TUV AUSTRIA ITALIA S.p.A.

Report no.: TAI-FS-R-25-0053

SIL ASSESSMENT REPORT

IEC 61508-1/7:2010

Pneumatic / hydraulic compact scotch-yoke spring return and double acting actuator

Series RC

Rotork Sweden AB
Kontrollvägen, 15
SE-791 22 Falun

Date: **2025-12-17**

Author
Carlo Tarantola

Signature

This document is only valid in its entirety, without any change.

INDEX

0 STATUS OF THE DOCUMENT

History: R 00: Initial release Date: 2025-12-17

Release status: Released to client

Author(s): Carlo Tarantola

1 INTRODUCTION

This report is related to the assessment according to standards:

IEC 61508-1/7:2010

for the following products:

pneumatic / hydraulic compact scotch-yoke spring return and double acting actuator series RC

The assessment covers the following aspects:

- Management of Functional Safety / Functional Safety Planning
- Safety Requirements Specification
- Design:
  - Quantifiable aspects:
    - Random Failure Rates, DC, SFF, PFD_{AVG}
    - β Factors
    - MRT
    - PTC
    - Architectural Constraints
  - Non-quantifiable aspects:
    - Behaviour of the safety function under fault conditions
    - Safety related SW
    - Systematic failures (Systematic Capability)
    - Behaviour under environmental conditions
- Verification and Validation
- Information for Use
- Modification

The report includes:

- List of reference documents
- Description of the safety function(s)
- Description of the product(s) subject to the assessment
- Assessment procedure
- Assessment of all the above-mentioned aspects
- Summary of results

NOTES:

- The results of this report can be used for the assessment of a complete Safety Instrumented System

2 REFERENCE DOCUMENTS

2.1 Standards

No.	Reference	Title
[N1]	IEC 61508:2010 Part 1–7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
[N2]	IEC 61511-1:2016 + A1:2017 IEC 61511:2016 Part 2–3	Functional Safety – Safety Instrumented Systems for the process industry sector

NOTES:

- [N2] is mentioned only because in its Part 1, par. 1, letter c) and related figures 2 and 3, it makes reference to [N1] as reference standard for manufacturers and suppliers of devices

2.2 Databases

No.	Reference	Title
[N3]	RiAC NPRD-2016	Non electronic Parts Reliability Data
[N4]	RiAC FMD-97/2013	Failure Modes/Mechanism Distributions
[N5]	NSWC	Handbook of Reliability Prediction Procedures for Mechanical Equipment
[N6]	Exida	Safety Equipment Reliability Handbook
[N7]	OREDA	Offshore Reliability Data

NOTES:

- For databases, where there is no indication of the publishing date it means that the reference is the latest edition

3 ASSESSMENT DOCUMENTS

No.	Reference	Title
Planning		
[D1]	Rotork document no. DOK-000166 Rev. C	Functional safety management plan
Specification		
[D2]	Rotork document no. DOK-000169 Rev. A	Safety requirements specification
Design		
[D3]	Rotork document no. PUB014-001-00 Ed. 11/23	Technical brochure
[D4]	Rotork Folder	Sectional drawings with component list
[D5]	Rotork document no. DOK-000173 Rev. A	HW systematic failure estimation
[D6]	Rotork document no. DOK-000173 Rev. A	Common cause failure estimation
[D7]	Rotork document no. DOK-000167 Rev. A	Random failure analysis
Verification and validation		
[D8]	Rotork document no. DOK-000168 Rev. A	Safety validation plan
[D9]	(Intentionally left blank)	(Intentionally left blank)
[D10]	Rotork internal document	Products database
[D11]	Rotork internal document	Failure database
Manuals		
[D12]	Rotork documents no. 706B, 836K, 883D	IOM manual
[D13]	Rotork document no. DOK-000165 Rev. B	Safety manual

NOTES:

- Specific documents mentioned in [D1] – [D13] (e.g. individual Test Reports referenced in [D8]) are not explicitly mentioned in the above list
- Even though some of Rotork documents (i.e. document [D3]) refer in the title only to pneumatic actuators, the same are applicable also to hydraulic actuators as specified in the respective text

