Combining Field Failure Data with New Instrument Design Margins to Predict Failure Rates for SIS Verification

White Paper

exida
80 N. Main St.
Sellersville, PA
www.exida.com

October 2014

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Abstract

Performance based functional safety standards like IEC 61511 offer many advantages including the opportunity to optimize and upgrade Safety Instrumented System (SIS) designs. But performance calculation depends upon realistic failure data for instruments used. A predictive analysis technique called Failure Modes Effects and Diagnostic Analysis (FMEDA) has been developed along with a component failure rate database that can predict failure rates of instruments based on their design strength and the expected stress environment. This method has been calibrated with over 150 billion-unit operating hours of field failure data over the last 15 years.

Conclusion

There is a strong indication that a predictive FMEDA with a good component data handbook [12] generates realistic failure data for any product type based on analysis of the design and the operational stress conditions. It is expected that recent emphasis on field failure data collection will aid in the generation of quality data for future refinement of the component database used to generate FMEDA results.

Introduction

Functional Safety Standards [1,2] have provided a logical framework for the lifecycle management of automatic protection functions called Safety Instrumented Functions (SIF) in the process industries. From the pioneering document done by ISA [3] in 1996 through the latest updates of the IEC standards, these methods have grown to become global common practice.

One of the essential concepts in these standards is the use of probabilistic analysis to provide a measure of performance for any specific design. An SIS designer creates an instrumentation design then obtains all failure rates for all devices in a SIF. Probabilistic failure analysis using that data will determine if the given design meets risk reduction targets. The failure rate data obtained must be realistic or even conservative.

Failure Rate Sources

Failure data can be obtained from several sources: Industry Databases, Committee Estimates, Manufacturer Warranty Analysis, and Company Failure Databases. Industry databases gather field failure data and publish aggregated results. One of the most useful for the process industries is the Offshore Reliability Data (OREDA)[4]. Failure data is gathered from member operating companies in the North Sea, analyzed by SINTEF in Norway, and published. SINTEF publishes the PDS Data Handbook [5] based on a number of sources including the OREDA data. The PDS Data Handbook presents generic data that is not product specific which includes safe failure rate, dangerous failure rate, diagnostic coverage,

factors, and common cause estimates. The data collection process is quite thorough with all failures recorded, both product related failures and site related failures such as maintenance errors [6].

Many organizations / companies have also created their own list of failure rates. In some examples, a committee meets and estimates failure rates based on the experience of the committee members. The methods used are rarely published yet those numbers are useful for comparison purposes as they represent an experienced opinion.

Some manufacturers will analyze their warranty return failure data and publish failure rates. This data can be useful for some purposes but definitions and limitations cause problems. Manufacturers tend to use a narrow definition of a "failure" that excludes many of the returned items. Hence a detail review shows many returns classified as "not a failure" or "no problem found" or "customer abuse." Given the limitations of not knowing what percentage of failed units are returned and the inability to know field operational hours, failure rates tend to be quite optimistic and not likely suitable for SIF verification. However, the data can be used to generate upper bound and lower bound numbers that are useful for comparison purposes.

Company Failure Databases represent great potential to provide realistic failure data. Although data collection process audits [7] have shown substantial differences in methods used to collect data, the biggest issue is the definition of "failure." That varies substantially from site to site with resulting differences of 2X to 20X in the resulting failure rates. Given good definitions of failure as used by SINTEF and clear definitions of what is included in the data, the analysis results can be the most valuable source of data. DOW published a study of their field failure data collection system [8]. The methods used were reviewed with exida during a series of meetings with DOW in the Netherlands and the details of the included devices were described. In the author's opinion, this study represents clearly defined, realistic data for product failures.

Failure Modes Effects and Diagnostics Analysis

One significant problem with all field failure data gathering techniques is that often a product will become obsolete before enough data is gathered to obtain a failure rate. It was clear when the functional safety standards were being debated that a predictive method was needed both for new products and for products where little data had been gathered.

The FMEDA technique was developed by engineers from exida to provide a means to predict not only failure rates but failure rates per failure mode, diagnostics coverage factors, and useful life. The method is based on the complexity and design strength of a product. The FMEDA method accounts for the automatic diagnostics being developed at the time. The technique was first published in 1992 as "Coverage Analysis" in Chapter 6 of [9] and later named FMEDA [10, 11].

The FMEDA method examines each component in a product design. For each component, all failure modes are listed, and analysis is done to determine the impact of that component failure mode on the product. An FMEDA is verified by a set of sample fault simulation / injection tests which are done to simulate the component failure mode in the actual product.

