



# C E R T I F I C A T E

**Certificate no. 18-SIL-0010024-01-TIC**

WE HEREBY CERTIFY THAT

**Product description**

**EL-O-MATIC™ PNEUMATIC RACK AND PINION SPRING  
RETURN ACTUATORS**

**Models**

**SERIES F (up to and including size 0600)**

**Manufacturer**

**EMERSON AUTOMATION SOLUTIONS**

**Eekboerstraat 28A  
7575 AX Oldenzaal  
The Netherlands**

IS IN COMPLIANCE WITH THE REQUIREMENTS OF THE STANDARDS

**IEC 61508 Parts 1–7:2010**

AS RESULT OF THE ASSESSMENT ACCORDING TO THE PROVISION  
SET OUT IN THE ABOVE-MENTIONED STANDARDS

**Summary Report no. RC-0818-SIL-TIC-PC-0010024-18-02**

**Expiry date**

**19.08.2021**

**Note**

This certificate is issued upon the request of the manufacturer as voluntary certification; it does not include the production surveillance.

This certificate does not allow the manufacturer to use the safety mark of TÜV INTERCERT.

Reggio Emilia, 20.08.2018



Dipl. Ing. Feridoon Sergizzarea

TÜV INTERCERT Certification Body



# C E R T I F I C A T E

## ANNEX to Certificate no. 18-SIL-0010024-01-TIC

Type	A
HFT	0
Safety functions	1. Delivery of a full stroke ( $90^\circ \pm$ tolerance) driven by the spring, with power fluid exhausted from the cylinder through the control system
Mode of operation	Low Demand Mode

Random failure rates				
Configuration	Safety function	$\lambda_{DU}$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_S$ [1/h]
F - No PST	1	2,55E-08	0,00E+00	0,00E+00
F - With PST	1	2,29E-09	2,32E-08	0,00E+00

Systematic capability	3 (Route 1 <sub>S</sub> applied)			
Architectural constraints	Route 1 <sub>H</sub> :	Applied	Route 2 <sub>H</sub> :	Applied
	The product can be used in: <ul style="list-style-type: none"><li>single channel configuration:<ul style="list-style-type: none"><li>up to SIL 2 without external diagnostic tests</li><li>up to SIL 3 considering external diagnostic tests</li></ul></li><li>double channel configuration: up to SIL 3</li></ul>			

### Remarks:

- For further details, including environmental conditions, limitations of use, lifetime, failure rates traceability, mean repair times, common cause factors and systematic capability constraints, make reference to Safety Manual DOC.SILM.EF.EN.

END OF CERTIFICATE

Reggio Emilia, 20.08.2018

  
Dipl. Ing. Feridoon Sergizzarea

TÜV INTERCERT Certification Body



TÜV INTERCERT S.r.l. – Group of TÜV Saarland  
*on behalf of*  
TÜV INTERCERT GmbH – Group of TÜV Saarland

Report no.: RC-0818-SIL-TIC-PC-0010024-18-02

## **SIL SUMMARY REPORT**

**IEC 61508-1/7: 2010**

**EL-O-Matic™ pneumatic rack and pinion spring  
return actuators**

**Series F**

**Emerson Automation Solutions  
Eekboerstraat 28A  
7575 AX Oldenzaal  
The Netherlands**

Date: **2018-08-07**

Place: **Reggio Emilia**

Author  
Carlo Tarantola

A handwritten signature in black ink, appearing to read "Carlo Tarantola". The signature is written in a cursive style and is positioned above a horizontal line.

**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:

EL-O-Matic™ pneumatic rack and pinion spring return actuators series F

### NOTES:

- This report is related to the assessment of EL-O-Matic™ pneumatic rack and pinion spring return actuators series F up to and including size 0600.
- The results of this report can be used for the assessment of a complete Safety Instrumented System.

