Explaining the Differences in Mechanical Failure Rates: FMEDA Predictions and OREDA Estimations

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

July 2015

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

Abstract

This white paper describes the distinction between failure rate prediction and estimation methods in general and then gives an overview of the procedures used to obtain dangerous failure rates for certain mechanical equipment using FMEDA predictions and OREDA estimations. Because the methods are quite different, it is not possible to compare their results directly. A methodology is presented which creates predictions and estimations that are more comparable. The methodology is then applied to specific equipment combinations and the results are compared. When differences in the results exist between the two methods, plausible explanations for the differences are provided. The relative merits of each method are discussed.

Introduction

In determining whether a safety related (sub)system or device will have an acceptable safety performance per national and international safety standards such as [1, 2], arguably the most influential parameter is the dangerous failure rate, λ_D, of the safety related (sub)system or device. All methods of determining λ_D can be broadly classified as prediction or estimation. In one method of prediction, λ_D for a (sub)system or device is derived based on the failure rates for each failure mode of the individual parts that comprise the (sub)system or device taking into account the specifics about the way in which, as well as the environment in which, the (sub)system or device is intended to function. In estimation, λ_D for a (sub)system or device is statistically determined from failure data gathered from a population of fielded (sub)systems or devices. A fuller description of methods for both prediction and estimation along with their advantages and disadvantages is available in [3].

Ideally, prediction and estimation should produce similar values for λ_D for a given (sub)system or device assuming the same application and environmental conditions. However, it is often the case that differences exist between the prediction and the estimation. For some field failure data sets, estimations have been twice as large as predictions. In other estimations, the failure rates have been several times lower than predictions. In this paper, the authors compare λ_D predicted via the failure modes, effects and diagnostics analysis (FMEDA) [4] technique to λ_D estimated by the statistical methods used by the Offshore Reliability Data (OREDA) project [5, 6, 7] and applied to the OREDA database of failures for certain mechanical equipment.

Following a Notation Section, this white paper

- provides sufficient background on FMEDA prediction and OREDA estimation to make the paper self-contained
- describes why a methodology for creating “apples-to-apples” comparisons between the results from the two methods is required
- details what data must be extracted from the published OREDA data in order to produce application specific failure rate estimates
- describes how FMEDA composites are constructed to match OREDA data boundaries
- compares FMEDA predictions and OREDA estimations for λ_D for three specific applications and for two equipment subsystems
- concludes with a discussion of the results and a comparison of the two techniques in general.

Notation

COT	close on trip
ESD	emergency shut down
FFD	field failure data
FMEDA	Failure Modes, Effects and Diagnostic Analysis
OREDA	Offshore Reliability Data
OOT	open on trip
(sub)system	subsystem or system
TSO	tight shut off
λ_D	dangerous constant failure rate

Background

Overview of FMEDA Predictions

The FMEDA technique is performed on a specific device (e.g., ball valve, pressure transmitter, temperature sensor, electronic module, etc.) specified down to the manufacturer and model. Based on the specifics of the design, the parts used to execute the design, the design margins, any automatic diagnostics, the application and the environment in which the device will be deployed, the FMEDA produces predictions for the dangerous detected and undetected failure rates, the safe detected and undetected failure rates, the diagnostic annunciation failure rates, the no effect failure rates, the dangerous and safe diagnostic coverages (for devices with self-diagnostic capabilities), and the useful life. The analysis is application specific because a particular failure mode may be dangerous in one application but safe in a different application; for example, consider the difference when a valve opens on trip (OOT) vs closes on trip (COT). Currently six different environmental profiles for mechanical equipment may be used in the exida FMEDA method. These profiles include cabinet mounted or climate controlled, general field mounted (two versions with differences in internal temperatures), offshore subsea, off shore topside and process wetted.

