

Getting Failure Rate Data

Dr. W.M. Goble, Principal Partner, exida

wgoble@exida.com

www.exida.com

INTRODUCTION

Safety verification calculations for each safety instrumented function are a key concept in functional safety standards like ISA 84.01 and IEC 61511. These calculations are done to insure a balanced and optimal design. However, the calculations require failure rate and failure mode information for all the instruments used – sensor to final element. When ISA84.01 was first released in 1996, one comment was made repeatedly, “No one has good failure rate data.” This led some to believe that the whole idea behind probabilistic failure calculations is impractical. Some are still making the comment.

The fact is that there has been failure rate data available and the data is getting much better as manufacturers understand safety instrumentation users needs. Even in the early years of the standard, industry failure databases could provide information. While this failure data was not product specific or application specific, it helped designers recognize problems in their designs. One such problem was the “weak link” design. These designs included expensive SIL3 safety PLCs that were connected to a switch and a solenoid. Many of these engineers thought they had a SIL3 design until they did the safety verification calculations. Such a design will not even meet SIL1! Another common problem was the final element, typically a remote actuated on-off valve. Some designs had triplicated sensors and a SIL3 rated safety PLC with a set of pneumatic controls mounted on a single ball valve. The design target was SIL3 but the safety verification calculations showed that the design only met SIL1. [See Appendix 1: “A sample SIF calculation”]

The safety verification calculations required by the new functional safety standards have shown designers how to design much more balanced designs that optimize cost and safety. The calculations have shown many how to do a better job. But, failure rate and failure mode data on the chosen equipment is a must.

Industry Failure Databases

One of the most popular failure rate databases is the OREDA database. OREDA stands for “Offshore Reliability Data.” The information is printed in a book that may be ordered from DNV in Norway (oreda@dnv.com). The third edition dated 1997 has been printed with a new version planned. This book presents detailed statistical analysis on many types of process equipment. Many engineers use it as a source of failure rate data to perform safety verification calculations. It remains an excellent reference for all who do data analysis.

Other data sources include:

1. FMD-97, Failure mode / Mechanism Distributions, 1997, Reliability Analysis Center, Rome, NY
2. Guidelines for Process Equipment Reliability Data, with Data Tables, 1989, Center for Chemical Process Safety of AIChE, New York, NY
3. NPRD-95, Nonelectronic Parts Reliability Data, 1995, Reliability Analysis Center, Rome, NY
4. IEEE Std. 500, IEEE Guide To The Collection and Presentation Of Electrical, Electronic, Sensing Component, And Mechanical Equipment Reliability Data For Nuclear-Power Generating Stations, 1984, IEEE, New York, NY
5. Reliability Data for Control and Safety Systems, 1998, SINTEF Industrial Management, Trondheim, Norway

And several other sources somewhat more specialized.

Many companies have an internal expert who has studied these sources as well as their own internal failure records and maintains the company failure rate database. Some use failure data compilations found on the internet. While the data in industry databases is not product specific or application specific, it does provide useful failure rate information for specific industries (nuclear, offshore, etc.) and a comparison of the data provides information about failure rates versus stress factors.

There is a problem with the industry databases though. A probability of fail-danger calculation for safety verification purposes does require more than just failure rate data. For each piece of equipment, one must know the failure modes (safe versus dangerous) and the effectiveness of any automatic diagnostics (the diagnostics coverage factor). This information is included only in rough form if at all in industry databases. So many engineers doing safety verification calculations provide an educated and conservative estimate. For most electronic equipment, the safe percentage is set to 50%. Relays have a higher percentage of safe failures with many picking a value of 70% or 80%. Mechanical components like solenoids might be more like 40% safe with many failure modes causing stuck in place failures that end up being dangerous in a safety protection application.

Diagnostic coverage can also be estimated. If "normal" diagnostics are available in a microprocessor based product, diagnostic coverage can be conservatively credited to 50%. Diagnostics for mechanical devices is usually given no credit, 0% detected failures, unless there is some special testing like automatic partial valve stroke testing due to a smart valve positioner.