4 ABBREVIATIONS AND DEFINITIONS

Term	Meaning
β, β_D	Beta common cause factor
λ_{BB}	“Black Box” Failure rate – Literature data
λ_D	Failure rate of dangerous failures
λ_{DD}	Failure rate of detected dangerous failures
λ_{DU}	Failure rate of undetected dangerous failures
λ_{NE}	Failure rate of no effect failures
λ_S	Failure rate of safe failures
λ_{SS}	“Steady State” Failure rate – Final value
DC	Diagnostic coverage
FMEDA	Failure modes, effects and diagnostic analysis
HDM	High demand mode
HFT	Hardware fault tolerance
LDM	Low demand mode
MRT	Mean repair time
PFD	Probability of failure on demand
PFD_{AVG}	Average probability of failure on demand
PFH	Probability of failure per hour
PST	Partial stroke test
PTC	Proof test coverage
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SLC	Safety lifecycle
SRS	Safety requirements specification
TI	Test interval for proof test (full stroke)
TI_D (TI_{PS})	Test interval for diagnostic test (partial stroke)

For definitions, standard [N1] (in particular Part 4) applies.

5 SAFETY FUNCTION(S)

The safety function is defined as follows:

- *Spring return actuators:*
    1. *The actuator performs the safety function on demand if it delivers a full stroke (90° ± tolerance) driven by the spring, with power fluid exhausted from the cylinder through the control system.*

NOTES: considering the functioning of the actuator to perform the safety function(s), the safety functions "close" and "open" can be considered equivalent. The safety function is in both cases driven by the spring.
The choice of the safety function to be implemented is responsibility of the system integrator.

- *Double acting actuators*
    1. *The actuator performs the safety function on demand if it delivers a full stroke (90° ± tolerance) driven by the piston of cylinder, powered by the specified medium working pressure.*

NOTES: considering the functioning of the actuator to perform the safety function(s), the safety functions "close" and "open" can be considered equivalent.
The choice of the safety function to be implemented is responsibility of the system integrator.

In the following paragraphs, the safety function is simply mentioned numbered **1**.

The assessment covers the above safety function(s).

6 PRODUCT DESCRIPTION

6.1 Scope of certification and exclusions

The products subject to certification are pneumatic / hydraulic compact scotch-yoke spring return actuators series RC, including models RCC, RCCO, RCE, RCI, RCIO, RCIOT, RCIT, RCO, RCOT, RCT.
Legenda after the two first letters (RC):

- C: carbon steel
- I: dimension in inches (only for external connection)
- O: overstroke
- T: extracorrosion
- E: RCE is the denomination for bare actuators used for Rotork complete hydraulic units (with motor, pump, tank and so on). They are exactly as RC hydraulic but with fastenings for the hydraulic unit

NOTE: the actuators can be supplied with pneumatic or hydraulic medium, without any modification to the design.

The assessment refers to the actuator only. Any additional device (e.g. solenoid valve, PST device) is outside the scope of the assessment.

Detailed information is included in point 6.5 and [D3], [D4], [D12], [D13].

6.2 Architecture

The product has a single channel configuration, HFT=0.

6.3 Classification

The product can be classified as Type A according to [N1], for use in High Demand Mode applications.

NOTES:

- The classification refers to the actuator itself. The classification remains Type A even in case the valve assembly is equipped with a (non-interfering) PST device, according to the definition included in [N1] Part 2, par. 7.4.4.1.2

6.4 Drawings and parts lists

Drawings and parts lists are included in [D4].

6.5 Details of design and functioning

Rotork RC actuators feature a modern scotch-yoke mechanism that provides high start- and end-torque output in a very compact package.
They are available in both double-acting and spring-return configurations with an optional integral manual override.
Spring return actuators feature springs that are safely contained within an epoxy-coated cartridge.

