



**Accurate Failure Metrics for Mechanical
Instruments in Safety Applications**

White Paper

exida

80 N. Main St.

Sellersville, PA

www.exida.com

October 2020

exida White Paper Library

<http://www.exida.com/Resources/Whitepapers>

Copyright exida.com L.L.C. 2018-2020



Keywords

FMEDA, PFD analysis, Safety Integrity Level verification, Final Elements, Safety Instrumented Systems

Abstract

Probabilistic calculations that are done to verify the integrity of a Safety Instrumented Function design require realistic failure rate and failure mode data of all equipment including the mechanical devices. For many devices, such data is only available in industry databases where only failure rates are presented. The failure mode information is rare, if available at all. Many give up and just say 50% safe and 50% dangerous thinking this is conservative. In some cases, this is not a conservative assumption.

Statistically significant quality field failure data is also lacking. However, the classical engineering solution to such a problem is to divide the big problem into smaller problems. We look at the components of the design where relevant statistical failure data is more likely. Techniques originally developed in the electronic industry do just that. A detailed Failure Modes Effects and Diagnostic Analysis (FMEDA) will provide relatively accurate failure mode and diagnostic coverage estimates for a product based on the data for the components. Component data for mechanical parts can be obtained from field failure reports. While these techniques continue to be developed and are arguably conservative (high failure rates), they can be used now to obtain data that is superior to that available from other sources for safety integrity verification purposes. As the techniques are used more frequently, the mechanical component failure rate and failure mode data will become even more accurate. Eventually failure metrics estimates will consider many individual stress factors and can be tailored to specific applications.

The mechanical FMEDA techniques are described with examples including a pneumatic actuator and a quick release valve.

Conclusions

A FMEDA is a technique used for several years now to more accurately estimate failure rates for each failure mode in products. These numbers have provided more accurate input to PFDavg calculations done for safety integrity verification. Recently FMEDA techniques have been applied to mechanical products with results that offer more accuracy than industry databases. This is expected since a FMEDA is product specific and is not meant to cover the worst of a broad range of products. FMEDA techniques will continue to be applied to electronic and mechanical products and will provide even more accuracy as the techniques are refined.

Safety Instrumented System Design

In industrial process design, experts analyze the process to identify potentially dangerous situations. For each of these risks, process risk experts evaluate all layers of protection designed into the process and determine if further risk reduction is needed. Following new functional safety standards [IEC 61508, IEC 61511], safety functions are specified in terms of the needed functionality and the risk reduction in terms of an order of magnitude level called a safety integrity level (SIL).

When further risk reduction is needed a process design engineer will frequently choose to install a safety instrumented system (SIS). A design is done for each safety function to detect the dangerous situation and automatically take action to prevent or mitigate the danger. Each design is called a safety instrumented function (SIF). A simple system is shown in Figure 1 with a logic solver and one of the safety instrumented functions. Actual SIS implementations typically involve many safety instrumented functions, one for each potentially dangerous condition, in one logic solver. The occurrence of a potentially dangerous condition is known as a “demand.”

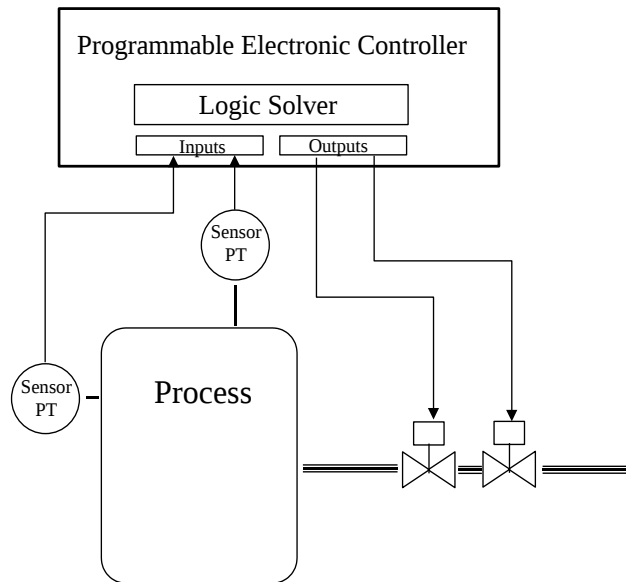


Figure 1: Simple Safety Instrumented System with one Safety Instrumented Function shown.

In the process industries, a SIS is composed of process connections, sensors, logic solver and final elements. Sensors may be temperature measurement devices, pressure measurements devices, flame detectors, toxic gas detectors, emergency switches or many other type devices. Logic solvers were traditionally relays but new designs almost exclusively use safety certified programmable electronic controllers. Final elements range from simple solenoid valves to large remoter actuated valves with an assortment of mechanical equipment.

