

---

**Test Report No.:** FS 28717071

**Version-No.:** 1

**Date:** 2017-08-03

**Product:** Spring return and double acting pneumatic rack and pinion actuator

**Model:** Series FieldQ

**Customer/Manufacturer:** **Emerson Automation Solutions**  
Asveldweg 11  
7556 BR Hengelo  
The Netherlands

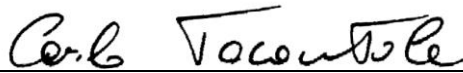
**Order No. / Date:** Emerson order dated 2017-02-10

**Test Specifications:** IEC 61508: 2010 Part 1÷7  
Functional Safety of Electrical/Electronic/Programmable Electronic  
Safety Related Systems

**Test Institute:** **TÜV Rheinland Italia S.r.l.**  
Via Enrico Mattei, 3  
20010 Pogliano Milanese (MI)

**Author:** Carlo Tarantola

(Signature)



---

*This document is only valid in its entirety and separation of any part is not allowed.*

---

## INDEX

<b>1</b>	<b>PURPOSE AND SCOPE.....</b>	<b>3</b>
<b>2</b>	<b>REFERENCE DOCUMENTS.....</b>	<b>4</b>
2.1	STANDARDS.....	4
2.2	DATABASES .....	4
<b>3</b>	<b>INSPECTION DOCUMENTS.....</b>	<b>4</b>
3.1	DOCUMENTATION PROVIDED BY THE CUSTOMER.....	4
3.2	DOCUMENTATION GENERATED BY TÜV RHEINLAND .....	4
<b>4</b>	<b>ABBREVIATIONS.....</b>	<b>5</b>
<b>5</b>	<b>DESCRIPTION OF PRODUCT .....</b>	<b>6</b>
5.1	SCOPE OF CALCULATION / TYPES .....	6
5.2	ARCHITECTURE .....	6
5.3	CLASSIFICATION .....	6
<b>6</b>	<b>SAFETY FUNCTION(S) .....</b>	<b>7</b>
<b>7</b>	<b>DETERMINATION OF RANDOM FAILURE RATES .....</b>	<b>8</b>
7.1	PROCEDURE.....	8
7.2	ASSUMPTIONS.....	8
7.3	DESCRIPTION OF THE FAILURE CATEGORIES .....	9
7.4	DETERMINATION OF NUMERICAL VALUES .....	10
<b>8</b>	<b>OVERALL RESULT.....</b>	<b>11</b>
<b>9</b>	<b>STATUS OF THE DOCUMENT .....</b>	<b>14</b>
<b>ANNEX A</b>	<b>DRAWINGS, PARTS LISTS.....</b>	<b>15</b>

---

## **FAILURE RATES CALCULATION REPORT OF SPRING RETURN AND DOUBLE ACTING PNEUMATIC RACK AND PINION ACTUATORS**

### **1 PURPOSE AND SCOPE**

This report summarises the results of a failure rates evaluation of spring return and double acting pneumatic rack and pinion actuators series FieldQ.

An evaluation is performed, according to IEC 61508-2, to evaluate the  $\lambda$  values (random HW failure rates) of the product.

The random HW failure rates evaluation according to IEC 61508-2 is only one of the steps to be taken to achieve functional safety certification according to IEC 61508 of a device.

For full functional safety certification purposes all the requirements of IEC 61508 (Part 1÷7) shall be considered.

#### **NOTES:**

- The elements of the control panel are not part of the assessment.

