Failure Modes, Effects and Diagnostic Analysis

Project:
El-O-Matic P-Series Pneumatic Rack & Pinion Actuators

Customer:
Emerson Valve Automation Division
Tampa, FL
USA

Contract No.: Q03/08-24r3
Report No.: VAD 03/08-24 R004
Version V1, Revision R2, November 1, 2005

Rachel Amkreutz - Lindsey Bredemeyer

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the El-O-Matic P-Series pneumatic rack & pinion, quarter turn, actuators. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety assessment per IEC 61508 of a device. From the FMEDA, a full set of failure rates is determined. For full functional safety assessment purposes all requirements of IEC 61508 must be considered.

The El-O-Matic P-Series pneumatic actuators are classified as Type A[1] devices, with a hardware fault tolerance of 0. The failure rates for the device are listed in Table 1.

Table 1 Failure rates El-O-Matic P-Series actuator

Failure category	Failure rate (in FIT)	
	Spring-Return	Double Acting
Fail Safe	80	0
Fail Dangerous Undetected	559	465
No Effect	1993	1265

The failure rates for the El-O-Matic P-Series pneumatic actuator when performing partial valve stroke testing are listed in Table 2.

Table 2 Failure rates El-O-Matic P-Series actuator with partial valve stroke testing

Failure category	Failure rate (in FIT)	
	Spring-Return	Double Acting
Fail Safe	80	0
Fail Dangerous Detected	370	256
Fail Dangerous Undetected	189	209
No Effect	1993	1265

Note that the "No Effect" failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful lifetime of the product. A user of the El-O-Matic P-Series pneumatic actuators can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

[1] Type A component: "Non-Complex" component with well-defined failure modes, for details see 7.4.3.1.2 of IEC 61508-2.

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition, this option consists of an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing (programmable electronic) devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the El-O-Matic P-Series pneumatic actuators. From this, failure rates and example PFD_{AVG} values are calculated.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

El-O-Matic International	Manufacturer of the El-O-Matic P-Series actuator
exida.com	Project leader of the FMEDA

Emerson Valve Automation Division contracted *exida.com* in December 2004 with the FMEDA of the above mentioned device.

2.3 Standards / Literature used

The services delivered by *exida.com* were performed based on the following standards / literature.

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N5]	Safety Equipment Reliability Handbook, 2003	exida.com L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N6]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	DOC.BR.E, 09.01	El-O-Matic brochure
[D2]	DOC 4.1 EDN, 99.08	El-O-Matic Operation & Installation

2.4.2 Documentation generated by *exida.com*

[R1]	Exida09 FMEDA1 Rev0.xls, 01/31/05	Failure Modes, Effects and Diagnostic Analysis, El-O-Matic P-Series pneumatic actuator
[R2]	VAD 03-08-24 R004 V1 R2.doc, 01/11/05	FMEDA report, El-O-Matic P-Series pneumatic actuator (this report)

3 Product Description

The Failure Modes, Effects and Diagnostic Analysis (FMEDA) is performed for the Emerson El-O-Matic P-Series pneumatic actuators. These are pneumatic rack and pinion actuators for application to ball, plug and butterfly valves. They can also be used in other quarter turn applications, such as dampers and pressure regulators. The actuators are made of high duty aluminium alloys, providing optimum strength and corrosion resistance. The actuator has a compact rack & pinion design and comes in two sizes.

Actuators with double stroke adjustment are also available for those applications on high performance butterfly valves (closed position).

The following versions were considered during the FMEDA.

- El-O-Matic P-Series pneumatic spring-return actuator
- El-O-Matic P-Series pneumatic double acting actuator

The El-O-Matic P-Series pneumatic actuators are classified as a Type A[2] devices according to IEC 61508. The hardware fault tolerance of the device is 0.

[2] Type A component: "Non-Complex" component with well-defined failure modes, for details see 7.4.3.1.3 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the information received from El-O-Matic and is documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the El-O-Matic P-Series pneumatic actuators, the following definitions for the failure of the product were considered.

Fail-Safe State	State where hold-open air is released and the spring is extended. (Spring-return option)
	State where air pressure is vented from pinion space and air pressure is applied to the cap space (Double Acting option).
Fail Safe	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that prevents the actuator from rotating with sufficient torque to move a valve to its fail-safe state.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by partial valve stroke testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by partial valve stroke testing.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2000, the No Effect failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA is from a proprietary mechanical component failure rate database derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class D (Outdoor Locations). It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the El-O-Matic P-Series pneumatic actuator.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Partial valve stroke testing is performed at a rate at least ten times faster than the expected demand rate.
- Partial valve stroke testing of the SIF includes position detection from actuator top mounted position sensors, typical of quarter turn installations.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The stress levels are average for an industrial outdoor environment and can be compared to IEC 60654-1, Class Dx (outdoor location) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Materials are compatible with process conditions.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- Actuator is installed per manufacturer's instructions.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis
- Failure rates for the double acting actuator do not include failure of the air supply

4.4 Results El-O-Matic P-Series Pneumatic Actuator

Using reliability data extracted from the exida.com component reliability database the following failure rates resulted from the actuator FMEDA.