Safety Instrumented System Probabilistic Verification

The process design engineer must verify that each SIF design meets requirements in terms of several metrics. These metrics include a measure called “PFDavg.” It has been defined as the mean of the time dependent probability of failure on demand [GOB02]. Another metric is called the Safe Failure Fraction (SFF). It is defined in IEC 61508. Both metrics are needed to determine if the proposed SIF design meets the SIL requirement.

In some cases simple quantitative techniques are used to verify that the SIF design meets the SIL. These methods use many assumptions. Some of these assumptions are not accurate and will create misleading results. Much of the problem is due to general failure rate and failure mode data for the

components used in the SIF. Other problems are due to the complicated nature of accurate probabilistic modeling.

As an example of a SIF probabilistic verification, consider the case of an overpressure protection SIF. The SIL requirement is SIL2. The initial design consists of a Yokogawa EJA pressure transmitter, a SIL3 safety PLC and a remote actuated ball valve interfaced with a 3 way solenoid.

Using an on-line internet tool [Exi02] to do the PFDavg and SFF calculations, the results for a single channel (1oo1) architecture are shown in Figure 2.

Sensor Part Information	
Sensor Group(s)	Edit
(1) Pressure	Details
PFDavg Sensor Part	3.24E-03
MTTFS Sensor Part (years)	122.23
Maximum SIL allowed (Architectural Constraints)	1

Logic Solver Part Information	
Logic Solver	Edit
(1) Logic Solver	Details
PFDavg Logic Solver Part	1.41E-04
MTTFS Logic Solver Part (years)	203.36
Maximum SIL allowed (Architectural Constraints)	3

Final Element Part Information	
Final Element Group(s)	Edit
(1) Valve	Details
PFDavg Final Element Part	2.89E-02
MTTFS Final Element Part (years)	22.39
Maximum SIL allowed (Architectural Constraints)	1

SIF Performance Metrics	
Safety Instrumented Function	Preview
Average Probability of Failure on Demand (PFDavg)	3.21E-02
Safety Integrity Level	1
Safety Integrity Level (Architectural Constraints)	1
Risk Reduction Factor	31
MTTFS (years)	17.31

Figure 2: SILver results for initial design pressure protection SIF.

This design does not meet SIL2, only SIL1 as indicated in the bottom section of Figure 2. The problem is primarily in the final element as it is contributing 82% of the total PFDavg for the SIF. This is shown in Figure 3. The failure rate and failure mode data for the solenoid, the pneumatic actuator and the ball valve were obtained from industry databases with conservative assumptions used to obtain failure mode percentage. The data is shown in Figure 4.

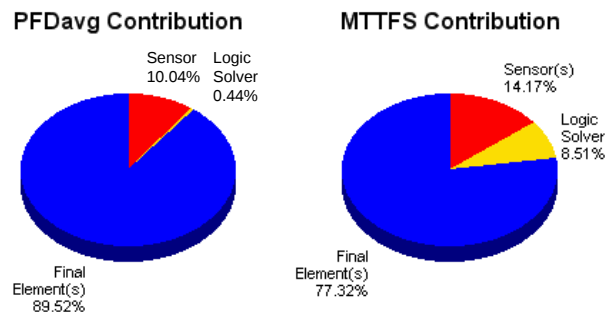


Figure 3: PFDavg contribution for each SIF subsystem.



Home : Applications : SILver : Final Element Part Information : Component Details

Final Element Group 1: Valve

Final Element / Interface Data						
Component	Failure Rate (1/hr)	MTTF (years)	% Safe Failures	Safe Coverage Factor (%)	Dangerous Coverage Factor (%)	Architectural Constraint Type
Generic 3-way solenoid	6.00E-06	19.03	60	0	0	A

Valve Data						
Component	Failure Rate (1/hr)	MTTF (years)	% Safe Failures	Safe Coverage Factor (%)	Dangerous Coverage Factor (%)	Architectural Constraint Type
Generic air operated ball valve	3.00E-06	38.05	55	0	0	A

Figure 4: Failure rate and mode data for the final element components.

Contributing to the problem is the lack of good failure rate and failure mode data, especially for mechanical devices like the solenoid, the pneumatic actuator and the ball valve. A failure modes effects and diagnostic analysis (FMEDA) of these products will produce more accurate data.

Failure Modes Effects and Diagnostic Analysis

A FMEDA is a systematic, detailed procedure where every component in an assembly is listed along with its known failure modes. For each component failure mode, the effect on the assembly is listed along with a failure rate estimate, failure mode distribution and the probability that any diagnostic within the system will detect this failure mode. More information on the analysis can be found in several references [Gob98a, Gob98b, Gob02].