## 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: 2016 Part 1÷3	Functional Safety – Safety Instrumented Systems for the process industry sector

### 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 INSPECTION DOCUMENTS

### 3.1 Documentation provided by the customer

No.	Reference	Title
[D1]	Emerson drawing no. VA-ED-003- 2440 Rev. 00	General assembly FieldQ QS350/QD350
[D2]	Emerson drawing no. VA-ED-003- 2491 Rev. 00	General assembly FieldQ QS600/QD600
[D3]	Emerson letter dated 2017-08-01	FMEDA results range expansion

### 3.2 Documentation generated by TÜV Rheinland

No.	Reference	Title
[R1]	17029 – FS 28717071	Random failure analysis

## 4 ABBREVIATIONS

$\beta$	Beta common cause factor
$\lambda_{NE}$	Failure rate of no effect failures
$\lambda_D$	Failure rate of dangerous failures
$\lambda_{DU}$	Failure rate of undetected dangerous failures
$\lambda_{DD}$	Failure rate of detected dangerous failures
$\lambda_S$	Failure rate of safe failures
$\lambda_{SU}$	Failure rate of undetected safe failures
$\lambda_{SD}$	Failure rate of detected safe failures
DC	Diagnostic Coverage factor
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect 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
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TI	Test Interval for Proof Test (Full-Stroke)
$TI_D$ ( $TI_{PS}$ )	Test Interval for Diagnostic Test (Partial-Stroke)
Type A element	"Non-Complex" element (using discrete components)
Type B element	"Complex" element (using micro controllers or programmable logic)

---

## 5 DESCRIPTION OF PRODUCT

### 5.1 Scope of calculation / types

This report is related to spring return and double acting pneumatic rack and pinion actuators series FieldQ.

Detailed information are included in [D1] and [D2].

### 5.2 Architecture

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

### 5.3 Classification

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

#### NOTES:

- The classification refers to the actuator itself. The classification remains Type A even in case the valve-actuator 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 SAFETY FUNCTION(S)

The safety function is defined as follows:

- a. *When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, drives the actuator to close the shut-down valve, venting air via the control system; or*
- b. *When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, drives the actuator to open the blow-down valve, venting air via the control system.*

### NOTES:

- Considering the functioning of the actuator to perform the safety function(s), the two safety functions can be considered equivalent.
- In case of spring return actuator, the safety action is always performed by the spring.

The choice of the safety function to be implemented is responsibility of the system integrator.

## 7 DETERMINATION OF RANDOM FAILURE RATES

### 7.1 Procedure

The determination of random failure rates is performed with a Failure Modes, Effects and Diagnostic Analysis (FMEDA), integrated with field feedback, according to the approach of IEC 61508-2 par. 7.4.4.3.3, using the Bayesian approach.

The FMEDA is based on the documentation (drawings with components lists) provided by the Manufacturer and is documented in [R1].

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

1. FMEDA of the product, with classification of failure modes (see the failure categories in subclause 10.3 of the present document)
2. Evaluation of  $\lambda_{BB}$  values (literature data)
3. Evaluation of field feedback
4. Integration between literature data and field feedback, using the Bayesian approach

### 7.2 Assumptions

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

- Failure rates are considered constant for the lifetime.
- 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.
- 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  $PFD_{AVG}$  is calculated in the hypothesis of perfect proof test performed by trained, skilled and competent personnel. See also the remarks in par. 8.
- The “rate” of systematic failures is controlled and minimised by the management of the safety lifecycle of the system.
- The installation, commissioning, operational and maintenance instruction are correctly applied by the final customer.
- The stress levels considered are average for an industrial environment (ground fixed).



### 7.3 Description of the failure categories

In order to judge the failure behaviour of the product, the following definitions for the failure of the product were considered:

Safe Failure	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: <ul style="list-style-type: none"> <li>a. results in the spurious operation of the safety function; or</li> <li>b. increases the probability of the spurious operation of the safety function</li> </ul>
Dangerous Failure	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: <ul style="list-style-type: none"> <li>a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode); or</li> <li>b. decreases the probability that the safety function operates correctly when required</li> </ul>
No Effect Failure	Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function
No Part Failure	Failure of a component that plays no part in implementing the safety function

#### GENERAL NOTES:

1. Failures of components of the pneumatic chamber 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 61508-4)
2. According to definitions 3.6.13 and 3.6.14 of IEC 61508-4, the no part and no effect failures are not used for SFF calculations.
3. According to definitions 3.6.8, 3.6.13, 3.6.14 of IEC 61508-4, the safe, no part and no effect failures do not contribute to  $PFD_{AVG}$  calculations.

