance</td>
</tr>
<tr>
<td>FO-F/SR</td>
<td>Normally-Open Vent Valve configuration with Series STOM and STOM-NI Electric actuator, spring-return</td>
</tr>
</tbody>
</table>

The MAXON Series MM11, MM12, MM21, and MM22 Electric Actuated Valves are classified as a Type A devices according to IEC 61508. The hardware fault tolerance of the devices is 0.
4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from the MAXON Corporation and is documented in [R5].

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 SafetyCase report, e.g. software development requirements for a product with no software.

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

- Product design
  - Hardware architecture and failure behavior, documented in an FMEDA

- Manufacturing process
  - Manufacturing quality system

The review of the development procedures is described in sections 5.1 through 5.8. The review of the product design is described in section 5.9.

4.2 Assessment level

The MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves have been assessed per IEC 61508 to the following levels:

- SIL 3 capable

The development procedures will be 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 MAXON Corporation for this development against the objectives of IEC 61508 parts 1 and 2. The assessment was done on-site at Muncie, IN. Additionally a Safety Case was completed, see [R5].

This functional safety assessment has shown that the process sufficiently meets the requirements of IEC 61508, SIL 3. The assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the MAXON Corporation development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited MAXON Corporation development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1 Functional Safety Management

FSM Planning
MAXON Corporation has a staged-gate process in place for product development with specific deliverables and approvals at each gate. This is documented in OP-0057 [D10]. The same process is used for modifications. It is a purely mechanical design process; no electronics or software are part of the design and therefore any requirements specific from IEC 61508 to electronics or software due not apply.

Version Control
All design drawing and documents are under version control.

Training, Competency recording
Personnel training records are kept per OP-0043 [D7]. The procedure and records were examined and found up-to-date and sufficient. MAXON Corporation hired exida to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

5.2 Safety Requirements Specification and Architecture Design

Product specifications are developed per the RFA procedure. exida reviewed the content of the specification for completeness per requirement of IEC 61508. As the valves are simple mechanical devices, there is no need for a separate architecture design phase. The specification will indicate if the design is new or based on an existing design.

Items from IEC 61508-2, Table B.1 include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, and inspection of the specification. As the function of the valve is simple and clearly defined there is no need for semi-formal methods such as functional block diagrams. The application is considered when specifying the requirements; the valves are required to meet specific applications standards, such as CSA 6.5-2000. This meets SIL 3.
5.3 Hardware Design

The process includes a systematic design approach with intermediate reviews. MAXON Corporation has standards for documentation with specified output documents. Items from IEC 61508-2, Table B.2 include observance of guidelines and standards, project management, documentation (design outputs are documented per OP-0058 [D11]), structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 3.

5.4 Manufacturing

The MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves are manufactured in an ISO 9001-2000 certified facility. All units are functionally tested. Field returns are tracked and reviewed monthly to identify quality issues and performance issues. Customer feedback is solicited and reviewed to identify performance issues and opportunities for product improvements. This meets SIL 3.

5.5 Validation

As the valves are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The valve performs only 1 safety function, which is extensively tested under various conditions during validation testing. Validation tests are clearly traceable to requirements. Validation Testing is done via documented plans written per the product specification and compliance testing per the application standards, such as CSA 6.5-2000.

The OP-0060 [D12] procedure specifies the corrective actions to be taken when tests fail. Items from IEC 61508-2, Table B.3 include functional testing, project management, documentation, and black-box testing (for valves 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 under environmental conditions, project management, documentation, failure analysis (analysis on product returns), and expanded functional testing and black-box testing. Interference surge immunity testing is not applicable and fault insertion testing is not feasible for these valves. This meets SIL 3.

5.6 Verification

The development steps are defined in the Design and Development Flowchart, referenced in the Development Plan. The following verification steps are defined: product specification (requirements) review, prototyping, pilot run, and standards compliance testing. All verification activities are documented. This meets SIL 3.

MAXON specifies a set of integrated design tools. Version numbers are listed and re-qualification is done when the tool vendor makes revisions. Re-qualification test results are documented and reviewed. This meets SIL 3.
5.7 Modifications

Modifications are performed per the Design Changes Procedure, OP-0055 [D9]. In general design changes are treated as a derived product and therefore the same general procedure is used for both new development and modifications. All design change requests are reviewed to determine if there is any negative impact on product safety. This review is done by both the assigned engineer and the appropriate engineering manager. This meets SIL 3.

5.8 User documentation

MAXON Corporation creates the following user documentation: Installation Instructions [D1] and [D2], and IEC 61508 additions to instructions, [D27]. These were assessed by exida. The final version is considered to be in compliance with the requirements of IEC 61508. These documents include all required operations, maintenance, and proof test procedures.

