FUNCTIONAL SAFETY ASSESSMENT REPORT

FOR THE

LIFECYCLE AND MANAGEMENT OF FUNCTIONAL SAFETY

Author: ..... **Paul Reeve** BEng CEng MIET MInstMC
Functional Safety Consultant
Sira Associate

Report checked: ..... **Hassan El-Sayed** BSc (Hons) MSc PhD Ceng FInstMC
Functional Safety Consultant
Sira Test & Certification

Date of issue: 5th of October 2012

Customer: Rotork Fluid Systems
(A Division of Rotork UK Ltd)

Report Number: R56A28091B V1.0 (abbreviated)

CONTENTS

REVISION HISTORY

Rev	Date	Comment
0.1	20-Aug-12	Initial draft based on document review and audit
0.2	25-Sep-12	Revised after assessment of corrective actions following audit
1.0	5-Oct-12	Report technical checked

This report is an abbreviated version of Sira report number R56A28091B (44 pages) aimed at a more open readership. Refer to the full version for a detailed clause by clause assessment against the standard.

This report should be read in conjunction with the Sira product assessment reports listed in section 1.2.

FUNCTIONAL SAFETY ASSESSMENT REPORT

1 INTRODUCTION

1.1 References

Carried out by:	Sira Test & Certification, Rake Lane, Eccleston, Chester, CH4 9JN
Sites audited:	Rotork Fluid Systems Regina House Ring Road Bramley Leeds LS13 4ET UK
Associated Products:	Skilmatic Intelligent Electro-hydraulic Quarter-turn Valve Actuators. Models including; SI-1Q, SI-2Q & SI-2.1Q
Date of Request for Assessment:	July 2012
Assessment standards:	IEC 61508-1:2010, clause 6 (management of functional safety) IEC 61508-2:2010, clause 7 (E/E/PE lifecycle)

1.2 Scope of this report

This assessment report covers the functional safety management (FSM) and the Electrical/Electronic/Programmable Electronic (E/E/PE) lifecycle that support a number of products manufactured by Rotork Fluid Systems against the requirements of IEC 61508 Parts 1 and 2 respectively. Conformity to these parts of the Standard are required to avoid the introduction of systematic failure modes and fully determine the suitability of the products for use in SIL-rated safety functions.

This report is produced as a common document to supplement failure rate assessments (e.g., based on Failure Mode, Effect and Diagnostic Analyses [FMEDA]) which have been performed or verified by Sira for each product.

Prior to the site audit, the process documentation was reviewed by Sira. Issues raised during this review were addressed during the audit visit. Some non-conformities were raised during the audit which were subsequently addressed by Rotork, re-assessed by Sira and incorporated in this report.

Refer to the full version of this report (with appendices) for a clause by clause assessment within the scope of this report.

The models that this report supports are listed in the following table.

Product	Description	Sira Assessment Report
SI-1Q	Intelligent Electro-hydraulic Quarter-turn Valve Actuator	R56A28091A
SI-2.1Q	Intelligent Electro-hydraulic Quarter-turn Valve Actuator	R56A28091A

Details of the qualitative assessments covering the lifecycle and the management of functional safety associated with the products are included in the Appendices of this report which use the CASS templates and methodology (www.cass.uk.net) as a framework to assess these requirements from IEC 61508.

The element safety function is implemented using simple electro-mechanical means and hence the SI-1Q and SI-2.1Q Intelligent Electro-hydraulic Quarter-turn Valve Actuators qualify as Type A Devices as defined by IEC 61508-2, clause 7.4.4.1.2. (The more complex functionality in the units is not part of and cannot interfere with the element safety function).

The devices associated with this assessment are all mature products which have been in the manufacturing phase for over ten years. Furthermore, the potential for systematic failure modes which might have been introduced back in the early stages of the design lifecycle that have not been identified to date is considered by Sira to be negligible. The relevant E/E/PE lifecycle and FSM system assessment therefore apply to relevant ongoing activities (such as manufacturing, design modifications, collection and analysis of field failure data, etc).

This report is only intended to support certification of the products listed above. The report is not a comprehensive assessment of Rotork Fluid Systems generic FSM capability that would be required to support a company FSM certificate.