FMEDA analysis requires a validated database of failure modes and failure rates for the parts which comprise the various devices [3, 8]. This database slightly skews the part failure rates to be certain that the device failure rate will be conservative. However, currently the FMEDA analysis does not account for the effects of site-specific end-user activities. Essentially FMEDA predicts the inherent failure rate of a specific product used in a specific application and environment assuming that end-users will take all appropriate end-user actions to insure that the equipment is appropriate to the task, properly installed and calibrated, and correctly functioning when installed, that all in-service maintenance is correctly and completely performed on schedule, that the equipment is maintained so that proof testing is completely and correctly performed, and that equipment is replaced when its useful life can no longer be extended by maintenance and refurbishment.

Over the years, a large number of devices have been subjected to FMEDA analysis at exida and all FMEDA results have been collected and retained in a FMEDA database (separate and different from the validate parts failure mode and rate database used by FMEDA). The FMEDA's in the database are continuously calibrated against field failure data (FFD) as such data become available. FMEDA's are updated if the parts database changes significantly. Based on this FMEDA database, generic failure rates are published [9] giving the minimum, maximum, mean and 25, 50, 75 and 90 percentile of all failure rates for devices of a common type assuming a specific application and that no diagnostic testing is performed between proof test intervals. Other percentiles can be extracted from the FMEDA database but are not published. Note that the percentiles are not confidence intervals because the FMEDA data does not represent a statistical sample of failures. Rather it provides the known range of failure rate predictions for similar devices which differ by design and manufacture. For example, FMEDA's have been performed on a total of 106 specific ball valves (manufacturer and model). These 106 ball valves include, for example, 31 different floating ball valves, 37 different trunnion-mounted ball valves, etc. The total number of different FMEDA's for ball values is 999 which is large because a specific ball valve may have been subjected to multiple analysis under different applications, environments, levels of diagnostic testing, etc.

Overview of OREDA Estimations

The OREDA project was established in 1981. Its main objective is to "improved safety and cost-effectiveness in design and operation of oil & gas E&P facilities … through collection and analysis of maintenance and operational data, establishment of a high quality reliability database, and exchange of reliability, availability, maintenance and safety (RAMS) technology among the participating companies[5]." OREDA has published six editions of its reliability data handbook in 1984, 1992, 1997, 2002, 2009, and 2015.

OREDA divides equipment according to equipment classes and further subdivides those classes by equipment taxonomy. Boundaries are defined for each (sub)system/equipment taxonomy for which data are collected; the data are environment specific (to subsea and topside). However, in most cases, the lowest level taxonomy includes more than one device. For example, for the subsystem "valves" the boundary includes not only the valve itself but also an actuator and solenoid or pilot valve as well as position monitoring equipment. The data are not specific to a single device much less to a manufacturer and model. A wealth of information for the equipment is published including the following items relevant to the comparisons presented in this paper: population, number of installations, aggregated time in service (both calendar and operational time), failure mode/severity class, number of failures, the mean of the estimated constant failure rate, lower and upper 90% uncertainty level for the estimated constant failure rate, and standard deviation for the estimated constant failure rate under the assumption of multi-sample population and the estimated constant failure rate under the assumption of a homogeneous sample population. Arguably, OREDA has produced the most significant collection of FFD available.

Equipment data collected during certain phases of the OREDA project may or may not appear in a handbook edition published after those phases were complete. So the population size of a given piece of equipment may vary from one handbook edition to the next and may actually decrease in later editions as some data is eliminated. Furthermore, since the data is collected from actual (but unidentified) specific devices and since the specific device distribution is unknown, the results of statistical analysis of the data may or may not apply to a different population or to a particular device. By virtue of the data collection methods, failures initiated by humans are, implicitly, included in the failure rate estimates [5]. This means that the estimated failure rates include not only the inherent product failures but also failures due to site specific end-user actions.

