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

Report no.: RC-0919-SIL-TIC-PC-0010513-19-06

SIL SUMMARY REPORT

IEC 61508-1/7: 2010

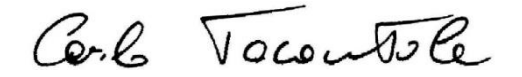
Switching valves

Series S3

Sitecna S.r.l. a socio unico
Via Giuseppe Di Vittorio, 22
I-20068 Peschiera Borromeo (MI)

Date: **2019-09-27** Place: **Reggio Emilia**

Author
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:
switching valves series S3

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	Switching valves	
Series	S3	
Models / configurations	S3 - No PST S3 - With PST	
Safety function(s)		
1.	De-energize-to-trip operation: when the signal pressure goes below the set value (regulated via the internal spring), the switching valve commutates, closing the pressure supply line and discharging the cylinder chamber of the actuator to the exhaust, or piloting a downstream power valve which performs the discharging of the cylinder chamber to the exhaust	
Mode of operation of the safety function(s)	Low 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, PFD_{AVG}, 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 considered 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]
S3 - No PST	1	1,14E-08	0,00E+00	1,05E-07
S3 - With PST	1	1,14E-10	1,13E-08	1,05E-07

DC	The product does not include internal diagnostics. Diagnostic is only be possible via external means, e.g. with a PST. The procedure for the PST is described in the Safety Manual.
SFF	• SFF (without external diagnostic tests): 90,15% • SFF (with external diagnostic tests): 99%
PFD_{AVG}	As the PFD_{AVG} value depends also on the test intervals and on the PTC and the coverage of external tests, which are not product-dependant quantities, the PFD_{AVG} values are not product relevant quantities, while λ values are. Anyway, PFD_{AVG} values are calculated for a certain number of combination of test intervals. See Annex A.
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 PFD_{AVG} calculations for redundant architectures.
MRT	• Substitution: 0,5 h • Repair using the spare part kit: 2 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	20 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.
• 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-0010513-19-06
Safety Manual	Sitecna document no. STC-SM-SW

3 STATUS OF THE DOCUMENT

History: R 00: Initial release Date: 2019-09-27

Release status: Released to client

Author(s): Carlo Tarantola

ANNEX A - EXAMPLES OF PFD_{AVG} CALCULATIONS

Type: S3 - No PST – Safety function: ***1***

Proof test interval (months)				
6	12	24	36	48
2,53E-05	5,04E-05	1,00E-04	1,51E-04	2,01E-04

Type: S3 - With PST – Safety function: ***1***

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	4,66E-06	4,91E-06	5,41E-06	5,91E-06	6,41E-06
	2	8,79E-06	9,04E-06	9,54E-06	1,00E-05	1,05E-05
	3	1,29E-05	1,32E-05	1,37E-05	1,42E-05	1,47E-05
	6		2,56E-05	2,61E-05	2,66E-05	2,71E-05
	9				3,90E-05	
	12			5,09E-05	5,14E-05	5,19E-05

NOTES:

- The above values of PFD_{AVG} are calculated for MRT=24 h and proof test coverage=100%. For other values of MRT, TI, TI_{PS} and/or non-perfect proof test, the PFD_{AVG} values must be re-calculated.
- The PFD_{AVG} values including partial stroke test are calculated considering the use of a commercial automatic partial stroking test system: for further details, see the Safety Manual.

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

ANNEX B - 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.