Items from IEC 61508-2, Table B.4 include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (valve performs well-defined action) 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.

5.9 Hardware Assessment

To evaluate the hardware design of the MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves a Failure Modes, Effects, and Diagnostic Analysis was performed by exida. This is documented in [R2], [R3], and [R4]. 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.

From the FMEDA failure rates are derived for each important failure category. Table 4 lists these failure rates as reported in the FMEDA reports. The failure rates are valid for the useful life of the valves. Based on MAXON endurance test data and general field failure data a useful life period of approximately 10 to 15 years or longer is expected for the MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves. This is listed in the FMEDA reports.
### Table 4 Failure rates according to IEC 61508

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>$\lambda_{sd}$</th>
<th>$\lambda_{su}^2$</th>
<th>$\lambda_{dd}$</th>
<th>$\lambda_{du}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series 8000, FC-D/SR</td>
<td>0 FIT</td>
<td>1854 FIT</td>
<td>0 FIT</td>
<td>1399 FIT</td>
</tr>
<tr>
<td>Series 8000, FC-F/SR</td>
<td>0 FIT</td>
<td>2399 FIT</td>
<td>0 FIT</td>
<td>854 FIT</td>
</tr>
<tr>
<td>Series 8000, FO-F/SR</td>
<td>0 FIT</td>
<td>2467 FIT</td>
<td>0 FIT</td>
<td>786 FIT</td>
</tr>
<tr>
<td>Series MA, FC-D/SR</td>
<td>0 FIT</td>
<td>797 FIT</td>
<td>0 FIT</td>
<td>1170 FIT</td>
</tr>
<tr>
<td>Series MA, FC-F/SR</td>
<td>0 FIT</td>
<td>1342 FIT</td>
<td>0 FIT</td>
<td>625 FIT</td>
</tr>
<tr>
<td>Series MA, FO-F/SR</td>
<td>0 FIT</td>
<td>1410 FIT</td>
<td>0 FIT</td>
<td>557 FIT</td>
</tr>
<tr>
<td>Series MM, FC-D/SR</td>
<td>0 FIT</td>
<td>699 FIT</td>
<td>0 FIT</td>
<td>1137 FIT</td>
</tr>
<tr>
<td>Series MM, FC-F/SR</td>
<td>0 FIT</td>
<td>1244 FIT</td>
<td>0 FIT</td>
<td>592 FIT</td>
</tr>
<tr>
<td>Series MM, FO-F/SR</td>
<td>0 FIT</td>
<td>1312 FIT</td>
<td>0 FIT</td>
<td>524 FIT</td>
</tr>
</tbody>
</table>

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 $PFD_{AVG}$ and Safe Failure Fraction requirements of the IEC 61508 must be verified for each specific design.

---

2 Note that the SU category includes failures that do not cause a spurious trip
6 Certification Renewal Audit

In order to renew the certification of the MAXON 8000 Series Gas Valves and Gas Electro-Mechanical Valves a recertification audit was conducted. The audit was conducted December 9, 2009 onsite at the Muncie, IN facility. The focus of the audit was to verify that the functional safety management plan being utilized, verify that the product modifications were being properly executed, and to verify the actual field performance of the valves correlated with expected performance. Specific items reviewed include:

- Four (4) product changes were reviewed to verify that the FSM Plan was being utilized and that the appropriate steps were in place. All reviewed changes were acceptable.

- PROJ-5735 Part Number 46009: Reviewed rubber stop design and incorporated a positive stop into the solenoid mounting bracket. This resulted in a product improvement. Rubber stops had fallen out resulting in the valve not being able to be reset electrically. Changes followed the ECR process [OP-0055] and documentation was organized, searchable and complete. Reviewed changes were acceptable.

- New Valve Trim Project: This project could impact the safety function of the device. The project was handled under the new product development procedure and the project followed the stage gate process. Documentation was organized and available. The execution of the project was acceptable.

- Field Returns: Reviewed field returns with the Service and Quality Departments. There is a well structured and thorough process. Returns receive an incoming inspection and those that may be quality related under go a thorough product evaluation.

The results of the audit and inspection are acceptable and indicate that the Functional Safety Management Plan is in place and effective. This meets SIL 3.
7 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 frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD_{AVG}  Average Probability of Failure on Demand
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 (sub)system  “Non-Complex” (sub)system (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B (sub)system  “Complex” (sub)system (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
8 Status of the document

8.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. exida accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

8.2 Releases

Version: V1
Revision: R1
Version History: V1, R1: Released; February 17, 2009
V0, R1: Draft; January 2, 2009
Authors: Chris O'Brien
Review: V0, R1 Rachel Amkreutz; January 5, 2009
Release status: Released

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Rachel Amkreutz

Chris O'Brien, Director of Business Development