The format of a FMEDA looks like a spreadsheet with columns to identify each part and each failure mode of each part. Other columns list the effect of component failure mode, the product failure mode, the component failure rate and the percentage of component failures in each mode. These columns are used to calculate the failure rates for each failure mode of a product. A portion of a FMEDA for a pneumatic actuator is shown in Figure 5.

Item	Part Description	Failure Mode	Effect	Mode	Qty.	Lambda	% distr.
1-10	Housing	Fracture	Torque transmission failure	D	1	5.00E-09	95%
		Deflection	No effect	#	1	5.00E-09	5%
1-20	Housing cover	Fracture	Valve will not move	D	1	5.00E-09	95%
		Deflection	No effect	#	1	5.00E-09	5%
1-30	Guide block assembly	Fracture - piston side power sw	Springforce will cause shut down	S	1	3.00E-08	32%
		Fracture - spring side power sw	Valve will not move	D	1	3.00E-08	32%
		Fracture - middle	Valve will not move	D	1	3.00E-08	32%
		Deflection	No effect	#	1	3.00E-08	5%
1-50	Extension rod assembly	Fracture	Springforce will cause shut down	S	1	5.00E-08	95%
		Deflection	No effect	#	1	5.00E-08	5%
1-60	Extension retainer nut assembly	Loss of Thread	Springforce will cause shut down	S	1	5.00E-08	20%
		Loosen	Springforce will cause shut down	S	1	5.00E-08	80%
1-70	Yoke	Fracture	Valve will not move	D	1	1.00E-07	75%
		Deflection	Valve not fully seated	D	1	1.00E-07	20%
		Wear	Valve not fully seated	D	1	1.00E-07	5%
1-80	Yoke pin	Fracture	Valve will not move	D	1	6.00E-08	95%
		Deflection	Valve not fully seated	D	1	6.00E-08	5%
2-20	Guide bar bearing	Excessive friction	No effect	#	1	3.00E-08	40%
		Excessive play	No effect	#	1	3.00E-08	10%
		Seized	Valve will not move	D	1	3.00E-08	50%
2-25	Yoke pin bearing	Excessive friction	No effect	#	1	3.00E-08	40%
		Excessive play	No effect	#	1	3.00E-08	10%
		Seized	No effect	#	1	3.00E-08	50%
2-30	Yoke/Guide block bushing	Tear	No effect	#	2	3.00E-08	100%
2-40	Yoke bearing	Excessive friction	No effect	#	2	3.00E-08	40%
		Excessive play	No effect	#	2	3.00E-08	10%
		Seized	No effect	#	2	3.00E-08	50%
2-50	O-ring seal	Leak	N/A	#	2		99%
		Complete failure	N/A	#	2		1%
2-80	Rod wiper	N/A	N/A	#	1		100%
2-90	O-ring seal	Leak	N/A	#	2		99%
		Complete failure	N/A	#	2		1%
3-10	Inner end cap	Fracture	Air leak	S	1	2.50E-08	95%
		Deflection	Air leak	S	1	2.50E-08	5%
3-20	Tie bar	Fracture	Valve will not move	D	2	2.50E-08	5%
		Fracture	Release of pressure	S	2	2.50E-08	90%
		Deflection	Valve will not move	D	2	2.50E-08	1%
		Deflection	Release of pressure	S	2	2.50E-08	4%
3-30	Piston	Fracture	Springforce will cause shut down	S	1	2.50E-08	95%
		Deflection	Valve not fully seated	D	1	2.50E-08	5%

Figure 5: Portion of a FMEDA for a mechanical product.

The result of an FMEDA is a list of failure rates for each failure mode of a product. This is exactly the information needed by system designers to perform the probabilistic SIL verification. Since the numbers are done for a specific product, the total failure rate is typically lower than the numbers given in industry databases. Databases represent a collection of different products including some with relatively poor quality. The results of a FMEDA for a pneumatic actuator are shown in Figure 6.



Total failure rate	1.38E-06		
Safe failure rate	9.19E-07	% safe failure	66.64%
Dangerous failure rate	4.60E-07		
NoEffect failure rate	4.26E-07		
PVST - dangerous detected	4.26E-07	SFF no PVST	74.51%
PVST - dangerous undetected	3.40E-08	SFF with PVS	98.12%

Figure 6: Results from a FMEDA for a pneumatic actuator, a mechanical product.

These results provide a total failure rate and the failure rate for dangerous failures and safe failures. Additionally, the effects of using partial valve stroke testing to do diagnostics on the actuator are shown in the form of the dangerous detected failure rate and the dangerous undetected failure rate. These numbers were used to calculate the safe failure fraction (SFF) for the product.