Methodology for Creating "Apples-to-Apples" Comparisons

In many cases, OREDA provides separate failure rate estimates for different severity classes as well as failure rate estimates for each failure mode reported within a severity class. OREDA estimated failure rates are for sub(systems) consisting of several different devices within a defined boundary. On the other hand, FMEDA provides predictions for failure rates for individual specific devices configured for specific applications and environments. These data differences present some challenges in comparing the respective resulting values of means for λ_D. To overcome these challenges, the authors have devised a methodology for ensuring, to the greatest extent possible, that comparisons are made in an "apples-to-apples" manner and where judgements are necessary that they be as safety-conservative as possible.

Extracting Relevant OREDA Data for Comparison to FMEDA Predictions

This methodology is best explained by example beginning with a general description of published OREDA information used, and then relating the information to specifics for a particular safety subsystem. First, consider the type of information available for a subsystem. OREDA provides a diagram defining the boundaries of the subsystem. The population and number of installations from which the data were collected are given. The time in service is recorded as both calendar time and operational time and failure rate estimates are given for both times. However, the authors believe that the failure rates computed using operational time give more accurate estimates. The failures are divided by severity class (critical, degraded, incipient, and unknown) and further subdivided within severity class by failure mode. A given failure mode may appear in multiple severity classes. Estimated failure rates are calculated for the severity class as a whole and for each of the failure modes within a severity class. When data comes from multiple installations, the calculations are made two different ways (as described in [5]) under two different assumptions. One assumption is that the data are homogeneous, i.e., that there is no difference between installations and all data statistically comes from a single sample population. The other assumption is that data from different installations represents multi-sample data requiring additional statistical treatment. There is insufficient information published by OREDA to identify the individual multi-sample subpopulations that make up the entire population. Thus, for purposes of comparison, if a failure rate estimate for one failure mode needs to be combined with a failure rate estimate for another failure mode, it is only possible to perform the combination based on the failure rate estimates under the homogenous assumption.

Now consider a specific example of the above described generalities. For the subsystem called "valves," the OREDA defined boundary includes a valve, an actuator, a solenoid or pilot valve, and position monitoring equipment. More specifically, consider the ESD ball valve data from OREDA. The 2015 edition gives a population of 58 ESD ball valve subsystems from a total of 11 installations (a multi-sample data problem). Time-in-service is recorded as 2.6073 x 10^6 hours calendar time and 2.6046 x 10^6 hours operational time. (Clearly, in this case, there is no loss of generality if failure rates are estimated based solely on operational time.) Table 1 reproduces the relevant OREDA data for the critical severity class which will be used in a numerical example and includes only estimates based on aggregated operational time. Table 2 provides the same information as Table 1 for 23 OREDA ESD gate valve subsystems in service at 6 installations with time-in-service of 1.3696 x 10^6 hours calendar time and 1.3681 x 10^6 hours operational time.

Table 1 A Portion of the Failure Data for ESD Ball Valve from OREDA 2015 Vol. 1

Failure Modes for Critical Severity Class	# Failures	Estimated Failure Rate (per 10^6 hours) Under Assumption Data Is	
		Multi-sample	Homogeneous
All Failure Modes Combined	9	3.45	3.46
External leakage – Process medium	1	0.92	0.38
Fail to close on demand	1	0.34	0.38
Fail to open on demand	2	0.81	0.77
Internal leakage	3	0.87	1.15
Spurious Operation	1	0.44	0.38
Valve leakage in closed position	1	0.42	0.38

Table 2 A Portion of the Failure Data for ESD Gate Valve from OREDA 2015 Vol. 1

Failure Modes for Critical Severity Class	# Failures	Estimated Failure Rate (per 10^6 hours) Under Assumption Data Is	
		Multi-sample	Homogeneous
All Failure Modes Combined	13	8.11	9.50
External leakage – Process medium	1	0.73	0.73
Fail to close on demand	2	1.47	1.46
Fail to open on demand	2	1.88	1.46
Internal leakage	1	0.73	0.73
Spurious Operation	7	4.33	5.12

Note that with the ball valve subsystem for the “all failure modes combined” the multi-sample and homogenous estimates are virtually the same. However, at the level of individual failure modes, the two assumptions may yield estimates that are relatively close or rather distinct. With the gate valve subsystem, for the “all failure modes combined” the multi-sample and homogeneous estimates are different. At the level of individual failure modes, again the two assumptions may yield estimates that are relatively close or rather distinct. Although the multi-sample estimates may provide more relevant information in some cases, the fact that they cannot be combined across failure modes means that they have limited value for our purposes of comparisons.