#### SPECIFIC NOTES:

1. According to the above definitions (in particular definitions 3.6.8 and 3.6.13 of IEC 61508-4), 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 “plays no part in implementing the safety function”, e.g. components of the pneumatic chamber, and so, according to definition 3.6.13 of IEC 61508-4, they cannot be used for the calculation of the SFF): hence  **$\lambda_S=0$  for each type of Single Acting actuator.**
2. According to the above definitions (in particular definitions 3.6.8 and 3.6.13 of IEC 61508-4), 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  **$\lambda_S=0$  for each type of Double Acting actuator.**
3. For this reason, according to definitions 3.6.15 of IEC 61508-4 we have:
  - $SFF=0$  without external diagnostic tests
  - $SFF>0$  with external diagnostic tests according to definition 3.8.7 of IEC 61508-4

## 7.4 Determination of numerical values

### FMEDA

The FMEDA was performed according to the following procedure:

- a. complete definition of the product;
- b. identification of all potential items and their failure modes;
- c. evaluation of each potential failure mode in terms of end system effect;
- d. identification of the failure detection methods and compensating provisions for each failure mode (if possible);
- e. association of a Failure Category to each failure mode.
- f. association of a Failure Rate / Failure Distribution to each item / Failure Mode.

The complete FMEDA is included in documents [R1].

### Classification of failures

Each single failure mode was classified, in document [R1], according to the description of the failure categories included in subclause 7.3 of the present document.

### Evaluation of $\lambda$ values, of SFF and $PFD_{AVG}$

#### Evaluation of $\lambda$ values

The complete calculations for the evaluation of  $\lambda$  values are included in document [R1].

#### Evaluation of SFF

The formula for SFF is the following:

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

#### Evaluation of $PFD_{AVG}$

According to document [N1], the following formula is used to estimate the  $PFD_{AVG}$  value:

$$PFD_{AVG} = \lambda_{DU} \cdot \left( \frac{TI}{2} + MRT \right) + \lambda_{DD} \cdot \left( \frac{TI_D}{2} + MRT \right)$$

## 8 OVERALL RESULT

The analysis gives the results summarised in the following Tables.

Series	$\lambda_D$ [1/h]	$\lambda_{DD(PST)}$ [1/h]
QS40, QS65, QS100, QS150, QS200, QS350	9,54E-08	8,68E-08
QD40, QD65, QD100, QD150, QD200, QD350	9,07E-08	8,50E-08
QS600, QS950, QS1600	9,34E-08	8,25E-08
QD600, QD950, QD1600	9,13E-08	8,31E-08

Table 1: Dangerous failure rates

### SPECIFIC NOTES:

1. In case of double acting actuators, the internal chamber is considered for safety action.
2. According to the definitions 3.6.8 and 3.6.13 of IEC 61508-4, 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 "plays no part in implementing the safety function", e.g. components of the pneumatic chamber, and so, according to definition 3.6.13 of IEC 61508-4, they cannot be used for the calculation of the SFF): hence  **$\lambda_S=0$  for each type of Single Acting actuator.**
3. According to the definitions 3.6.8 and 3.6.13 of IEC 61508-4, 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  **$\lambda_S=0$  for each type of Double Acting actuator.**
4. For this reason, according to definitions 3.6.15 of IEC 61508-4 we have:
  - SFF=0 without external diagnostic tests
  - SFF>0 with external diagnostic tests, carried out according to definition 3.8.7 of IEC 61508-4

Test Interval Frequency (months)				
6	12	24	36	48
2,11E-04	4,20E-04	8,38E-04	1,26E-03	1,67E-03

Table 2a:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (no Partial Stroke Test)  
– Models QS40, QS65, QS100, QS150, QS200, QS350

