Failure Modes, Effects and Diagnostic Analysis

Project:
Rotex DRS, ECF and SSF Series Valve Actuators

Company:
Rotex Manufacturers & Engineers Private Limited
Dombivli, Maharashtra
India

Contract Number: Q10/04-018
Report No.: ROT 10/04-018 R001
Version V1, Revision R2, November 3, 2011
Gregory Sauk

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Rotex DRS, ECF and SSF Series Valve Actuators. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Rotex DRS, ECF and SSF Series Valve Actuators. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The DRS Valve Actuator Series is a line of heavy duty Pneumatic or Hydraulic Scotch Yoke Valve Actuators. The ECF/SSF Series Valve Actuator is a line of double Rack and Pinion Valve Actuators.

Table 1 lists the versions of the Rotex DRS, ECF and SSF Series Valve Actuators that have been considered for the hardware assessment.

Table 1 Version Overview

DRS Series	DRS Frame Sizes AA to M, Spring Return Scotch Yoke Actuators
DRS Series	DRS Frame Sizes AA to M, Double Acting Scotch Yoke Actuators
ECF Series	ECF/SSF - Sizes 32 to 350, Single Acting Rack and Pinion Actuators
ECF Series	ECF/SSF - Sizes 32 to 350, Double Acting Rack and Pinion Actuators

Failure rates for the DRS Series Valve Actuators are listed in Table 2 and for the ECF/SSF Series Valve Actuators in Table 3. Failure rates are listed both with and without Partial Valve Stroke Testing (PVST).

Double Acting applications failure rates do not take into account the loss of the air supply to the Actuator.

Table 2 Failure Rates for DRS Series Valve Actuator in FIT

Failure Category	No PVST		With PVST	
	Spring Return (Single Acting)	Double Acting	Spring Return (Single Acting)	Double Acting
Fail Safe Detected	0	0	490	0
Fail Safe Undetected	490	0	0	0
Fail Dangerous Detected	0	0	331	570
Fail Dangerous Undetected	497	877	166	307
No Effect	975	758	975	758

Table 3 Failure Rates for ECF/SSF Series Valve Actuator in FIT

Failure Category	No PVST		With PVST	
	Spring Return (Single Acting)	Double Acting	Spring Return (Single Acting)	Double Acting
Fail Safe Detected	0	0	399	0
Fail Safe Undetected	399	0	0	0
Fail Dangerous Detected	0	0	165	283
Fail Dangerous Undetected	312	448	147	165
No Effect	468	697	468	697

The DRS and ECF/SSF Valve Actuators are classified as Type A[1] devices according to IEC 61508, having an internal hardware fault tolerance of 0.

The complete final element subsystem, of which a Rotex DRS, ECF or SSF Series Valve Actuator is a component of, will need to be evaluated to determine the Safe Failure Fraction.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 4 lists the failure rates for the Rotex DRS, ECF and SSF Series Valve Actuators according to IEC 61508, ed2, 2010 (see Appendix D for rates according to 2000 edition of IEC 61508).

Table 4 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
DRS Actuator, Spring Return	0	490	0	497	-
DRS Actuator, Spring Return w/PVST	490	0	331	166	-
DRS Actuator, Double Acting	0	0	0	877	-
DRS Actuator, Double Acting w/PVST	0	0	570	307	-
ECF/SSF Actuator, Spring Return,	0	399	0	312	-
ECF/SSF Actuator, Spring Return w/PVST	399	0	165	147	-
ECF/SSF Actuator, Double Acting	0	0	0	448	-
ECF/SSF Actuator, Double Acting w/PVST	0	0	283	165	-

[1] Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

[2] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

[3] Safe Failure Fraction needs to be calculated on (sub)system level

A user of the Rotex DRS, ECF and SSF Series Valve 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). A full table of failure rates is presented in section 4.4 along with all assumptions.