## 2 ASSESSMENT AND RESULTS

Product identification		
Device	EL-O-Matic™ pneumatic rack and pinion spring return actuators	
Series	F	
Models / configurations	F - No PST F - With PST	
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)	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	<p>The assessment of the design included the following aspects:</p> <ul style="list-style-type: none"> <li>Quantifiable aspects: random failure rates, DC, SFF, PFD<sub>AVG</sub>, <math>\beta</math> factors, MRT, PTC, architectural constraints</li> <li>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</li> </ul> <p>See below for the results.</p>
Verification and Validation	Assessed	The verification and validation activities performed by the manufacturer include review, analysis and tests.
Information for use	Assessed	<p>The assessment covers:</p> <ul style="list-style-type: none"> <li>the installation, operation and maintenance instructions (IOM Manual)</li> <li>the particular instructions required by Annex D of IEC 61508 Part 2 (Safety Manual)</li> </ul>
Modification	Assessed	Procedures for modification activity are described in specific documents, referenced in the safety planning.
<b>Results</b>		
Selected assessment routes		<ul style="list-style-type: none"> <li>For architectural constraints: Routes 1<sub>H</sub> and 2<sub>H</sub></li> <li>For Systematic Capability: Route 1<sub>S</sub></li> </ul> <p>Furthermore, the requirements in paragraphs 7.4.10.1–7.4.10.7 of IEC 61508 Part 2 are assessed and considered fulfilled, as:</p> <ul style="list-style-type: none"> <li>the product has a restricted and specified functionality and is designed to perform specified safety functions</li> <li>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</li> <li>the manufacturer has an effective system for reporting failures</li> </ul>
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	$\lambda_{DU}$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_S$ [1/h]
F - No PST	1	2,55E-08	0,00E+00	0,00E+00
F - With PST	1	2,29E-09	2,32E-08	0,00E+00
Spurious trip rate	4,80E-09 [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 be possible via external means, e.g. with a PST. The procedure for the PST is described in the Safety Manual.			
SFF	Considering that $\lambda_S=0$ , according to definitions 3.6.15 of IEC 61508 Part 4: <ul style="list-style-type: none"> <li>SFF=0 without external diagnostic tests</li> <li>SFF&gt;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</li> </ul>			
PFD <sub>AVG</sub>	As the PFD <sub>AVG</sub> 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 <sub>AVG</sub> values are not product relevant quantities, while $\lambda$ values are. Anyway, PFD <sub>AVG</sub> values are calculated for a certain number of combination of test intervals. See Annex A.			
$\beta$ factors	$\beta=\beta_D=0,05$ <ul style="list-style-type: none"> <li>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.</li> <li>The above value is calculated in the hypothesis of redundancy without diversity</li> </ul> The $\beta$ factors can be used when performing PFD <sub>AVG</sub> calculations for redundant architectures.			
MRT	1 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: <ul style="list-style-type: none"> <li>single channel configuration: <ul style="list-style-type: none"> <li>up to SIL 2 without external diagnostic tests</li> <li>up to SIL 3 considering external diagnostic tests</li> </ul> </li> <li>double channel configuration: up to SIL 3</li> </ul>			

Expected lifetime	10 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.
<b>Remarks</b>	
<ul style="list-style-type: none"> <li>The random failure rates in the above table are valid for all the possible configurations of the product.</li> <li>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, <b><math>\lambda_S=0</math> for each type of single acting actuator.</b></li> <li>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.</li> <li>The <math>\lambda_S</math> values are not divided in <math>\lambda_{SD}</math> and <math>\lambda_{SU}</math>, as this subdivision has no relevance for any of the SIL parameters.</li> <li>For further details, make reference to the Safety Manual.</li> </ul>	
<b>Reference documents</b>	
SIL Assessment Report	TÜV INTERCERT document no. RC-0818-SIL-TIC-PC-0010024-18-01
Safety Manual	Emerson document no. DOC.SILM.EF.EN

### 3 STATUS OF THE DOCUMENT

History: R 00: Initial release  
Release status: Released to client  
Author(s): Carlo Tarantola

Date: 2018-08-07

## ANNEX A - EXAMPLES OF $PFD_{AVG}$ CALCULATIONS

Type: F - No PST – Safety function: 1

Proof test interval (months)				
6	12	24	36	48
5,64E-05	1,12E-04	2,24E-04	3,36E-04	4,47E-04

Type: F - With PST – Safety function: 1

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	1,41E-05	1,91E-05	2,92E-05	3,92E-05	4,93E-05
	2	2,26E-05	2,76E-05	3,76E-05	4,77E-05	5,77E-05
	3	3,10E-05	3,61E-05	4,61E-05	5,62E-05	6,62E-05
	6		6,15E-05	7,15E-05	8,16E-05	9,16E-05
	9				1,07E-04	
	12			1,22E-04	1,32E-04	1,42E-04

### NOTES:

- The above values of  $PFD_{AVG}$  are calculated for  $MRT=24$  h and proof test coverage=100%. For other values of  $MRT$ ,  $TI$ ,  $TIPs$  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
$\beta, \beta_D$	Beta common cause factor
$\lambda_{BB}$	“Black Box” Failure rate – Literature data
$\lambda_D$	Failure rate of dangerous failures
$\lambda_{DD}$	Failure rate of detected dangerous failures
$\lambda_{DU}$	Failure rate of undetected dangerous failures
$\lambda_{NE}$	Failure rate of no effect failures
$\lambda_S$	Failure rate of safe failures
$\lambda_{SS}$	“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.



