Quantifying the Impacts of Human Factors on Functional Safety

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

April 2016

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

Keywords: systematic failure rate, product failure rate, site-generated failure rate, FMEDA, PFDavg

Abstract

It is not difficult to think of numerous ways in which human factors might impact functional safety. For example, imperfect repair, improper calibration, faulty installation, etc. can all contribute to decreases in functional safety performance. However, if actions are to be taken to mitigate these impacts then it is essential to have some quantitative measure of the impacts so that the actions' effectiveness can be assessed. This paper describes how the Site Safety Index™ (SSI) is used to adjust safety metrics, computed under the assumptions that human factors play no part in safety system performance, to reflect the effects of human factors on safety system performance on a site by site basis. Examples of the application of the method showing the safety performance changes attributable to human factors are provided.

Conclusion

This paper clearly shows that the impacts of end-user activities and practices on safety performance of a SIF can be quantified through a simple model like the SSI. It also explains how the SSI modification multipliers are being calibrated and will be updated as increasing amounts of FFD become available. The methodologies presented here and in [4] allow end-users to measure quantitatively their own activities and practices on a site-by-site basis and to measure the impacts of those activities and practices on SIF safety performance.

Introduction

A safety instrumented function (SIF) has an inherent product failure rate based on its design and implementation and the assumption that the end user will take all necessary actions (i.e., meet all IEC 61508 [1] and/or IEC 61511 [2] requirements) to insure that the inherent product failure rate will be achieved. In practice, end-user activities and practices often fall short of this ideal and, consequently, the safety performance achieved by the SIF is often less than the ideal [3]. The SSI measures, on a scale of 0 to 4, the extent to which end-user actions support the achievement and retention of ideal SIF safety performance. The SSI is described in detail in [4]. This paper explains how end-user actions as measured by SSI affect various parameters that are used to calculate SIF safety performance and show how different levels of SSI impact various safety metrics.

Notation

FFD	field failure data
FMEDA	failure modes, effects and diagnostic analysis
IEC	International Electrotechnical Commission
MTTFS	mean time to fail safe
OREDA	Offshore and Onshore Reliability Data
PFDavg	average probability of dangerous failure on demand
RRF	risk reduction factor
SIF	safety instrumented function
SIL	safety integrity level
SRS	Savannah River Site

SSI	Site Safety Index™
1oo1	1-out-of-1 architecture

Using SSI to Measure Impacts of End-User Activities and Practices on Safety Performance of SIFs

Why a Site Safety Index™?

Studies [5] have shown that the failure rates estimated from field failure data (FFD) for identical modules in the same industrial application exhibit a difference in estimated failure rates for the same product from site to site. Typically, when compared to inherent predicted failure rates for the same products, the FFD estimates are approximately 1.2 to 3 times higher depending on product type. Site audits have attributed these differences to dissimilarities in end-user activities and practices which vary from site to site. This variation in end-user activities and practices can be captured by the SSI [4]. Further, these variations in activities and practices directly impact many variables used in models which assess the safety performance of SIFs.

The Key Variables Impacting PFDavg and Other Metrics

A key metric for measuring the safety performance of SIFs is average probability of failure on demand (PFDavg). Other closely related metrics are risk reduction factor (RRF), safety integrity level (SIL), and mean time to fail safe (MTTFS). Based on studies of FFD and proof test reports, nine key variables impacting PFDavg have been identified [6]. These nine variables are

1. Failure rates of each device including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of devices chosen and of end-user practices);
2. Proof Test Effectiveness (an attribute of the proof test method and, to the extent that there is more than one possible proof test method, an attribute of end-user practices);
3. Proof Test Intervals (assignable by end-user practices);
4. Mean Time to Restore (an attribute of end-user practices);
5. Probability of Initial Failure (PIF) (an attribute of end-user practices);
6. Mission Time (an attribute of end-user practices);
7. Proof Test Duration (an attribute of end-user practices);
8. Site Safety Index™ (an attribute of end-user practices); and
9. Redundancy of Devices including common cause failures (an attribute of SIF design).