The main characteristics are:

- Cylinder dimensions: from 55 to 200 mm diameter
- Single and double piston (double piston configuration as “worst case”)
- Bearings: polymer for standard application and brass for low temperature application

In respect to normal RC series, RC88 series is characterised by the following main differences:

- Double actuator configuration
- Internal and external springs (only for spring return actuators)

Further information is included in [D3] and [D4].

7 ASSESSMENT PROCEDURE

The basis for the certification is provided by the assessment of the following phases:

1. Management of functional safety / Functional safety planning
2. Safety requirements specification
3. Design:
    a. quantifiable aspects: random failure rates, DC, SFF, PFD_{AVG}; β factors; MRT; PTC; architectural constraints
    b. non-quantifiable aspects: behaviour of the safety function under fault conditions; safety-related software; systematic failures (Systematic Capability); behaviour under environmental conditions
4. Verification and validation
5. Information for use
6. Modification

8 MANAGEMENT OF FUNCTIONAL SAFETY

8.1 Management of functional safety / Functional safety planning

A functional safety audit of the management systems and of the functional safety planning is conducted to document and highlight that the development of the product under consideration is compliant with [N1].

Assessment result:
The documentation structure and the structure of the functional safety management system are adequately documented.
The audit, interviews and document reviews conducted have shown that the requirements laid down in [N1] with respect to functional safety management are fulfilled, with particular reference to:

- Organisation and responsibilities
- Competence of personnel
- Procedures used and documentation issued for each applicable phase of the SLC
- Techniques/measures used for each phase of the SLC

The following existing Company Quality Certifications have been considered:

- EN ISO 9001:2015

Assessed documents:
[D1] and related documents.

8.2 Safety requirements specification

The SRS [D2] is assessed with respect to its consistency and completeness in a comparison with the applicable requirements of [N1] Part 1, par. 7.10.

Assessment result:
The audit revealed that the SRS completely describes the safety function(s) to be implemented, in terms of functional and safety requirements.

Assessed documents:
[D2].

9 DESIGN

9.1 Quantifiable aspects

9.1.1 Random failure rates, DC, SFF, PFD_{AVG}

9.1.1.1 Procedure

The determination of random failure rates is performed with a Failure Modes, Effects and Diagnostic Analysis (FMEDA), integrated with field feedback (documented in [D11]), according to [N1] Part 2 par. 7.4.4.3.3, using the Bayesian approach.

The procedure used for the determination of random hardware failures is the following:

1. FMEDA of the product, with classification of failure modes
2. Evaluation of λ_{BB} values (literature data)
3. Evaluation of field feedback
4. Integration between literature data and field feedback, using the Bayesian approach
5. Determination of λ_{SS} values (final value)

The FMEDA is based on the documentation (drawings with components lists) provided by the manufacturer, and the other design documentation referenced in par. 3, and is documented in [D7].

The FMEDA includes the following information:

Item	Meaning
Position	Position of the component on the drawing
Component	Description of the component
Function	Function of the component
Quantity	No. of components which have the same function
Local Architecture	Local redundancy of the component (if any), to perform the specific function
Beta Factor	Parameter used in case of local redundancy
Failure rate	Total failure rate of the single component – Taken from the databases referenced in par. 2.2.
Total failure rate	Total failure rate, considering the values of Quantity and Beta Factor
Failure Mode	Failure Mode taken from the databases referenced in par. 2.2.
Failure Distribution	% of the total failure rate allocated to the specific failure mode
Mode failure rate	Failure rate of the specific failure mode
Effect	Effect of the failure mode on the safety function(s)
SIL Classification	Failure category according to [N1]. See par. 9.1.1.2 for details.
Diagnostics	Diagnostic test (internal or external) able to detect the specific failure mode
DC	Diagnostic Coverage of the identified diagnostic test
λ_S, λ_{DD}, λ_{DU}, λ_{NE}	Failure rate of the failure mode, for the specific failure category

The system for reporting failures is based on field feedback from end users, with:

- Identification of the claim/failure
- Root cause analysis to identify cause and responsibility of the failure
- Identification of the possible effect of the failure on the safety function
- Classification of the failure considering the failure categories of [N1]