Manufacturer	Product	Description	FMEDA Report	61508 Certification
Det-tronics	Pointwatch Eclipse IR	Hydrocarbon Gas detector	exida	None
	X3301 multi-spectrum IR	Flame Detector (fire detection)	exida	None
ABB	600T	Pressure Transmitter	TUV	TUV
Honeywell	ST3000	Pressure Transmitter	exida	None
	STT250	Temperature Transmitter	exida	None
Moore Industries	TRY	Temperature Transmitter	exida	None
	SPA	Site Programmable Alarm	exida	None
Rosemount	3051C	Pressure Transmitter	FM	None
	3051T	Pressure Transmitter	exida	None
	3144P	Temperature Transmitter	exida	None
	3051S	Pressure Transmitter	exida	None
	8800C	Vortex Flowmeter	exida	None
Yokogawa	EJA	Pressure Transmitter	exida	None
	YTA	Temperature Transmitter	exida	None
WIKA	T32	Temperature Transmitter	exida	None
Elcon	HD 2026 (SK)	Smart isolator	exida	None
	HD 2030 (SK)	Smart isolator	exida	None
	HD 2842	Switch/Proximity Detector	exida	None
Pepperl+Fuchs	ED2-STC***	Smart isolator	exida	None
	KFA*-S***-Ex*	Isolated Barrier	exida	None
	MUX 2700	HART Gateway	exida	None
MTL	MTL 5042	Repeating Power Supply	BASEEFA	BASEEFA
Magnetrol	Eclipse Model 705	Guided Wave Radar Level Transmitter	exida	None
	Eclipse Model 708	Guided Wave Radar Level Transmitter	exida	None
Endress & Houser	Fieldgate FXA 520	HART Gateway	exida	None
Fisher Controls	DVC6000	Valve controller	exida	TUV
Metso Automation	VG800	Valve controller	exida	TUV
Bettis Corporation	G series	Pneumatic Valve actuator	exida	None
	CB series	Pneumatic Valve actuator	exida	None
Mokveld	RXD series	Valve	AEA	TUV

Figure 7: Listing of products that have completed a FMEDA.

A FMEDA has been done for many products. A partial list is shown in Figure 7. A review of the list shows however that most of products are electronic or electro-mechanical. It is true that the techniques were developed for electronic products however the fundamental concept of breaking a product into its components and analyzing the component failures applies equally to mechanical products. The key is known component failure modes and distributions. These are well known for most mechanical parts.

Problems and Solutions

No one would argue that this method produces perfectly accurate predictions of field failure rates. Component failure rate data is quite variable as a function of the application. Specific stress-strength analysis is needed for more accuracy. If this analysis is combined with specific application stress data, even more accuracy can be obtained. The analysis tools required to this work are available. We will see better and better mechanical failure rates as these tools are used.



References

1. [IEC00] IEC 61508, *Functional Safety of electrical / electronic / programmable electronic safety-related systems*, 2000.
2. [IEC02] IEC 61511
3. [ISA02] TR84.0.02-2002, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, ISA, NC: Research Triangle Park, 2002 .
4. [Buk02] Bukowski, Dr. J. V., Rouvroye, Dr. J., Goble, Dr. W. M., *What is PFDavg?*, exida.com, 2002, Available on the www.exida.com free article web page.
5. [Exi02] exida.com SILver SIL verification tool, Version 2.1, 2002.
6. [Buk01] Bukowski, Dr. J. V., *Modeling and Analyzing the Effects of Periodic Inspection in the Performance of Safety-Critical Systems*, IEEE Transactions on Reliability, Volume 50, Number 3, IEEE, NY: New York, September 2001. Available on the www.exida.com free article web page.
7. [Gob98a] Goble, Dr. W. M., *Control System Safety Evaluation and Reliability*, ISA, 1998.
8. [Gob98b] Goble, Dr. W. M., *The Use and Development of Quantitative Reliability and Safety Analysis in New Product Design*, 1998, exida.
9. [Gob02] Goble, Dr. W. M., *Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage and Failure Modes in Instrumentation*, exida.com, www.exida.com/articles.asp, 2002.
10. [NSWC98] *Handbook of Reliability Prediction Procedures for Mechanical Equipment*, Naval Surface Warfare Center, West Bethesda, MA, 1998.

Revision History

Authors: Dr. William M. Goble

Release 1.0	January 2003	W.M. Goble
-------------	--------------	------------

Presented at the IEC 61508 Symposium, RWTUV, Augsburg, Germany

Release 1.1	March 19, 2003	W.M. Goble
-------------	----------------	------------

Presented at ISA Safety Symposium, Houston, TX

Release 2.0 Update	July 2008	W.M. Goble
--------------------	-----------	------------

Release 2.1 Reformat	October 2020	W.M. Goble
----------------------	--------------	------------



exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool



excellence in dependable automation

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)
- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
 - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
 - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com