How Key Variables Are Modified to Quantify the Impacts on PFDavg and Other Metrics

Clearly, redundancy of devices is not an attribute of end-user practices or activities. The SSI itself is not modified in safety performance calculations; rather it is used to modify many of the other variables which impact PFDavg and other metrics. Specifically, whenever SSI is less than 4, the following five key variables are modified:

- failure rates of each device
- proof test effectiveness
- proof test intervals

- mean time to restore
- PIF

Failure rates of each individual device in the SIF are increased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less than ideal end-user practices than are sensors or logic solvers. By increasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance. Proof test effectiveness, i.e., the likelihood that all failures are discovered and completely repaired, is also decreased with decreasing SSI.

Proof test intervals, mean time to restore, and PIF are increased by specific multipliers determined by SSI value. It is common to find that less than ideal end-user practices include delaying proof testing, reducing proof test coverage, requiring additional restoration time, and introducing initial failures through imperfect pre- or post-installation testing. Final elements that may develop failures simply due to lack of motion of the moving parts over an extended time (a few months) are especially vulnerable to initial failures in excess of 1% [7, 8, 9].

The two variables not modified are mission time and proof test duration. Mission time is not modified because its impact is generally small unless the mission time is sufficiently beyond the SIF useful life so as to cause the SIF to see failures due to ageing, i.e., failures no longer modeled by a constant failure rate, without renewal during the mission time. Proof test duration has no impact if proof testing is performed with the process off-line. For proof testing performed on-line, proof test duration generally has only a very small effect unless proof testing frequency is very frequent, i.e., greater than or equal to once per month – an impractical situation for most industrial processes.

Calibrating the Multipliers

As with the development of the Failure Modes, Effect and Diagnostic Analysis (FMEDA) failure rate predictive technique [10] and its associated validated databases [11, 12, 13], it is necessary to calibrate the database of multipliers for the various modifications and to provide on-going validation against actual FFD. The initial calibration phase is still in progress and uses the extensive FFD of the Offshore and Onshore Reliability Data Project (OREDA) [14, 15] as well as the detailed proof testing and root cause failure records of the Savannah River Site (SRS) [8].

Examples of Quantifying the Impacts of SSI on Various Metrics

The same simple 1oo1 SIF was analyzed under five different levels of SSI. Figure 1 shows the impacts on PFDavg and SIL of these variations in SSI. For the same 1oo1 system, Figure 2 shows the impacts on RRF and SIL of variations in SSI. Finally, Figure 3 shows the impact on MTTFS of variations in SSI.