Failure data for each component is required. This component data comes from a component database that must include failure rates and failure mode distributions of each component as a function of environmental operating profile (expected stress conditions) [12]. The useful life of each component should also be listed as a function of operating profile. Both electronic and mechanical components must

be included [13]. An FMEDA can provide realistic predictions of failure rates for each failure mode and useful life. However, the FMEDA method can also generate nonsense if the analyst does not have a good component failure data handbook. Therefore, it is essential that such component failure rates be constantly compared with actual field failure data.

Comparison of exida FMEDA Results with Field Failure Data

Consider a pressure transmitter. Most designs are microcomputer based with complex electronics as well as mechanical parts. Figure 1 shows several total failure rate numbers from exida FMEDAs compared to the DOW field data [8]. The average of the FMEDA results from several different transmitter designs equals 5.02E-07 compared to the DOW number of 4.96E-07. This is extremely close given the uncertainty of the results.

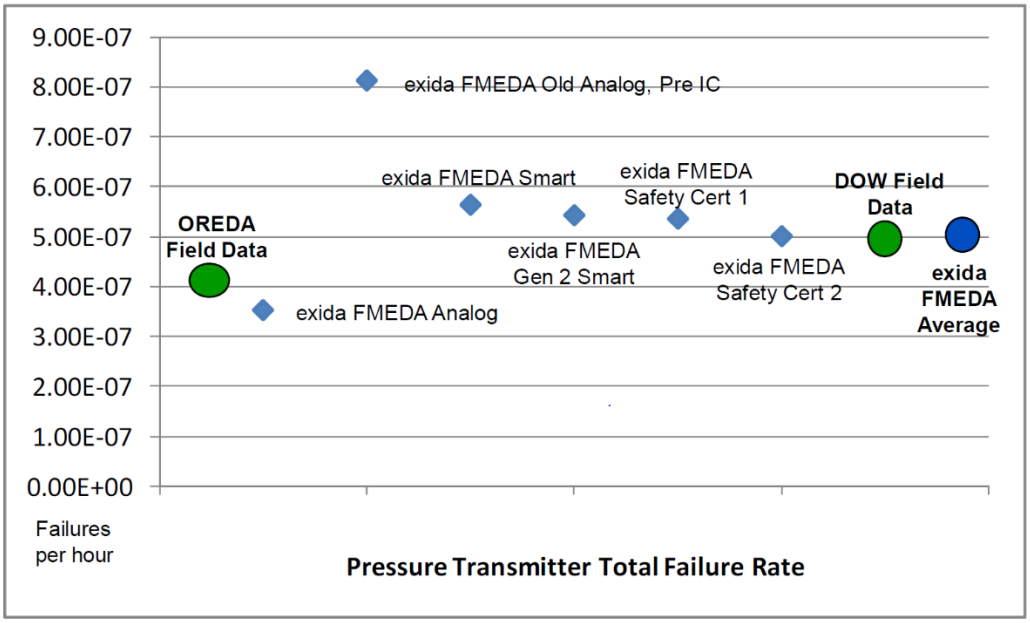

Figure 1: Pressure Transmitter Total Failure Rate Comparison

The PDS Handbook based on OREDA states clearly that their pressure transmitter numbers include "the sensing element, local electronics and process isolation valves / process connections." So that number cannot provide any useful comparison as none of the above numbers included isolation valves or process connections. OREDA Volume 1 [4] states that the mean failure rate for pressure transmitters (Taxonomy 4.2.3) is 4.2E-07 failures per hour. That is also very close to the FMEDA results but may indicate that FMEDA failure rate numbers are slightly and conservatively high.

The FMEDA technique can be used for mechanical devices as well [13, 14]. A comparison of total failure rate numbers for solenoid valves is shown in Figure 2. FMEDA results distinguish the difference between solenoid valve designs. The difference in complexity between a poppet design and a spool design is significant and shows up in the predicted failure rates. DOW engineers did confirm that their data aggregates different types of solenoid valves including both poppet and spool. The FMEDA average of two poppet types and two spool types is higher than the DOW number but well within a reasonable range. The OREDA data book provides failure rate data only for final element assemblies. Therefore, no information applicable to a solenoid valve was found.

It is important to compare published failure rates to realistic field studies. Some published data points appear to be unrealistic. Two data points, a manufacturer warranty data point [15], is well below all other data points. Other "FMEA" based numbers published for a solenoid valve are quite low [16].