1.3 Some common terms and abbreviations

E/E/PES	Electrical/Electronic/Programmable-Electronic safety-related Systems
PLC	Programmable Logic Controller
SIL	Safety Integrity Level
UKAS	United Kingdom Accreditation Service
PFD	Probability of failure on demand
SIS	Safety Instrumented System
FSM	Functional safety management
SIF	Safety instrumented function
HFT	Hardware fault tolerance
SFF	Safety failure fraction
FMEA	Failure modes and effects analysis
MTTR	Mean time to repair

1.4 Overall description of the equipment

The products are electromechanical valve actuators for use in process control applications in hazardous areas. They feature a fail-safe design and are available with different options in terms of return spring speed, control interface, supply voltage, mounting, size, torque, etc. The element safety function and a more detailed description of the product is contained in the associated Sira product assessment report (refer to the table in section 1.2 above).

1.5 Sites visited / audited

The following Rotork Fluid Systems site was audited:

FSM and E/E/PE lifecycle audit, 16-Aug-12:	Rotork Fluid Systems Regina House Ring Road Bramley Leeds LS13 4ET UK
Rotork Fluid Systems representatives:	Sam Ferguson, Design Engineer Adam Russell, Quality Engineer Simon Rodgers, R&D Manager
Sira representatives:	Paul Reeve, Functional Safety Assessor

Documentation defining the FSM and lifecycle (i.e., the design procedures referred to in the Quality Manual) that addressed each of the CASS TOEs was requested for review prior to the audit of their implementation.

The following agenda was used for the audit:

1. Introductions (SIRA and Rotork Fluid Systems)
2. Opening Meeting to define the scope of the audit
3. Audit of the Management of Functional Safety (using the CASS FSM template) www.cass.uk.net
4. Audit of the development Lifecycle (using the CASS template for Part 2, E/E/PE) www.cass.uk.net
5. Review of the techniques and measures from IEC 61508-2 Annex B

2 SCOPE OF THE ASSESSMENT

2.1 Assessment procedures, tools and techniques used

During examination of the documentation and the audit, the following procedures, tools and techniques were used:

- Use was made of the The CASS Scheme Common Schedules and the relevant schedule of TOEs in The CASS Guide (www.cass.uk.net)
- The Sira Certification Service procedures manual for functional safety assessment

2.2 Existing certification relevant to this assessment

Rotork Fluid Systems has an accredited ISO 9001:2008 quality management system issued by BSI (UKAS 003 accredited) with relevant scope covering the lifecycle activities considered in this assessment. The certificate is in the name of Exeeco Ltd, which is the legal entity that trades as Rotork Fluid Systems at the Bramley address.

Details of the ISO 9001:2008 Quality Management System certificate are:

- BSI certificate No FM 02245
- Original issue date: 01-Nov-1989
- Latest issue date: 05-May-2011
- Expiry date: 05-Nov-2012

The above approval is relevant to most aspects of the management of functional safety (IEC 61508 Part 1 clause 6) and the lifecycle (IEC 61508 Part 2 clause 7) that are relevant to these products. The ISO 9001 provides a baseline on which the additional requirements of FSM are added. Sira does not re-assess the existing (certified) ISO 9001 scope in its complete depth, but takes it into account where relevant during the process audits.

3 SUMMARY OF THE ASSESSMENT

3.1 Management of functional safety

An assessment of Rotork Fluid Systems management of functional safety was performed. To avoid the introduction of systematic failures in these types of electromechanical devices there is much reliance on an effective quality management system coupled with the additional requirements for functional safety from IEC 61508 Part 1, clause 6. There is no direct guidance in IEC 61508-1 clause 6 for rigour against SIL.

Overall, Rotork Fluid Systems has a well established and stable QMS comprising a number of linked documents with contents that are straightforward to understand. All staff have read-access to the procedures; write-access is restricted to authorised members of the Quality Department. Much of the framework required by IEC 61508 for the management of functional safety already exists in the form of the ISO 9001 QMS.

There were some issues that were raised from the document review and site audit using the CASS TOEs for FSM but which Rotork Fluid Systems have now fully addressed. A summary record of these findings is provided in Appendix 4.