In comparing dangerous failure rates from OREDA estimates and FMEDA predictions for a ball valve, it may be tempting, for example, to compare the OREDA mean estimate for “all failure modes combined” from the critical severity category and the average FMEDA prediction for all FMEDA’s for ball valves as these seem (at first glance) to be the comparable parameters. In this case, the flawed comparison would be between the OREDA estimate of 3.45 per 10^6 hours and the average prediction for all ball valve FMEDA’s of 0.79 per 10^6 hours leading to the erroneous conclusion that OREDA and FMEDA data are in no way comparable. Such a comparison and conclusion would be wrong for at least two reasons.

First, note that not all of the failure modes in the critical severity category can belong to a particular application. For example, if a valve is used in a "close on trip" application, "fail to open on demand" is not a valid dangerous failure mode for that application. Yet the "fail to open on demand" failure mode and rate appear in the overall critical severity estimated failure rate! Clearly, the overall critical failure rate is not an "apples-to-apples" comparison with FMEDA predictions. In comparing OREDA estimates to FMEDA application specific predictions the OREDA estimates should include only those OREDA failure modes which FMEDA also uses to predict dangerous failures in a particular application. To complicate matters, some of the failure modes may be either safe or dangerous (relative to a particular application configuration) but OREDA's limited failure mode descriptions make it impossible to know how the particular OREDA failure mode should be classified. In keeping with the stated policy of making safety-conservative decisions, a failure mode that would be included by FMEDA and which could be dangerous **or** safe in a given application is fully included in dangerous failure rate calculations even though there is insufficient information to know for certain if every actual field failure of this mode was dangerous or not.

As examples of extracting OREDA data to match application specific FMEDA data, consider the OREDA ball valve and OREDA gate valve subsystems. The most common applications for these valves are COT, Tight Shut Off (TSO), and OOT. As COT and TSO have the same underlying dangerous failure modes, they are treated as a single application labeled COT/TSO. Table 3 categorizes the critical failure modes from the OREDA ESD ball valve data as conservatively belonging to COT/TSO and/or OOT and using the homogeneous critical failure modes in each application to form OREDA application-specific estimates for λ_D. Table 4 does the same for OREDA ESD gate valves. The total estimated dangerous failure rate for each application is formed by summing the individual failure mode estimated λ_D's. Note that the failure mode "spurious operation" is not included in either COT/TSO or OOT as this failure mode is generally associated with safe failures. The external leakage failure mode is not included in either COT/TSO or OOT because this failure mode is not used by FMEDA to calculate λ_D as it is not considered a dangerous failure mode relative to the valve safety function. However, external leakage failure rate is always noted on FMEDA reports since external leakage would cause a hazard if the process medium were dangerous to humans or the environment.

Table 3 Summary of Critical Failure Modes

Included in Estimates of λ_D Based on OREDA ESD Ball Valve Data

	Estimates of λ_D based on OREDA Critical Failure Modes (per 10^6 hours)	
Failure Mode	COT/TSO Application	OOT Application
External leakage – Process medium	N/A	N/A
Fail to close on demand	0.38	N/A
Fail to open on demand	N/A	0.77
Internal leakage	1.15	1.15
Spurious operation	N/A	N/A
Valve leakage in closed position	0.38	N/A
Total OREDA Estimated λ_D per Application	1.91	1.92