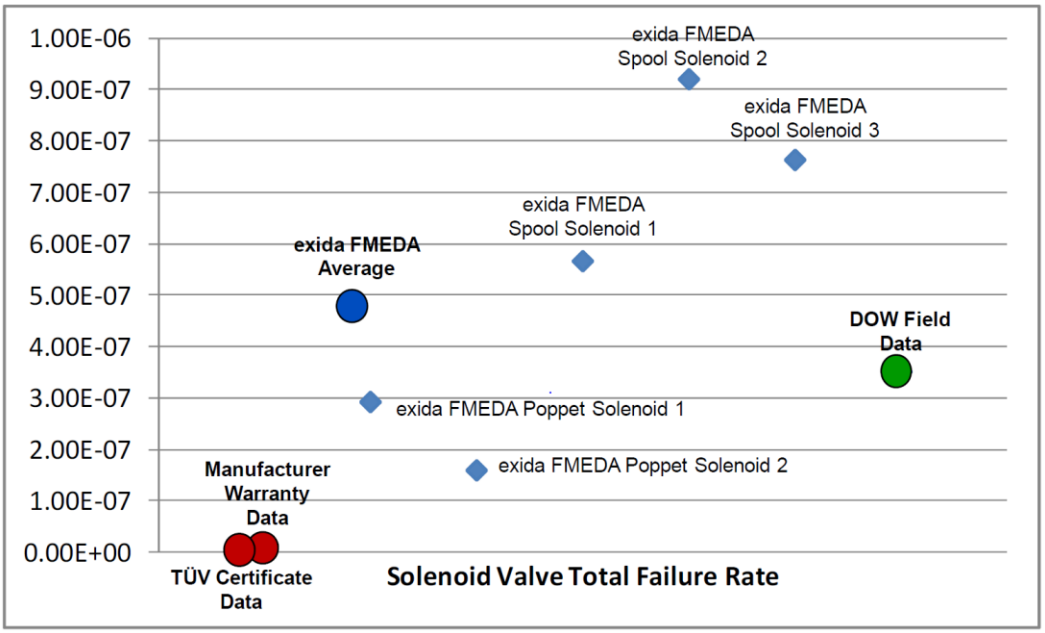

Figure 2: Solenoid Valve Total Failure Rate Comparison

References

1. *IEC 61508, Functional Safety of electrical / electronic / programmable electronic safety- related systems*, Geneva, Switzerland, 2000.
2. *IEC 61511, Application of Safety Instrumented Systems for the Process Industries*, Geneva, Switzerland, 2003.
3. *ISA 84.01-1996* (now called ANSI / ISA 84.00.01-2004 (IEC 61511)), International Society of Automation, Research Triangle Park, NC, 1996.
4. *OREDA, Offshore Reliability Data, 5th Edition, Volume 1 - Topside Equipment*, Det Norske Veritas, Trondheim, Norway, 2009.
5. *Reliability Data for Safety Instrumented Systems, PDS Data Handbook*, 2014 Edition, SINTEF Technology and Society, Trondheim, Norway, 2010.
6. Aarø, Ragnar, *Use of failure data from analysis and operational experience*, IFEA Seminar on IEC 61508/61511, Sandefjord, Norway, 7th – 8th March, 2012.
7. Goble, W. M., *Field Failure Data – the Good, the Bad and the Ugly*, exida, Sellersville, PA, www.exida.com/resources/whitepapers.
8. Skweres, Patrick and Thibodeaux, John, *Establishing a Instrument and Analyzer Reliability Program in Support of Independent Protection Layers*, Proceedings of the 63rd Annual Instrument Symposium for the Process Industries, Texas A&M, January 29-31, 2008.

9. Goble, W. M., *Evaluating Control Systems Reliability, Techniques and Applications*, NC: Research Triangle Park, Instrument Society of America, 1992.
10. Goble, W.M., *The Use and Development of Quantitative Reliability and Safety Analysis in New Product Design*, University Press, Eindhoven University of Technology, Netherlands: Eindhoven, 1998.
11. W. M. Goble and A. C. Brombacher, *Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems*, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
12. *Electrical & Mechanical Component Reliability Handbook*, 4th Edition, exida, Sellersville, PA, 2014. See www.exida.com
13. W.M. Goble and J.V. Bukowski, *Development of a Mechanical Component Failure Database*, 2007 Proceedings of the Annual Reliability and Maintainability Symposium, NY: NY, IEEE, 2007.
14. Bukowski, J. V., Goble, W. M., "Validation of a Mechanical Component Constant Failure Rate Database," Proceedings Annual Reliability and Maintainability Symposium, January 2009, Fort Worth, TX, pp. 338-343.
15. IEC 61508 Component Assessment, FP10, AEAT/61508/LRSB/10738/A03, AEA Technology, 28 June 2005.
16. Report No. V372 2010 S1, TÜV Rheinland Energie and Umwelt GmbH, 2011.

Revision History

Authors: Iwan van Beurden, William M. Goble, PhD

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
  - 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