Furthermore, the requirements in [N1] Part 2, par. 7.4.10.1–7.4.10.7 are assessed and considered fulfilled (as detailed in [D7]), as:

- the product has a restricted and specified functionality and is designed to perform specified safety functions
- the product has an adequate documentary evidence (including extensive operating experience and results of suitability analysis and testing), sufficient to claim the declared failure rates
- the company has an effective system for reporting failures, as above described

The FMEDA for use in HDM has been developed basing on the existing FMEDA for LDM application, with the following procedure:

- identification of components for which the high utilization rate can generate a greater wear or minor ageing (blockage)
- for these components, identification of specific failure modes that can be influenced by greater wear or minor ageing
- for these failure modes, estimation of failure rate increase (because of more wear) or, respectively, failure rate decrease (because of less ageing)
- estimation of increase / decrease of failure rate is made considering:
  - differences between use in LDM and HDM reported in reference databases, as NSWC and Exida EMCRH
  - technical analysis among experts in the field
  - combination of the two above-mentioned techniques
- obtaining λ_{BB} result
- to achieve λ_{SS} value, the same corrective factor derived from the Bayesian analysis for LDM has been used

9.1.1.2 Description of the failure categories

The following table lists:

- The failure types considered in the assessment
- The failure definition according to [N1]
- For each failure type, examples of failures considered for the specific product

Failure Type	Failure definition according to [N1]	Examples for the specific product
Safe	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. results in the spurious operation of the safety function; or b. increases the probability of the spurious operation of the safety function	• According to the definition in the previous column (in particular definitions 3.6.8 and 3.6.13 of [N1] Part 4), no Safe Failures are possible in a single acting actuator: each failure mode of the actuator itself shall be classified as “Dangerous” or “No Effect” (failures which can generate the spurious operation of the safety function are only external to the actuator itself, or are related to components that “play no part in implementing the safety function”); hence, **λ_S=0 for each type of single acting actuator**. • According to the definition in the previous column (in particular definitions 3.6.8 and 3.6.13 of [N1] Part 4), no Safe Failures are possible in a double acting actuator: each failure mode of the actuator itself shall be classified as “Dangerous” or “No Effect” (failures which can generate the spurious operation of the safety function are only external to the actuator itself, and even in the case of loss of power supply the actuator “stays put”); hence, **λ_S=0 for each type of double acting actuator**.
Dangerous	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode); or	• Binding / sticking of components involved in the safety function • Breakage of components involved in the safety function

Failure Type	Failure definition according to [N1]	Examples for the specific product
	b. decreases the probability that the safety function operates correctly when required	
No Effect	Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function	• Superficial score / dent of structural components
No Part	Failure of a component that plays no part in implementing the safety function	• Failures of accessories for transportation • Only for single acting actuators: Failures of components of the cylinder (this kind of failures can even generate spurious trips)

NOTES:

1. For single acting actuators, failures of components of the cylinder which can generate spurious trips shall be correctly classified as “No Part” and not “Safe”, being related to components that “play no part in implementing the safety function” (see definition 3.6.16 of [N1] Part 4)
2. For double acting actuators, failures of components of the cylinder cannot generate spurious trips
3. According to definitions 3.6.13 and 3.6.14 of [N1] Part 4, the no part and no effect failures are not used for SFF calculations
4. According to definitions 3.6.8, 3.6.13, 3.6.14 of [N1] Part 4, the safe, no part and no effect failures do not contribute to PFD_{AVG} calculations

9.1.1.3 Assumptions

The following assumptions are used for the evaluation of random hardware failures:

- Failure rates are considered constant for the lifetime (25 years, as stated in the Safety Manual [D13])
- Failure rates and failure modes in the FMEDA are taken from databases [N3] – [N7]
- A single component failure fails the entire product, except for redundant configurations. For β values used, see par. 9.1.2
- Propagation of failures is considered not relevant, unless a clear propagation path is present: in this case, the failure is considered a single failure, with failure rate corresponding to the failure rate of the first failure
- The components that are not part of the safety function and cannot influence the safety function are excluded from the evaluation
- After a proof test, the product will be “as new”
- The installation, commissioning, operational and maintenance instruction are correctly applied by the final customer

9.1.1.4 Determination of λ values, DC, SFF and PFD_{AVG}

λ values

The total random failure rates – λ values – are calculated from the FMEDA + field feedback.

