TÜV INTERCERT S.r.l. – Group of TÜV Saarland

Report no.: RC-0919-SIL-TIC-PC-0010061-17-02

SIL SUMMARY REPORT

IEC 61508-1/7:2010

Pneumatic / hydraulic compact scotch-yoke spring return actuators

Series RC

Rotork Sweden AB
Kontrollvägen, 15
SE-791 22 Falun

Date: **2019-09-12** Place: **Reggio Emilia**

Author
Carlo Tarantola

Carlo Tarantola

Signature

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

1 INTRODUCTION

This report summarises the results of the assessment according to standards:
IEC 61508-1/7:2010
for the following products:
pneumatic / hydraulic compact scotch-yoke spring return actuators series RC

NOTES:

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

2 ASSESSMENT AND RESULTS

Product identification		
Device	Pneumatic / hydraulic compact scotch-yoke spring return actuators	
Series	RC	
Models / configurations	RC - No on-line monitoring RC - With on-line monitoring RC88 - No on-line monitoring RC88 - With on-line monitoring	
Safety function(s)		
1.	Delivery of a full stroke (90° ± tolerance) driven by the spring, with power fluid exhausted from the cylinder through the control system. NOTE: 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.	
Mode of operation of the safety function(s)	High demand mode	
Reference standards		
General functional safety standard	IEC 61508-1/7:2010	
Product specific functional safety standard	None	
Assessment phases		
Management of functional safety / functional safety planning	Assessed	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 IEC 61508.
Safety requirements specification	Assessed	The Safety requirements specification is assessed with respect to its consistency and completeness in a comparison with the applicable requirements of IEC 61508.

Design	Assessed	The assessment of the design included the following aspects: • Quantifiable aspects: random failure rates, DC, SFF, PFH, β factors, MRT, PTC, architectural constraints • Non-quantifiable aspects: behaviour of the safety function under fault conditions, safety-related software (not applicable to the product under consideration), systematic failures, behaviour under environmental conditions See below for the results.
Verification and Validation	Assessed	The verification and validation activities performed by the manufacturer include review, analysis and tests.
Information for use	Assessed	The assessment covers: • the installation, operation and maintenance instructions (IOM Manual) • the particular instructions required by Annex D of IEC 61508 Part 2 (Safety Manual)
Modification	Assessed	Procedures for modification activity are described in specific documents, referenced in the safety planning.

Results	
Selected assessment routes	• For architectural constraints: Routes 1_H and 2_H • For Systematic Capability: Route 1_S Furthermore, the requirements in paragraphs 7.4.10.1–7.4.10.7 of IEC 61508 Part 2 are assessed and considering fulfilled, 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 manufacturer has an effective system for reporting failures
Element type (A or B)	Type A
HFT	The product has a single channel configuration, HFT=0.

Random failure rates	The determination of random failure rates is performed with a FMEDA, integrated with field feedback, according to IEC 61508 Part 2 Par. 7.4.4.3.3, using the Bayesian approach.

Configuration	**Safety function**	**λ_{DU} [1/h]**	**λ_{DD} [1/h]**	**λ_{S} [1/h]**
RC - No on-line monitoring	1	4,65E-08	0,00E+00	0,00E+00
RC - With on-line monitoring	1	4,18E-09	4,23E-08	0,00E+00
RC88 - No on-line monitoring	1	4,57E-08	0,00E+00	0,00E+00
RC88 - With on-line monitoring	1	4,12E-09	4,16E-09	0,00E+00

Spurious trip rate	• RC: 4,75E-08 [1/h] • RC88: 8,75E-08 [1/h] NOTE: 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 IEC 61508 Part 4). Anyway the spurious trip rate is estimated.
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 if: • the actuator has a very High Utilization Rate • 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 The procedure for the external diagnostic tests is described in the Safety Manual.
SFF	Considering that $\lambda_S=0$, according to definitions 3.6.15 of IEC 61508 Part 4: • SFF=0 without external diagnostic tests • SFF>0 with external diagnostic tests, carried out according to definition 3.8.7 of IEC 61508 Part 4, and according to what written in the Safety Manual
PFH	• RC - No on-line monitoring: 4,65E-08 [1/h] • RC - With on-line monitoring: 4,18E-09 [1/h] • RC88 - No on-line monitoring: 4,57E-08 [1/h] • RC88 - With on-line monitoring: 4,12E-09 [1/h]
β factors	$\beta=\beta_D=0,05$ • The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to IEC 61508 Part 6, Table D.5. • The above value is calculated in the hypothesis of redundancy without diversity The β factors can be used when performing calculations for redundant architectures.
MRT	24 h The MRT considered is the Technical Mean Repair Time, i.e., it takes in consideration availability of skilled personnel, adequate tools and spare parts.

PTC	The procedure for the Proof Test is described in the Safety Manual.
Architectural constraints	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
Expected lifetime	25 years
Behaviour of the safety function under fault conditions	The product does not include internal diagnostics.
Safety related SW	No SW is used to implement the safety function.
Systematic Capability	3
Behaviour under environmental conditions	The behaviour in environmental conditions is assessed evaluating the relevant environmental tests.
Limitations for use	Make reference to the Safety Manual.
Remarks	
• The random failure rates in the above table are valid for all the possible configurations of the product.	
• According to the definition of IEC 61508 (in particular definitions 3.6.8 and 3.6.13 of IEC 61508 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**.	
• 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 IEC 61508 Part 4). Anyway the spurious trip rate is estimated.	
• The λ_S values are not divided in λ_{SD} and $\lambda_{SU,}$ as this subdivision has no relevance for any of the SIL parameters.	
• For further details, make reference to the Safety Manual.	
Reference documents	
SIL Assessment Report	TÜV InterCert document no. RC-0919-SIL-TIC-PC-0010061-17-01
Safety Manual	Rotork document no. SM-RC-A-00-E

3 STATUS OF THE DOCUMENT

History:	R 00:	Initial release	Date: 2019-09-12
Release status:	Released to client		
Author(s):	Carlo Tarantola		

ANNEX A - 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
HFT	Hardware fault tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year
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)
Type A	"Non-complex" element (using only discrete components to implement the safety function)
Type B	"Complex" element (using also micro controllers or programmable logic to implement the safety function)

For definitions, standard IEC 61508 (in particular Part 4) applies.