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	5,28E-05	7,16E-05	1,09E-04	1,47E-04	1,84E-04
	2	8,45E-05	1,03E-04	1,41E-04	1,78E-04	2,16E-04
	3	1,16E-04	1,35E-04	1,73E-04	2,10E-04	2,48E-04
	6		2,30E-04	2,68E-04	3,05E-04	3,43E-04
	9				4,00E-04	
	12			4,58E-04	4,95E-04	5,33E-04

Table 2b:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (with Partial Stroke Test)  
– Models QS40, QS65, QS100, QS150, QS200, QS350

Test Interval Frequency (months)				
6	12	24	36	48
2,01E-04	3,99E-04	7,97E-04	1,19E-03	1,59E-03

Table 3a:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (no Partial Stroke Test)  
– Models QD40, QD65, QD100, QD150, QD200, QD350

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	5,17E-05	7,01E-05	1,07E-04	1,44E-04	1,81E-04
	2	8,27E-05	1,01E-04	1,38E-04	1,75E-04	2,12E-04
	3	1,14E-04	1,32E-04	1,69E-04	2,06E-04	2,43E-04
	6		2,25E-04	2,62E-04	2,99E-04	3,36E-04
	9				3,92E-04	
	12			4,48E-04	4,85E-04	5,22E-04

Table 3b:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (with Partial Stroke Test)  
– Models QD40, QD65, QD100, QD150, QD200, QD350

Test Interval Frequency (months)				
6	12	24	36	48
2,07E-04	4,12E-04	8,21E-04	1,23E-03	1,64E-03

Table 4a:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (no Partial Stroke Test)  
– Models QS600, QS950, QS1600

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	5,02E-05	6,81E-05	1,04E-04	1,40E-04	1,75E-04
	2	8,03E-05	9,82E-05	1,34E-04	1,70E-04	2,05E-04
	3	1,10E-04	1,28E-04	1,64E-04	2,00E-04	2,36E-04
	6		2,19E-04	2,54E-04	2,90E-04	3,26E-04
	9				3,81E-04	
	12			4,35E-04	4,71E-04	5,07E-04

Table 4b:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (with Partial Stroke Test)  
– Models QS600, QS950, QS1600

Test Interval Frequency (months)				
6	12	24	36	48
2,02E-04	4,02E-04	8,02E-04	1,20E-03	1,60E-03

Table 5a:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (no Partial Stroke Test)  
– Models QD600, QD950, QD1600

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	5,05E-05	6,85E-05	1,05E-04	1,41E-04	1,77E-04
	2	8,08E-05	9,88E-05	1,35E-04	1,71E-04	2,07E-04
	3	1,11E-04	1,29E-04	1,65E-04	2,01E-04	2,37E-04
	6		2,20E-04	2,56E-04	2,92E-04	3,28E-04
	9				3,83E-04	
	12			4,38E-04	4,74E-04	5,10E-04

Table 5b:  $PFD_{AVG}$  values according to IEC 61508 for different values of TI (with Partial Stroke Test)  
– Models QD600, QD950, QD1600

NOTES:

- The above values of  $PFD_{AVG}$  are calculated for MRT=24 h and Proof Test Coverage=100%. For other values of MRT, TI,  $T_{ID}$  and/or non-perfect Proof Test, the  $PFD_{AVG}$  values must be re-calculated.

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

---

## 9 STATUS OF THE DOCUMENT

History:	R 1:	Modification of par. 8 according to customer's request:	Date: 2017-08-03
		<ul style="list-style-type: none"><li>• Inclusion of list of models</li><li>• Inclusion of PFD<sub>AVG</sub> results with Partial Stroke Test</li></ul>	
	R 0:	Initial release	Date: 2017-06-29
Release status:	Released to client		
Author(s):	Carlo Tarantola		

---

## **ANNEX A DRAWINGS, PARTS LISTS**