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* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. 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}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per 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* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Rotex DRS, ECF and SSF Series Valve Actuators. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a final element subsystem meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

2 Project Management

2.1 *exida*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rotex Manufacturers & Engineers	Manufacturer of the DRS, ECF/SSF Valve Actuators
exida	Performed the hardware assessment according to Option 1 (see Section 1)

Rotex Manufacturers & Engineers Private Limited contracted *exida* in Feburary 2011 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	exida LLC, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	EMCR Handbook, 2011 Update	exida LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	O'Brien, C. & Bredemeyer, L., 2009	exida LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

2.4 *exida* Tools used

[T1]	V2.5.1.7	*exida* exSILentia – Integrated Safety Lifecycle Tool

2.5 Reference documents

2.5.1 Documentation provided by Rotex Manufacturers & Engineers Private Limited

[D1]	DRS IOM, Rev 0, Oct 2010	Rotex DRSB to DRSM Pneumatic Actuator Service Instructions
[D2]	MI2-0710	Rotex DRS Series Scotch Yoke Actuators Brochure
[D3]	HPHDA-1110-M2-RO-MI, March 2011	Heavy Duty Actuators Catalog, High Flow Valves Product Brochure
[D4]	Actuator Models, Rev 1, 6/6/11	Models for Certification, Lists models to be certified and equivalencies for different markets
[D5]	ECF IOM, Rev 01, 4/1/08	IOM - ROTEX ECF Series ACTUATORS Installation Manual
[D6]	ECF-SSF, V3-1, April 2010	Rotex Rotary Actuator ECF/SSF Series Brochure

2.5.2 Documentation generated by *exida*

[R1]	Rotex DRS Actuator FMEDA R3.xls, 10/31/2011	Failure Modes, Effects, and Diagnostic Analysis – DRS and ECF/SSF Series Valve Actuator (internal document)
[R2]	ROT Q10-04-018 DRS-ECF Actuators FMEDA V1R2.doc, 11/03/2011	FMEDA report, Rotex DRS, ECF and SSF Series Valve Actuators (this report)

3 Product Description

3.1 DRS Series Valve Actuator

The Rotex DRS Valve Actuator Series is a line of heavy duty Pneumatic or Hydraulic Scotch Yoke Valve Actuators. They feature internal tie rods and hard chrome plated cylinders. They are available in both Single Acting (aka Spring Return) and Double Acting. Units can be easily converted from Double Acting to Single Acting in the field.

This analysis covers the DRS Series frame sizes AA to M and Pneumatic bore sizes of 63 to 1300mm. Figure 1 shows a typical Spring Return DRS Actuator that is covered in this report.

Figure 1: typical DRS Spring Return Valve Actuator

3.2 ECF/SSF Series Valve Actuator

The Rotex ECF Valve Actuator Series is a line of double Rack and Pinion Valve Actuators. The ECF series has an extruded Aluminum hard anodized body. These may be also be Single or Double Acting devices and will always consist of two Racks / Pistons. The SSF series is similarly constructed as the ECF except that they have a Stainless Steel body and end covers. The ECF series is also sold in the US and Canada as the ECV series (same but with imperial mounting pattern) and it is also included in this analysis. Figure 2 shows a typical Double Acting ECF Actuator that is covered in this report.

Figure 2: typical ECF Valve Actuator

The Rotex DRS, ECF and SSF Series Valve Actuators are classified as a Type A[4] device according to IEC 61508, having a hardware fault tolerance of 0.

Table 5 gives an overview of the different versions that were considered in the FMEDA of the Rotex DRS and ECF Series Valve Actuators.

Table 5 Version Overview

DRS Series	DRS Frame Sizes AA to M, Spring Return Scotch Yoke Actuators
DRS Series	DRS Frame Sizes AA to M, Double Acting Scotch Yoke Actuators
ECF Series	ECF/SSF - Sizes 32 to 350, Single Acting Rack and Pinion Actuators
ECF Series	ECF/SSF - Sizes 32 to 350, Double Acting Rack and Pinion Actuators

[4] Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Rotex Manufacturers & Engineers Private Limited and is documented in [R1].

4.1 Failure Categories description

In order to judge the failure behavior of the Rotex DRS and ECF Series Valve Actuators, the following definitions for the failure of the device were considered.