Assessment result:
The results are included in the following table.

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_S [1/h]
Series RC spring return - No on-line monitoring	1	1,39E-08	0,00E+00	0,00E+00
Series RC spring return - With on-line monitoring	1	1,25E-09	1,27E-08	0,00E+00
Series RC88 spring return - No on-line monitoring	1	2,35E-08	0,00E+00	0,00E+00
Series RC88 spring return - With on-line monitoring	1	2,12E-09	2,14E-08	0,00E+00
Series RC double acting - No on-line monitoring	1	1,40E-08	0,00E+00	0,00E+00
Series RC double acting - With on-line monitoring	1	1,26E-09	1,27E-08	0,00E+00
Series RC88 double acting - No on-line monitoring	1	2,36E-08	0,00E+00	0,00E+00
Series RC88 double acting - With on-line monitoring	1	2,13E-09	2,15E-08	0,00E+00

NOTES:

- The results in the table are valid for all the configurations listed in par. 6 (worst-case values)
- For definitions of Safety Functions, see par. 5
- For the reason why λ_S=0, see par. 9.1.1.2
- The λ_S values are not divided in λ_{SD} and λ_{SU}, as this subdivision would have no relevance for any of the SIL parameters
- As specified in par. 9.1.1.2, failures of components of the cylinder:
  - For spring return actuators, they can generate spurious trips and therefore shall be correctly classified as “No Part” and not “Safe”, being related to components that “play no part in implementing the safety function” (see definition 3.6.16 of [N1] Part 4). The “spurious trip rate” is estimated in:
    - Series RC: 1,42E-08 [1/h]
    - Series RC88: 4,50E-08 [1/h]
  - For double acting actuators, they cannot generate spurious trips. The “spurious trip rate” is therefore 0,00E+00 [1/h]

Assessed documents:
[D7] and related documents.

DC

The product does not include internal diagnostics.
Diagnostic is only possible via external means, e.g. with on-line monitoring by the process.
On-line monitoring by the process is considered relevant and effective if:

- the actuator has a High Utilization Rate, and
- the Safety Function operates in LDM, or in HDM but with Demand Rate at least ten times lower than the Utilization Rate of the actuator

On the contrary, PST is considered not relevant in HDM application.

The procedure for the external diagnostic tests is described in the Safety Manual [D13].
The effect of an external diagnostic test is considered during the FMEDA, to discriminate between λ_{DD} and λ_{DU}.

Assessment result:
Considering the application of the described on-line monitoring procedure, the test coverage can be considered:

- ≥ 90%

Assessed documents:
[D3] – [D7].

SFF

The formula for SFF is the following:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}$$

The value of SFF is calculated using the λ values resulting from the FMEDA + field feedback.

Assessment result:
Considering that λ_S=0, according to definitions 3.6.15 of [N1] Part 4:

- SFF=0 without external diagnostic tests
- SFF>0 with external diagnostic tests, carried out according to definition 3.8.7 of [N1] Part 4, and according to what written in the Safety Manual

Assessed documents:
[D3] – [D7].

PFH

According to [N1], the following formula is used to estimate the PFH value:

$$PFH = \lambda_{DU}$$

Assessment result:
The results are given in the following table.

Configuration	Safety function	PFH [1/h]
RC spring return - No on-line monitoring	1	1,39E-08
RC spring return - With on-line monitoring	1	1,25E-09
RC88 spring return - No on-line monitoring	1	2,35E-08
RC88 spring return - With on-line monitoring	1	2,12E-09
RC double acting - No on-line monitoring	1	1,40E-08
RC double acting - With on-line monitoring	1	1,26E-09
RC88 double acting - No on-line monitoring	1	2,36E-08
RC88 double acting - With on-line monitoring	1	2,13E-09

The values in the above table are compatible with SIL 3.