# C E R T I F I C A T E

**Certificate no. 18-SIL-0010024-03-TIC**

WE HEREBY CERTIFY THAT

*Product description*

**EL-O-MATIC™ PNEUMATIC RACK AND PINION SPRING  
RETURN ACTUATORS**

*Models*

**SERIES F (from size 0950 up to and including size 4000)**

*Manufacturer*

**EMERSON AUTOMATION SOLUTIONS**

**Valve Automation, Inc.**

**19200 NW Freeway**

**Houston, TX 77065**

**USA**

IS IN COMPLIANCE WITH THE REQUIREMENTS OF THE STANDARDS

**IEC 61508 Parts 1–7:2010**

AS RESULT OF THE ASSESSMENT ACCORDING TO THE PROVISION  
SET OUT IN THE ABOVE-MENTIONED STANDARDS

*Summary Report no.* **RC-0120-SIL-TIC-PC-0010024-18-02**

*Expiry date* **29.01.2023**

**Note**

This certificate is issued upon the request of the manufacturer as voluntary certification; it does not include the production surveillance.

This certificate does not allow the manufacturer to use the safety mark of TÜV INTERCERT.

Reggio Emilia, 30.01.2020



Dipl. Ing. Feridoon Sergizzarea

TÜV INTERCERT Certification Body



# C E R T I F I C A T E

**ANNEX to Certificate no. 18-SIL-0010024-03-TIC**

Type	A
HFT	0
Safety functions	1. Delivery of a full stroke (90° ± tolerance) driven by the spring, with power fluid exhausted from the cylinder through the control system
Mode of operation	Low Demand Mode

Random failure rates				
Configuration	Safety function	$\lambda_{DU}$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_S$ [1/h]
F - No PST	1	2,61E-08	0,00E+00	0,00E+00
F - With PST	1	2,34E-09	2,37E-08	0,00E+00

Systematic capability	3 (Route 1 <sub>S</sub> applied)			
Architectural constraints	Route 1 <sub>H</sub> :	Applied	Route 2 <sub>H</sub> :	Applied
	The product can be used in:			
	<ul style="list-style-type: none"> <li>single channel configuration:                             <ul style="list-style-type: none"> <li>up to SIL 2 without external diagnostic tests</li> <li>up to SIL 3 considering external diagnostic tests</li> </ul> </li> <li>double channel configuration: up to SIL 3</li> </ul>			

**Remarks:**

- For further details, including environmental conditions, limitations of use, lifetime, failure rates traceability, mean repair times, common cause factors and systematic capability constraints, make reference to Safety Manual DOC.SILM.EF.EN.

END OF CERTIFICATE

Reggio Emilia, 30.01.2020

  
Dipl. Ing. Feridoon Sergizzarea

TÜV INTERCERT Certification Body



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

Report no.: RC-0120-SIL-TIC-PC-0010024-18-02

## **SIL SUMMARY REPORT**

**IEC 61508-1/7:2010**

**EL-O-Matic™ pneumatic rack and pinion spring  
return actuators**

**Series F**

**(from size 0950 up to and including size 4000)**

**Emerson Automation Solutions  
Valve Automation, Inc.  
19200 NW Freeway  
Houston, TX 77065  
USA**

Date: **2020-01-27**

Place: **Reggio Emilia**

Author  
Carlo Tarantola

A handwritten signature in black ink, appearing to read 'Carlo Tarantola', written over a horizontal line.

**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:

EL-O-Matic™ pneumatic rack and pinion spring return actuators series F (from size 0950 up to and including size 4000)

### NOTES:

- This report is related to the assessment of EL-O-Matic™ pneumatic rack and pinion spring return actuators series F from size 0950 up to and including size 4000.
- The results of this report can be used for the assessment of a complete Safety Instrumented System.