Fail-Safe State

Spring Return	State where hold position air is released and the spring is extended. (may also be referred to as Single Acting)
Double Acting	State where the hold position pressure is released and pressure is supplied to the trip side of the actuator.
Fail Safe	Failure that causes the Actuator and Valve to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by any automatic diagnostic.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics such as Partial Valve Stroke Testing.
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
External Leakage	Failure that causes the operating media to leak outside of the Actuator. External Leakage is not considered part of the safety function and therefore this failure rate is not included in the Safe Failure Fraction calculation.

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 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation.

External leakage failure rates do not directly contribute the reliability of an Actuator but should be reviewed for secondary safety and environmental issues if other than air is used as the operating media.

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.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the 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, etc.) 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* in this FMEDA are from the Electrical and Mechanical Component Reliability Handbook [N2] and [N3] which was 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 *exida* Profile 3. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application in all modes of operation.

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 Rotex DRS, ECF and SSF Series Valve Actuators.

- Only a single component failure will fail the entire Valve Actuator.

- Failure rates are constant, wear-out mechanisms are not included.
- 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 environment and can be compared to the *exida* Profile 3 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.
- The device 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 options do not include failure of the air supply.
- When used as an automated diagnostic, 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.
- Worst-case internal fault detection time is the time between automated PVST tests.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Rotex DRS, ECF and SSF Series Valve Actuators FMEDA. Table 6 lists the failure rates DRS Series Valve Actuator and in Table 7 for ECF/SSF Series Valve Actuator. Both the normal failure rates and the failure rates when performing Partial Valve Stroke Testing (PVST) as an automatic diagnostic are listed.

Table 6 Failure rates DRS Series Valve Actuator in FIT

Failure Category	No PVST		With PVST	
	Spring Return (Single Acting)	Double Acting	Spring Return (Single Acting)	Double Acting
Fail Safe Detected	0	0	490	0
Fail Safe Undetected	490	0	0	0
Fail Dangerous Detected	0	0	331	570
Fail Dangerous Undetected	497	877	166	307
No Effect	975	758	975	758

Table 7 Failure rates ECF/SSF Series Valve Actuator in FIT

Failure Category	No PVST		With PVST	
	Spring Return (Single Acting)	Double Acting	Spring Return (Single Acting)	Double Acting
Fail Safe Detected	0	0	399	0
Fail Safe Undetected	399	0	0	0
Fail Dangerous Detected	0	0	165	283
Fail Dangerous Undetected	312	448	147	165
No Effect	468	697	468	697

In addition to the failure rates listed above, the external leakage failure rate of the DRS Series Valve Actuator is 134 FIT for Spring Return devices, and 204 FIT for the Double Acting. The ECF/SSF Series Valve Actuator has 190 FIT for Spring Return, and 433 FIT for the Double Acting. The above listed No Effect rates already have these rates included as air is normally the operating media. In the event that air is not the operating media (for example natural gas is used), then the No Effect rate should be adjusted accordingly. External leakage failure rates do not directly contribute to the reliability of the Actuator but should be reviewed for secondary safety and environmental issues.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

Table 8 lists the failure rates for the Rotex DRS, ECF and SSF Series Valve Actuators according to IEC 61508, ed2, 2010. For reference purposes, a table listing the failure rates according to the previous 2000 edition of the standard is listed in Appendix D. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the DRS or ECF/SSF Series Valve Actuator is only one part of a (sub)system, the SFF should be calculated for the entire final element combination. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF:

$SFF = 1 - \lambda_{DU} / \lambda_{TOTAL}$

Where $\lambda_{TOTAL} = \lambda_{SD+} \lambda_{SU+} \lambda_{DD+} \lambda_{DU}$

Table 8 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
DRS Actuator, Spring Return	0	490	0	497	-
DRS Actuator, Spring Return w/PVST	490	0	331	166	-
DRS Actuator, Double Acting	0	0	0	877	-
DRS Actuator, Double Acting w/PVST	0	0	570	307	-
ECF/SSF Actuator, Spring Return,	0	399	0	312	-
ECF/SSF Actuator, Spring Return w/PVST	399	0	165	147	-
ECF/SSF Actuator, Double Acting	0	0	0	448	-
ECF/SSF Actuator, Double Acting w/PVST	0	0	283	165	-

The architectural constraint type for the Rotex DRS, ECF and SSF Series Valve Actuators is A. The hardware fault tolerance of the device is 0. The SFF and required SIL 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] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

[6] Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The following sections describe how to apply the results of the FMEDA.