So, the data is there. Using a combination of industry databases, company data and experience, the calculation methods required in functional safety standards like ISA 84.01 and IEC 61511 are being performed.

Product Specific Failure Data

It is clear that some are uncomfortable with the level of accuracy in the data. Questions about failure rate versus stress conditions in particular applications come up. Questions about specific products are constantly being asked especially when one must attempt to pick a better product to achieve higher safety.

Fortunately, several instrumentation manufacturers are doing detailed analysis of their products to determine a more accurate set of numbers useful for safety verification purposes. A Failure Modes Effects and Diagnostic Analysis (FMEDA) provides specific failure rates for each failure mode of an instrumentation product. The percentage of failures that are safe versus dangerous is clear and relatively precise for each specific product. The diagnostic ability of the instrument is precisely measured. Overall, the numbers from such an analysis are indeed product specific and provide a much higher level of accuracy when compared to industry database numbers and experience based estimates.

A FMEDA is done by examining each component in a product. For each failure mode of each component, the effect on the product is recorded. Will this resistor failure cause the product to fail safety, fail dangerously, lose calibration? If the serial communication line from the A/D to the microprocessor gets shorted, how does the product respond? If this spring fractures does that cause a dangerous or a safe failure? The failure rate of each component is entered according to component failure mode and the various categories are added. The end result is a product specific set of failure data that includes failure rates for each failure mode, failure rates that are detected and undetected by diagnostics, safe failure fraction calculations and often an explanation on how to use the numbers to do safety verification calculations.

FMEDA is sometimes done by the manufacturer but typically done by third party experts including TÜV, FM, BASEEFA and exida. Often the work is done as part of a IEC61508 functional safety certification effort by the product manufacturer. Many manufacturers have recently issued FMEDA reports as shown in Table 1, a listing of field instrumentation reports. The FMEDA failure rate and failure mode is product specific and generally shows lower failure rates than industry database generic data. A comparison is done in Appendix 2.

Table 1: Field Instrumentation FMEDA reports available.

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

The future of failure data

Although product specific FMEDA reports offer superior data sources when compared to industry databases, they still do not account for application specific stress conditions that may affect actual failure rates. Ideally in the future manufacturers will be able to provide not only point estimates of failure rates but perhaps even equations with application specific variables to more precisely calculate the needed numbers. That will happen if there is demand and the needed data is collected.

One effort in the right direction is the PERD (Process Equipment Reliability Database) initiative from the Center for Chemical Process Safety (CCPS) of the AIChE (www.aiche.org/ccps/perd/). That group has defined failure taxonomies for various types of process equipment. The important data that must be collected for a failure event has been defined. Operating companies from chemical, petrochemical, industrial gases and other industries become members and are working to set up inspection and failure reporting. They have created data collection software that members use to report field failures to a central database. There is potential that this information could someday become the best possible source of product specific and application specific failure rate and failure mode data. We look forward to better data with more accuracy as we move forward.

Appendix 1: A sample SIF calculation.

A safety instrumented function has been defined where high pressure in a process vessel must stop “sour gas” fuel flow to a burner. The risk reduction requirement results in a SIL2 target for the SIF. The proposed safety instrumented function design is shown in figure 1.