## 2 ASSESSMENT AND RESULTS

Product identification		
Device	EL-O-Matic™ pneumatic rack and pinion spring return actuators	
Series	F	
Models / configurations	F - No PST F - With PST	
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)	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	<p>The assessment of the design included the following aspects:</p> <ul style="list-style-type: none"> <li>Quantifiable aspects: random failure rates, DC, SFF, PFD<sub>AVG</sub>, <math>\beta</math> factors, MRT, PTC, architectural constraints</li> <li>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</li> </ul> <p>See below for the results.</p>
Verification and Validation	Assessed	The verification and validation activities performed by the manufacturer include review, analysis and tests.
Information for use	Assessed	<p>The assessment covers:</p> <ul style="list-style-type: none"> <li>the installation, operation and maintenance instructions (IOM Manual)</li> <li>the particular instructions required by Annex D of IEC 61508 Part 2 (Safety Manual)</li> </ul>
Modification	Assessed	Procedures for modification activity are described in specific documents, referenced in the safety planning.
<b>Results</b>		
Selected assessment routes	<ul style="list-style-type: none"> <li>For architectural constraints: Routes 1<sub>H</sub> and 2<sub>H</sub></li> <li>For Systematic Capability: Route 1<sub>S</sub></li> </ul> <p>Furthermore, the requirements in paragraphs 7.4.10.1–7.4.10.7 of IEC 61508 Part 2 are assessed and considered fulfilled, as:</p> <ul style="list-style-type: none"> <li>the product has a restricted and specified functionality and is designed to perform specified safety functions</li> <li>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</li> <li>the manufacturer has an effective system for reporting failures</li> </ul>	
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	$\lambda_{DU}$ [1/h]	$\lambda_{DD}$ [1/h]	$\lambda_S$ [1/h]
F - No PST	1	2,61E-08	0,00E+00	0,00E+00
F - With PST	1	2,34E-09	2,37E-08	0,00E+00
Spurious trip rate	3,77E-09 [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 be possible via external means, e.g. with a PST. The procedure for the PST is described in the Safety Manual.			
SFF	Considering that $\lambda_S=0$ , according to definitions 3.6.15 of IEC 61508 Part 4: <ul style="list-style-type: none"> <li>SFF=0 without external diagnostic tests</li> <li>SFF&gt;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</li> </ul>			
PFD <sub>AVG</sub>	As the PFD <sub>AVG</sub> 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 <sub>AVG</sub> values are not product relevant quantities, while $\lambda$ values are. Anyway, PFD <sub>AVG</sub> values are calculated for a certain number of combination of test intervals. See Annex A.			
$\beta$ factors	$\beta=\beta_D=0,05$ <ul style="list-style-type: none"> <li>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.</li> <li>The above value is calculated in the hypothesis of redundancy without diversity</li> </ul> The $\beta$ factors can be used when performing PFD <sub>AVG</sub> calculations for redundant architectures.			
MRT	1 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: <ul style="list-style-type: none"> <li>single channel configuration: <ul style="list-style-type: none"> <li>up to SIL 2 without external diagnostic tests</li> <li>up to SIL 3 considering external diagnostic tests</li> </ul> </li> <li>double channel configuration: up to SIL 3</li> </ul>			

Expected lifetime	10 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.
<b>Remarks</b>	
<ul style="list-style-type: none"> <li>The random failure rates in the above table are valid for all the possible configurations of the product.</li> <li>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, <b><math>\lambda_S=0</math> for each type of single acting actuator.</b></li> <li>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.</li> <li>The <math>\lambda_S</math> values are not divided in <math>\lambda_{SD}</math> and <math>\lambda_{SU}</math>, as this subdivision has no relevance for any of the SIL parameters.</li> <li>For further details, make reference to the Safety Manual.</li> </ul>	
<b>Reference documents</b>	
SIL Assessment Report	TÜV INTERCERT document no. RC-0120-SIL-TIC-PC-0010024-18-01
Safety Manual	Emerson document no. DOC.SILM.EF.EN

### 3 STATUS OF THE DOCUMENT

History: R 00: Initial release  
Release status: Released to client  
Author(s): Carlo Tarantola

Date: 2020-01-27

## ANNEX A - EXAMPLES OF $PFD_{AVG}$ CALCULATIONS

Type: F - No PST – Safety function: 1

Proof test interval (months)				
6	12	24	36	48
5,77E-05	1,15E-04	2,29E-04	3,43E-04	4,57E-04

Type: F - With PST – Safety function: 1

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	1,44E-05	1,95E-05	2,98E-05	4,01E-05	5,04E-05
	2	2,31E-05	2,82E-05	3,85E-05	4,87E-05	5,90E-05
	3	3,17E-05	3,69E-05	4,71E-05	5,74E-05	6,77E-05
	6		6,28E-05	7,31E-05	8,34E-05	9,36E-05
	9				1,09E-04	
	12			1,25E-04	1,35E-04	1,46E-04

### NOTES:

- The above values of  $PFD_{AVG}$  are calculated for  $MRT=24$  h and proof test coverage=100%. For other values of  $MRT$ ,  $TI$ ,  $TIPs$  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
$\beta, \beta_D$	Beta common cause factor
$\lambda_{BB}$	“Black Box” Failure rate – Literature data
$\lambda_D$	Failure rate of dangerous failures
$\lambda_{DD}$	Failure rate of detected dangerous failures
$\lambda_{DU}$	Failure rate of undetected dangerous failures
$\lambda_{NE}$	Failure rate of no effect failures
$\lambda_S$	Failure rate of safe failures
$\lambda_{SS}$	“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.