Table 4 Summary of Critical Failure Modes

Included in Estimates of λ_D Based on OREDA ESD Gate Valve Data

	Estimates of λ_D based on OREDA Critical Failure Modes (per 10^6 hours)	
Failure Mode	COT/TSO Application	OOT Application
External leakage – Process medium	N/A	N/A
Fail to close on demand	1.46	N/A
Fail to open on demand	N/A	1.46
Internal leakage	0.73	0.73
Spurious operation	N/A	N/A
Total OREDA Estimated λ_D per Application	2.19	2.19

Constructing Composite FMEDA'S to Match OREDA Boundaries

The second point to note is that the OREDA data labeled "ESD Ball Valve" and labeled "ESD Gate Valve" contain additional devices besides the ball or the gate valves. So in comparing OREDA estimates to FMEDA predictions (which are only for individual devices and not composite subsystems), it is necessary to construct composite FMEDA predictions including the additional devices. To construct a composite FMEDA "ESD Ball Valve Subsystem" matching the OREDA boundaries, the application appropriate FMEDA predictions for average dangerous failure rates for ball valves, actuators, and solenoids must be summed. (The monitoring equipment included in the OREDA boundary for "valve" is not included in these comparisons because it is not part of the same safety function as the valve.) The construction of a composite FMEDA "ESD Gate Valve Subsystem" matching OREDA boundaries is handled similarly but must take into account the fact that some individual devices called gate valves include actuators while other individual devices are just gate valves. Tables 5 and 6 show how the composite FMEDA predictions for λ_D were calculated.

Table 5 Construction of Composite FMEDA Predictions for ESD Ball Valve Subsystems

Application	COT		TSO		COT/TSO		OOT	
Device	# FMEDA	Mean ($/10^6$hr)	# FMEDA	Mean ($/10^6$hr)	# FMEDA	Mean ($/10^6$hr)	# FMEDA	Mean ($/10^6$hr)
Ball	61	0.55	60	1.37	121	0.96	59	0.39
Actuator	41	0.54	41	0.54	41	0.54	41	0.54
Solenoid	76	0.36	76	0.36	76	0.36	76	0.36
Total λ_D		1.45		2.27		1.86		1.29

Table 6 Construction of Composite FMEDA Predictions for ESD Gate Valve Subsystems

Application	COT		TSO		COT/TSO		OOT	
Device	# FMEDA	Mean (/10^6hr)	# FMEDA	Mean (/10^6hr)	# FMEDA	Mean (/10^6hr)	# FMEDA	Mean (/10^6hr)
Individual Gate	4	0.333	4	0.785	8	0.559	4	0.264
Individual Actuator	41	0.539	41	0.539	41	0.539	41	0.539
Individual Gate/Act Average	164* Combin-ations	0.872	164*	1.324	328*	1.098	164*	0.803
Gate/ Actuator Combo	5	0.663	4	1.637	9	1.096	4	0.591
Average All Gate/ Actuator	169	0.866	168	1.331	337	1.098	168	0.798
Solenoid	76	0.362	76	0.362	76	0.362	76	0.362
Total λ_D		1.228		1.693		1.460		1.160
*Summing the averages of 4 gates and 41 actuators is equivalent to finding the average of all 164 possible combinations of gates and actuators. Similarly for 328.								

Examples Comparing FMEDA Predictions and OREDA Estimations

Table 7 shows a comparison of OREDA estimates and composite FMEDA predictions for the $\lambda_{D,}$ for COT, TSO, COT/TSO (combined) and OOT applications, and for both the OREDA ESD Ball Valve and OREDA ESD Gate Valve subsystems. For dangerous FMEDA predicted failure rates, the minimum and maximum composite failure rates are also provided.