Table 3 Failure rates El-O-Matic P-Series pneumatic actuator

Failure category	Failure rate (in FIT)	
	Spring-Return	Double Acting
Fail Safe	80	0
Fail Dangerous Undetected	559	465
No Effect	1993	1265

The failure rates for the El-O-Matic P-Series pneumatic actuator when performing partial valve stroke testing are listed in Table 4.

Table 4 Failure rates El-O-Matic P-Series pneumatic actuator with partial valve stroke testing

Failure category	Failure rate (in FIT)	
	Spring-Return	Double Acting
Fail Safe	80	0
Fail Dangerous Detected	370	256
Fail Dangerous Undetected	189	209
No Effect	1993	1265

The actuator is classified as a Type A component according to IEC 61508. The hardware fault tolerance of the device is 0. The SFF and required SIL of the Safety Instrumented Function determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5 Using the FMEDA results

5.1 Double Acting Actuator

When using the double acting El-O-Matic P-Series Actuator option in Safety Instrumented Functions, failure of the air supply should be included in the average Probability of Failure on Demand (PFD_{AVG}) calculation of the Safety Instrumented Function. If an accumulator system is used to protect against air supply failure, the accumulator subsystem needs to be reviewed and the dangerous failure rates of the accumulator subsystem should be added to the actuator failure rates.

5.2 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) El-O-Matic P-Series Spring-Return actuator. The failure rate data used in this calculation is displayed in section 4.4. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} values for a single El-O-Matic P-Series Spring-Return actuator with and without Partial Valve Stroke Testing (PVST) are shown. The PFD_{AVG} for a single El-O-Matic P-Series pneumatic Spring-Return actuator, without Partial Valve Stroke Testing, with a proof test interval of 1 year equals 2.44E-03.

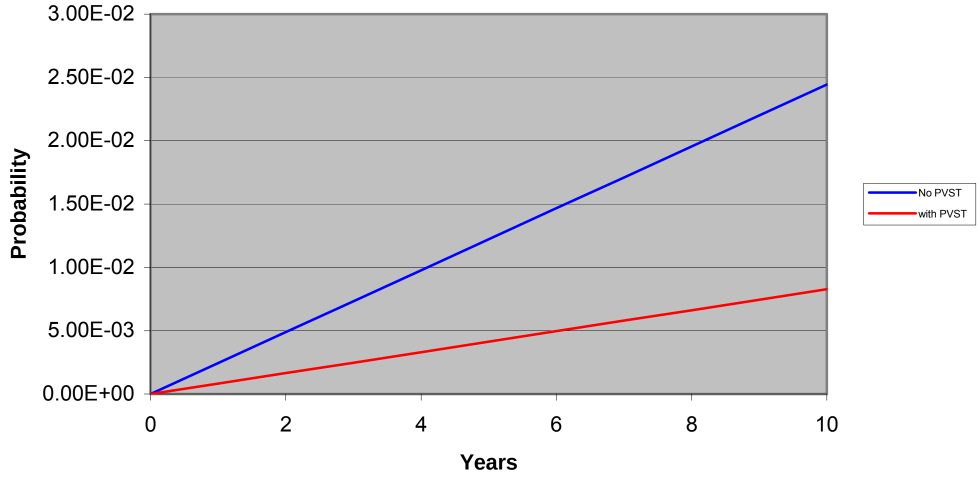

Figure 1: PFD_{AVG}(t) El-O-Matic P-Series pneumatic Spring-Return actuator

The values are intended as a rough approximation only. It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. Exida recommends the accurate Markov based SILver tool for this purpose. For SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application without partial valve stroke testing, the PFD_{AVG} for a 1-year Proof Test Interval of the El-O-Matic P-Series Spring-Return actuator is approximately equal to 24% of the range.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	"Non-Complex" component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	"Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version:	V1	
Revision:	R2	
Version History:	V1, R2:	Data update based on field experience; November 1, 2005
	V1, R1:	Internal draft; February 4, 2005
	V0, R1:	Internal draft; February 3, 2005
Authors:	Rachel Amkreutz - Lindsey Bredemeyer	
Review:	V0, R1:	Rachel Amkreutz (exida.com); February 4, 2005
	V1, R1:	Emerson Valve Automation Division; October 2005
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dr. William M. Goble, Principal Partner

Lindsey Bredemeyer, Product Analyst

Ir. Rachel Amkreutz, Safety Engineer

Appendix A Useful life

It is the responsibility of the end user to maintain and operate the actuator per manufacturer's instructions. A major factor influencing the useful life is the air quality. Furthermore regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 20 years is expected for the El-O-Matic P-Series pneumatic actuators.