Assessed documents:
[D7] and related documents.

9.1.2 β factors

The product has a single channel configuration, HFT=0.
The β factors can be used when performing calculations for redundant architectures.

Assessment result:
The evaluation of Common Cause factors, relevant when the product is used in redundant configuration, is performed according to [N1], Part 6.
The result is:

- $\beta=\beta_D=0,05$

NOTES:

- The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to [N1] Part 6, Table D.5
- The above value is calculated in the hypothesis of redundancy without diversity

Assessed documents:
[D6].

9.1.3 MRT

The MRT is estimated taking in consideration the failure distribution and the estimated repair time for the main failure modes.

Assessment result:
The MRT is indicated in the following table.

Model / Configuration	MRT [h]
Series RC	24

NOTE:

- the MRT considered is the Technical Mean Repair Time, i.e., it takes in consideration availability of skilled personnel, adequate tools and spare parts.

Assessed documents:
[D13].

9.1.4 PTC

The procedure for the Proof Test is described in the Safety Manual [D13].

Assessment result:
Considering the application of the described test procedure, the PTC, in case of automatic procedure, can reach values > 99%. It could be lower considering test procedure imperfections (e.g. uncalibrated instrumentation, non-safety software functions used for the test).
In case of manual procedure, the test coverage shall take into account also the test imperfections and the reliability/competence of the operator.

Assessed documents:
[D13].

9.1.5 Architectural constraints

For the evaluation of the conformity to the requirement of hardware safety integrity architectural constraints, both Route 1_H and Route 2_H are used.

As the product is classified as “Type A”, no requirements for SFF are given for Route 2_H.

Assessment result:

Safety Function	Type	HFT	SFF[1]	Route 1_H	Route 2_H	Max. SIL according to architectural constraints
1	A	0	≥90%	Applied in case of performing of on-line monitoring and assuming an on-line monitoring coverage up to ≥90%. For a type A element with SFF≥90%, Route 1_H results in a maximum claimable SIL equal to 3.	Applied. The application of Route 2_H results in a maximum claimable SIL equal to 1.	3

The product can be used in:

- single channel configuration:
  - up to SIL 1 without on-line monitoring by the process
  - up to SIL 3 considering on-line monitoring by the process
- double channel configuration: up to SIL 3

Assessed documents:
[D3] – [D7].

9.2 Non-quantifiable aspects

9.2.1 Behaviour of the safety function under fault conditions

As written in par. 9.1.1.4, the product does not include internal diagnostics.
Diagnostic is only be possible via external means, e.g. with on-line monitoring by the process.

Assessment result:
The behaviour of the safety functions under fault condition is evaluated with the FMEDA, and is described in [D7].
See also paragraph 9.1.1.4 for details.

Assessed documents:
[D3] – [D9], [D13].

9.2.2 Safety-related software

No SW is used to implement the safety function.

[1] The performing of on-line monitoring has been taken into account when evaluating the Safe Failure Fraction.

9.2.3 Systematic failures (Systematic Capability)

The systematic capability is assessed using Route 1_S, evaluating the application of adequate techniques and measures to control and avoid systematic failures (Tables A.15 – A.17 and B.1 – B.5 of [N1] Part 2).
Evidence was identified for each technique/method used.

Assessment result:
The techniques and measures used to control and avoid the occurrence of systematic failures are adequate up to a SIL 3 value.
The audit, interviews and document reviews have shown that the requirements laid down in [N1] with respect to systematic failures are fulfilled, with particular reference to:

- Organisational measures: project management, documentation structure, information for use, etc.
- Technical measures: safety design, correct choice of components, test planning and reports, etc.