5.1 Air quality failures

The product failure rates that are listed in this report are failure rates that reflect the situation where the device is used with clean filtered air. Contamination from poor control air quality may affect the function or air flow in the device. For applications where these assumptions do not apply, the user must estimate the failure rates due to the contaminated media and add this failure rate to the product failure rates.

5.2 PFD_{AVG} Calculation DRS Series Valve Actuator

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) DRS Series Valve Actuator with *exida's* exSILentia tool. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 96 hours. Table 9 lists the proof test coverage (see Appendix B) used for this configuration as well as the results when the proof test interval equals 1 year.

Table 9 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD_{AVG}	% of SIL 1 Range
DRS - Spring Return	93%	3.54E-03	3.5%
DRS – Spring Return w/PVST	78%	2.20E-03	2.2%

The resulting PFD_{AVG} Graph generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 3.

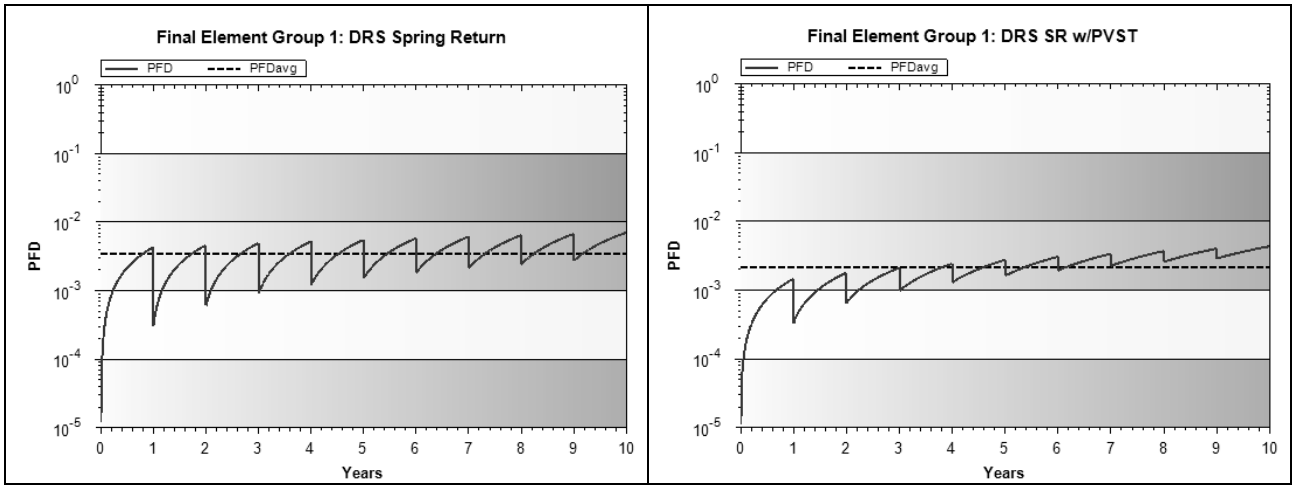


Figure 3 PFD_{AVG} value for a single, DRS Actuator with proof test intervals of 1 year

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the DRS Series Valve Actuator with automated PVST diagnostics is approximately equal to 2.2% 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 demand interval for operation made on a safety-related system is greater than twice the proof test interval
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequently than the proof test; therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus 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 element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* 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.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

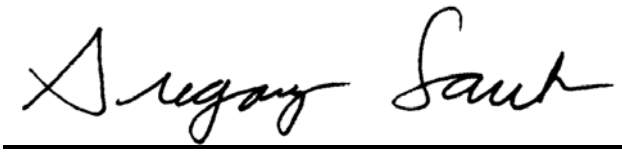
7.2 Releases

Version:	V1	
Revision:	R2	
Version History:	V1, R2:	Added smaller DRS sizes; November 3, 2011
	V1, R1:	Released to Rotex; October, 28 2011
	V0, R2:	Added ECF, SSF and ECV Actuators, October 27, 2011
	V0, R1:	Draft; July 21, 2011
Author(s):	Gregory Sauk	
Review:	V0, R2:	Steven Close (*exida*); October 28, 2011
	V0, R1:	Rudolf Chalupa (*exida*); July 22, 2011
Release Status:	Released to Rotex Manufacturers & Engineers Private Limited	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Gregory Sauk, CFSE, Safety Engineer