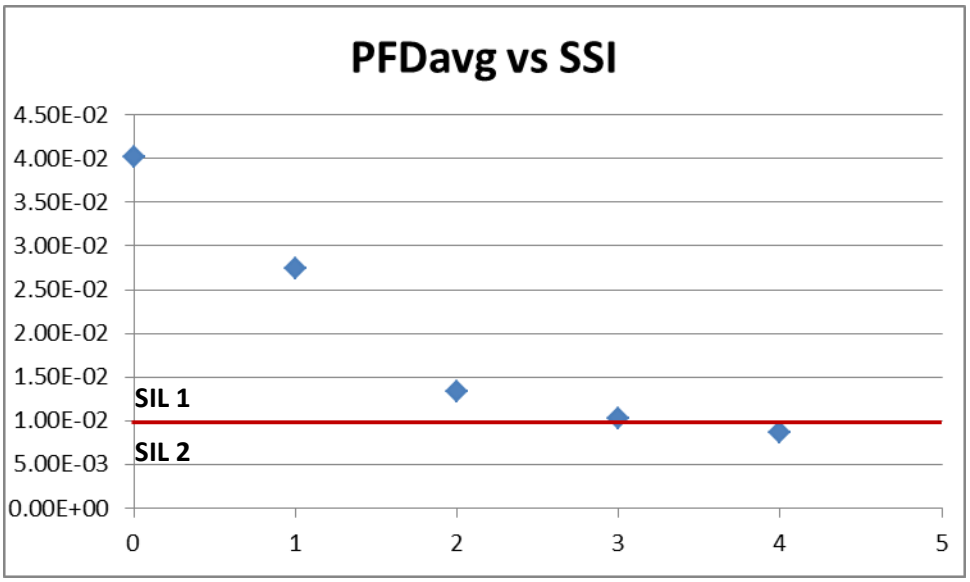

Figure 1. Impacts on PFDavg and SIL of Variations in SSI.

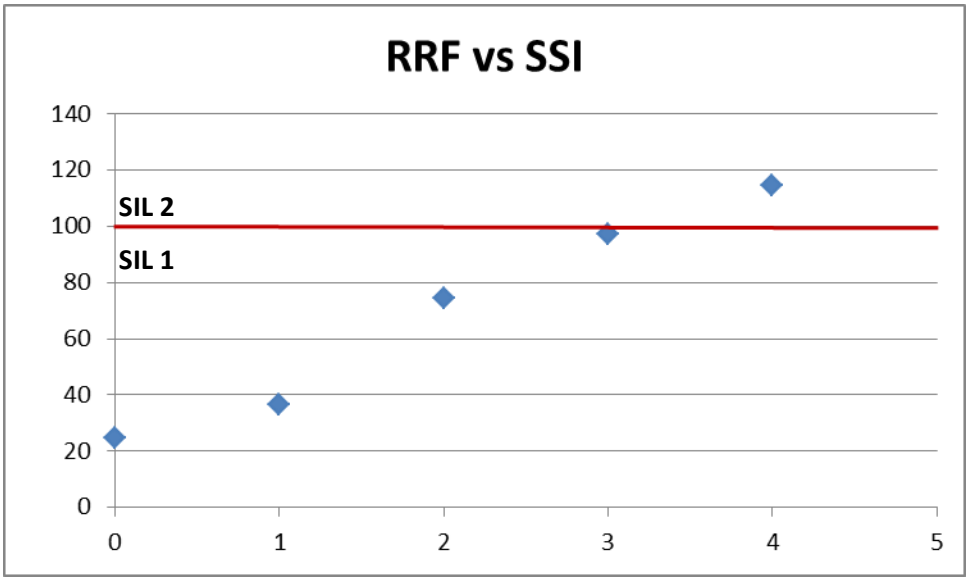

Figure 2. Impacts on RRF of Variations in SSI.