Tests and analysis are performed (see [D8] – [D9] and related documents) to assess the functional and integrity requirements. The following analysis and tests are planned and documented:

- Normal functional tests (production tests)
- Extended and worst-case analyses and tests
- Failure analysis and tests:
  - Random failure analysis
  - Systematic failure analysis
  - Common cause analysis
  - Fault insertion tests
- Environmental tests / analysis

The existing tests have been considered for the assessment.

Assessed documents:
[D5], [D8] – [D9] and related documents.

9.2.4 Behaviour under environmental conditions

The behaviour in environmental conditions is assessed evaluating the results of adequate environmental tests.

Assessment result:
Functional tests in the relevant extreme environmental conditions are performed.
The tests in environmental conditions do not impact the functional safety of the product.

Assessed documents:
[D8] – [D9] and [D12] – [D13].

10 VERIFICATION AND VALIDATION

The verification and validation activities performed by the manufacturer using review, analysis and tests, are assessed.

Assessment result:
After each design phase, a verification activity is performed by the manufacturer to check that the requirements of the specific phase are fulfilled.
The verification and validation activities cover the following:

- Design review
- Design calculations
- Normal functional tests
- Extended and worst-case analyses and tests
- Failure analysis and tests
- Environmental tests

Assessed documents:
[D1] and related documents, [D8] – [D9] and related documents.

11 INFORMATION FOR USE

The assessment covers:

- the installation, operation and maintenance instructions (IOM Manual)
- the particular instructions required by Annex D of [N1] Part 2 (Safety Manual)

Assessment result:
The relevant instructions for the installation, operation and maintenance of the product are included in the IOM manual [D12].
The Safety Manual [D13] includes all the information required by [N1] Part 2, Annex D.

Assessed documents:
[D12] – [D13].

12 MODIFICATION

Procedures for modification activity are described in specific documents, referenced in [D1].

13 SUMMARY OF RESULTS

The analysis gives the results summarised in the following table.

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_S [1/h]	Systematic Capability	Max. SIL according to Architectural Constraints
Series RC spring return - No on-line monitoring	1	1,39E-08	0,00E+00	0,00E+00	3	1
Series RC spring return - With on-line monitoring	1	1,25E-09	1,27E-08	0,00E+00	3	3
Series RC88 spring return - No on-line monitoring	1	2,35E-08	0,00E+00	0,00E+00	3	1
Series RC88 spring return - With on-line monitoring	1	2,12E-09	2,14E-08	0,00E+00	3	3
Series RC double acting - No on-line monitoring	1	1,40E-08	0,00E+00	0,00E+00	3	1
Series RC double acting - With on-line monitoring	1	1,26E-09	1,27E-08	0,00E+00	3	3
Series RC88 double acting - No on-line monitoring	1	2,36E-08	0,00E+00	0,00E+00	3	1
Series RC88 double acting - With on-line monitoring	1	2,13E-09	2,15E-08	0,00E+00	3	3

NOTES:

- The results in the table are valid for all the configurations listed in par. 6 (worst-case values)
- For definitions of Safety Functions, see par. 5
- For the reason why λ_S=0, see par. 9.1.1.2
- The λ_S values are not divided in λ_{SD} and λ_{SU}, as this subdivision would have no relevance for any of the SIL parameters
- As specified in par. 9.1.1.2, failures of components of the cylinder:
  - For spring return actuators, they can generate spurious trips and therefore shall be correctly classified as “No Part” and not “Safe”, being related to components that “play no part in implementing the safety function” (see definition 3.6.16 of [N1] Part 4). The “spurious trip rate” is estimated in:
    - Series RC: 1,42E-08 [1/h]
    - Series RC88: 4,50E-08 [1/h]
  - For double acting actuators, they cannot generate spurious trips. The “spurious trip rate” is therefore 0,00E+00 [1/h]
- The product can be used in:
  - single channel configuration:
    - up to SIL 2 without external diagnostic tests
    - up to SIL 3 considering external diagnostic tests
  - double channel configuration up to SIL 3
- For further details, make reference to the Safety Manual [D13]

The results of this report can be used for the assessment of a complete Safety Instrumented System.