Dr. William M. Goble, Principal Partner

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[7] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is the responsibility of the end user to maintain and operate the Rotex Valve Actuator per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

A major factor influencing the useful life is the air quality.

Based on general field failure data a useful life period of approximately 10 to 15 years is expected for the Rotex DRS, ECF and SSF Series Valve Actuators.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[7] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof tests to reveal dangerous undetected faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested proof test consists of a full cycle of the Valve Actuator and Valve, see Table 10.

Table 10 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the air supply to the Actuator to force the Actuator and Valve to Fail-Safe state and confirm that the Safe State was achieved and within the correct time.
3.	Re-store the air supply to the Actuator and inspect the Actuator for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
4.	Remove the bypass and otherwise restore normal operation

For the test to be effective the movement of the Actuator and Valve must be confirmed. To confirm the effectiveness of the test both the travel of the Valve and slew rate must be monitored and compared to expected results to validate the testing.

B.2 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 11.

Table 11 Proof Test Coverage – DRS and ECF/SSF Series Valve Actuators

Device	No PVST	with PVST
DRS Series Valve Actuator - Spring Return	93%	78%
DRS Series Valve Actuator - Double Acting	91%	76%
ECF/SSF Series Valve Actuator - Spring Return	91%	82%
ECF/SSF Series Valve Actuator - Double Acting	91%	76%

Appendix C *exida* Environmental Profiles

Table 12 *exida* Environmental Profiles

EXIDA ENVIRONMENTAL PROFILE		GENERAL DESCRIPTION	PROFILE PER IEC 60654-1	AMBIENT TEMPERATURE [°C]		TEMP CYCLE [°C / 365 DAYS]
				AVERAGE (EXTERNAL)	MEAN (INSIDE BOX)	
1	Cabinet Mounted Equipment	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings	B2	30	60	5
2	Low Power /Mechanical Field Products	Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings	C3	25	30	25
3	General Field Equipment	General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings. Non-process wetted components of valves and actuators.	C3	25	45	25
4	Unprotected Mechanical Field Products	Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation. Process wetted components.	D1	25	30	35

Appendix D Failure Rates according to IEC 61508 2000 edition

The failure rates for the Rotex DRS, ECF and SSF Series Valve Actuators listed below in Table 13 are suitable for comparison purposes to other devices that only have rates disclosed based on the 2000 edition of IEC 61508. Note that calculating the SFF based on the higher λ_{SU} values listed below will result in a significantly higher SFF number for the complete final element subsystem. However the latest version of the standard no longer allows the No Effect failure rates to be included with the Safe Undetected category. The below numbers are not intended for use in currently calculating the SFF, and are only listed for comparison purposes with older failure rate tables of other devices.

Table 13 Failure rates according to IEC 61508 2000 edition in FIT

Device	λ_{SD}	λ_{SU}[8]	λ_{DD}	λ_{DU}	SFF[9]
DRS Actuator, Spring Return	0	1465	0	497	-
DRS Actuator, Spring Return w/PVST	490	975	331	166	-
DRS Actuator, Double Acting	0	758	0	877	-
DRS Actuator, Double Acting w/PVST	0	758	570	307	-
ECF/SSF Actuator, Spring Return,	0	867	0	312	-
ECF/SSF Actuator, Spring Return w/PVST	399	468	165	147	-
ECF/SSF Actuator, Double Acting	0	697	0	448	-
ECF/SSF Actuator, Double Acting w/PVST	0	697	283	165	-

[8] It is important to realize that the No Effect failures are included in the Safe Undetected failure category according to IEC 61508:2000 ed. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

[9] Safe Failure Fraction needs to be calculated on (sub)system level