The results of the assessment indicate that the Rotork Fluid Systems management of functional safety that is applied to the products listed in section 1.2 for which certification is being sought is appropriate and sufficient to satisfy the relevant requirements of IEC 61508-1 clause 6 for the ongoing lifecycle.

Details of the audit are provided in Appendix 1.

3.2 E/E/PE System Safety Lifecycle

Rotork's Fluid Systems have a core design and development procedure (Q303 FEN) supported with various forms which describes the product lifecycle from initial concept to release to the market. It breaks the product realisation down into defined stages to manage the business and technical aspects and defines the responsibilities for those involved in the implementation, review and approval process.

Rotork's design and development procedures, including forms, have been reviewed by Sira against the requirements of IEC 61508 and audited for correct implementation on the products for which certification has been applied. The products listed in section 1.2 were not originally developed to a fully compliant IEC 61508-2 lifecycle, however, their safety functions are implemented by simple ('Type A') technology and Sira consider that it is therefore sufficient only to apply the requirements of the IEC 61508-2 lifecycle for on-going activities. These activities (where they are in addition to the existing ISO 9001 system) include adding functional safety parameters to specifications, modification impact analysis, adding functional safety information to user documentation, field failure analysis and maintaining integrity throughout the manufacturing process.

Overall, the realisation lifecycle can be mapped to the model in IEC 61508 Part 2. The level of test and inspection for the manufacturing activities is very good and coverage of the routine factory tests provides an appropriate validation of the functionality of each product being despatched.

There were some issues that were raised from the document review and site audit against the CASS TOEs for the E/E/PE realisation lifecycle but which Rotork Fluid Systems have now fully addressed. A summary record of these findings is provided in Appendix 4.

The results of the assessment indicate that the Rotork Fluid Systems E/E/PES realisation lifecycle for the products for which certification is being sought is appropriate and sufficient to satisfy the relevant requirements of IEC 61508-2 clause 7 for the ongoing lifecycle.

Details of the audit are provided in Appendix 2.

3.3 Techniques and Measures from IEC 61508-2 Annex B

Rotork Fluid Systems use a number of the mandatory (M), highly recommended (HR) and recommended (R) techniques and measures (T&Ms) described in IEC 61508-2 to avoid introducing failure modes throughout the phases of the E/E/PE realization lifecycle.

Details of the Techniques and Measures from IEC 61508-2 Annex B that are used by Rotork Fluid Systems are provided in Appendix 3.

Overall, the selection of the various T&Ms make the products suitable for use in safety related systems up to SIL 3 and hence support a claim for Systematic Capability of SC3.

4 CONCLUSIONS AND RECOMMENDATIONS

The assessment of the evidence provided by Rotork Fluid Systems has shown that the current management of functional safety and the E/E/PE realisation lifecycle for the products listed in section 1.2 of this report for which certification is being sought is appropriate and meets the relevant requirements of IEC 61508 Parts 1 and 2 for use in safety functions up to and including SIL 3.

The actual SIL-capability of each product will also depend on the quantitative assessment by Sira for the product in question.

This report may be used to augment and support the recommendations in the assessments of the products listed in section 1.2 of this report, particularly in relation to each product's Systematic Capability (SC) parameter.

It is recommended that Sira refers to the record of initial audit findings (Appendix 4) when planning the first surveillance audit to ensure the corrective measures are being used consistently.

APPENDIX 1: FUNCTIONAL SAFETY MANAGEMENT (IEC 61508-1: 2010)

Refer to full version of Sira assessment report R56A28091B (43 pages).

APPENDIX 2: E/E/PE LIFECYCLE (IEC 61508-2: 2010)

Refer to full version of Sira assessment report R56A28091B (43 pages).

APPENDIX 3: TECHNIQUES AND MEASURES FROM IEC 61508-2: 2010, ANNEX B

Refer to full version of Sira assessment report R56A28091B (43 pages).

APPENDIX 4: SUMMARY AND STATUS OF INITIAL AUDIT FINDINGS

Refer to full version of Sira assessment report R56A28091B (43 pages).