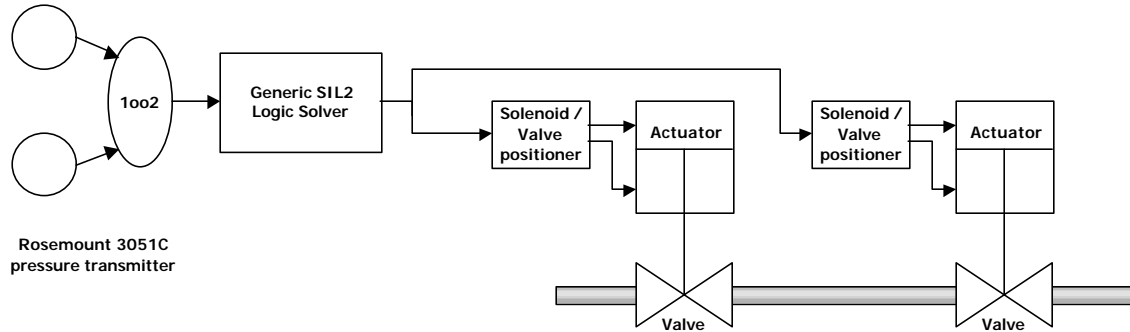


Figure 1 Conceptual design SIL2 Safety Instrumented Function

The conceptual design of this safety instrumented function consists of the following equipment. Two pressure transmitters in a 1oo2 voting arrangement are used as the sensor devices. A PLC certified for SIL2 is used as the logic solver. Finally two 3-way solenoids each operating an pneumatic actuator with ball valve in a 1-out-of-2 voting arrangement are used as the final element devices.

A proof test interval of 12 months and a Mean Time To Repair of 8 hours are specified. The results of the SIL verification using the exida software tool SILver, shown in figure 2, indicate that the conceptual design of the safety instrumented function meets the SIL2 requirements based on the average Probability of Failure on Demand value. Furthermore the conceptual design of the SIF also meets the SIL2 requirements based on the architectural constraints requirement of IEC 61511.

Sensor Part Information	
Sensor Group(s)	Edit
(1) Pressure group	Details
PFDavg Sensor Part:	3.25E-05
MTTFS Sensor Part (years):	123.23
Maximum SIL allowed (Architectural Constraints):	2
Logic Solver Part Information	
Logic Solver	Edit
(1) Safety PLC	Details
PFDavg Logic Solver Part	2.00E-03
MTTFS Logic Solver Part (years)	3.27
Maximum SIL allowed (Architectural Constraints):	2
Final Element Part Information	
Final Element Group(s)	Edit
(1) Shutoff valves	Details
PFDavg Final Element Part:	1.84E-03
MTTFS Final Element Part (years):	12.39
Maximum SIL allowed (Architectural Constraints):	2
SIF Performance Metrics	
Safety Instrumented Function	Preview
Average Probability of Failure on Demand (PFDavg)	3.86E-03
Safety Integrity Level	2
Safety Integrity Level (Architectural Constraints)	2
Risk Reduction Factor	259
MTTFS (years)	2.53

Figure 2 SIL verification results for conceptual design SIL2 SIF

Appendix 2: A comparison of failure rates.

Failure rates may be obtained from industry databases, manufacturer FMEDA analysis, manufacturer field failure studies, company failure records or other sources. Most reliability engineers consider application specific and product specific data to be the most accurate. Generally, less specific data turns out to be more conservative and that is appropriate for safety verification purposes following the rule that “the less one knows, the more conservative one must be.”

Table 2 shows a comparison of data for a pressure transmitter. The failure rate numbers from the database sources are significantly higher than the FMEDA reports.

Table 2 – failure rate data for a pressure transmitter

Source	Component	Total Failure Rate (1/hr)	% Safe Failures	Safe Cov. Factor (%)	Dangerous Cov. Factor (%)	Range
CCPS-89	Transmitters - Differential Pressure	1.01E-06	-	-	-	low
	Transmitters - Differential Pressure	6.56E-05	-	-	-	mean
	Transmitters - Differential Pressure	2.54E-04	-	-	-	high
NPRD-95	Transducer, Pressure	8.13E-06	-	-	-	mean
Rosemount	FMEDA, 3051T Pressure Transmitter, exida	4.46E-07	64	100	27.5	FMEDA
Honeywell	FMEDA, ST3000 Pressure Transmitter, exida	4.90E-07	60	100	24.7	FMEDA