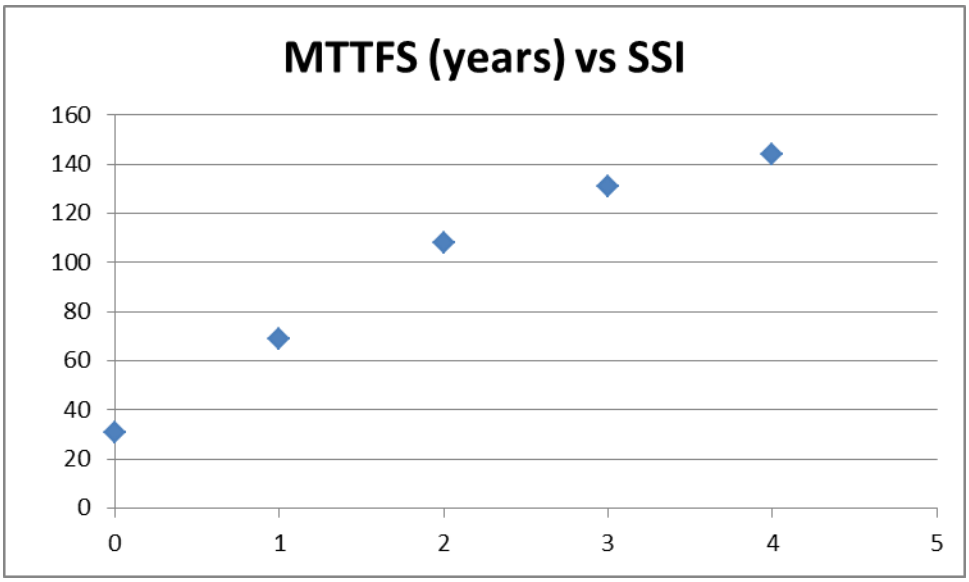

Figure 3. Impacts on MTTFS of Variations in SSI

References

[1] IEC 61508, *Functional Safety of electrical / electronic / programmable electronic safety-related systems*, Geneva, Switzerland, 2010.

[2] IEC 61511, *Application of Safety Instrumented Systems for the Process Industries*, Geneva, Switzerland, 2nd edition, 2004.

[3] J. V. Bukowski, W. M. Goble, and I van Beurden, "Product Failure Rates vs Total Failure Rates at Specific Sites: Implications for Safety," *Proceeding AIChE 11th Global Congress on Process Safety*, Austin, TX, April 2015.

[4] J. V. Bukowski and D. Chastain-Knight, "Assessing Safety Culture via the Site Safety Index™," *Proceeding AIChE 12th Global Congress on Process Safety*, Houston, TX, April 2016.

[5] W. M. Goble, "Maintenance capability: Does it matter in the long term?" *Hydrocarbon Processing,* June 1, 2013.

[6] "The Key Variables Needed for PFDavg Calculation," White Paper, exida 2015, http://www.exida.com/Resources/Whitepapers/the-key-variables-needed-for-pfdavg-calculation

[7] J. V. Bukowski, R. E. Gross and W. M. Goble, "Probability of Initial Failure for Spring Operated Relief Valves," *Proceedings of the ASME 2011 Pressure Vessels and Piping Division Conference*, Baltimore, MD, July 2011.

[8] J. V. Bukowski, R. E. Gross and W. M. Goble, "The Adhesion Failure Mode in Stainless Steel Trim Spring Operated Pressure Relief Valves," *ASME Journal of Pressure Vessel Technology*, Vol 135 No 6, December 2013.

[9] L. Stewart, J. V. Bukowski and W. M. Goble, "Improving Reliability & Safety Performance of Solenoid Valves by Stroke Testing," *Proceedings AIChE 9th Annual Global Conf on Process Safety – Process Plant Safety Symposium*, San Antonio, TX, April-May 2013.

[10] 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, Nov 1999, pp. 145-148.

[11] W. M. Goble and J. V. Bukowski, "Development of a Mechanical Component Failure Database," *Proceedings of the 2007 Annual Reliability and Maintainability Symposium*, Orlando, FL, January 2007, pp. 451-455.

[12] J. V. Bukowski and, W. M. Goble, "Validation of a Mechanical Component Constant Failure Rate Database," 2009 *Proceedings Annual Reliability and Maintainability Symposium*, Fort Worth, TX, January 2009, 338-343.

[13] J. V. Bukowski and L. Stewart, "Comparing Failure Rates for Safety Devices: FMEDA Prediction vs OREDA Estimation," exida White Paper available at www.exida.com.
[14] SINTEF, *OREDA Offshore and Onshore Reliability Data Handbook, Vol 1. – Topside Equipment and Vol. 2 – Subsea Equipment*, 6th Ed, OREDA Participants, 2015.
[15] SINTEF, *OREDA Offshore Reliability Data Handbook, Vol 1. – Topside Equipment and Vol. 2 – Subsea Equipment*, 5th Ed, OREDA Participants, 2009.

Revision History

Authors: Julia V. Bukowski, PhD, Loren Stewart

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