Table 7 Comparison of OREDA Based Estimates and Composite FMEDA Predictions

for Two Different Valve Subsystems

	Failure Rates (per 10^6 hours)							
	ESD Ball Valve Subsystem				ESD Gate Valve Subsystem			
Application	COT	TSO	COT/TSO	OOT	COT	TSO	COT/TSO	OOT
FMEDA $\lambda_{D\ MAX}$	3.95	5.10	5.10	3.63	3.66	5.79	5.79	3.60
OREDA λ_D	1.91	1.91	1.91	1.92	2.19	2.19	2.19	2.19
FMEDA $\lambda_{D\ AVG}$	1.45	2.27	1.86	1.29	1.23	1.69	1.46	1.16
FMEDA $\lambda_{D\ MIN}$	1.45	1.25	0.70	0.51	0.46	0.98	0.45	0.42

Discussion

The above comparisons show that the OREDA failure rates are well within the range of the FMEDA results. The comparisons also show that, with two exceptions discussed below, the average FMEDA predictions for dangerous failure rates are only slightly less than those of the OREDA estimations.

The two exceptions in Table 7 where FMEDA average values are higher than OREDA are both for the ball valve subsystem and both involve the TSO application prediction. TSO failure modes are the same as COT failure modes; the difference is that the requirements for successful TSO are much more severe. For example, after closure of the valve, only very small values of leakage (ANSI Class 6) are acceptable in TSO whereas some COT applications allow for minimal leakage (ANSI Class 4) after closure. Consequently, a given ball valve will have a higher predicted failure rate in a TSO application than in a COT application. Since there is no indication in the OREDA data what the distribution of applications were for the sampled population, the lower OREDA estimate for λ_D compared to the TSO prediction may merely be reflective of the fact that most or even the entire OREDA population of ESD ball valve subsystems was of the COT application type, in which case the comparison is favorable. However, there is really no way to know. The higher predicted λ_D for the TSO application results in the combined COT/TSO prediction being higher than the COT prediction alone and nearly equal to the OREDA estimate.

In addition to the TSO issue, there may be other reasons that FMEDA and OREDA are not quite the same:

- The monitoring equipment included in the OREDA boundary may have contributed to the failures counted in that analysis leading to a higher failure rate.
- The population included in the OREDA analysis may not represent the full range of designs included the FMEDAs.
- The OREDA data includes site specific human-induced failures.

The authors believe that the most significant factor influencing these differences is that OREDA estimates implicitly include failures initiated by humans whereas the FMEDA predictions assume a safety culture / operational excellence as required by functional safety standards.

The issue of human-initiated failures is an interesting one. It is not uncommon when comparing FMEDA predictions for product inherent failure rates to estimated failure rates based on FFD (other than OREDA data) to find the estimated rates are two times or more the FMEDA predictions [10]. The authors are also aware of a specific comparison of FFD failure rate estimations to FMEDA predictions for a particular device at a single facility where, unlike OREDA data, the device field failures could be sorted into those inherent to the product and those directly initiated by humans. The overall FFD estimates were about twice the size of the FMEDA predictions. However, in that specific comparison, FMEDA predictions of inherent product failure rates compared very favorably with FFD estimates based *solely on inherent product failures* [11]. The remaining failures were attributable to humans at that specific site.

It is essential that realistic failure rates including these site-specific failures be included in PFDavg calculations. However, it is preferable that the safety culture / operational capability of a site be evaluated and directly modeled in the PFDavg calculation. This provides more accurate results than simply using an average for all sites. Detailed study of the field failure reports shows that more than failure rates are impacted by the key variable of operational capability. Probability of successful repair, probability of successful proof test, proof test schedule, and failure rates are different depending on this key variable.

Operational capability evaluation and modeling techniques have been developed [10] and are available in PFDavg calculation tools [12].

In comparing the FMEDA and OREDA methods themselves the following observations are relevant. The FMEDA prediction technique provides direct prediction which is device, application and environment specific. It is easy to construct composite FMEDA's for specific combinations of devices for a given application and environment. For each specific application, FMEDA analysis includes all known failure modes and can predict the failure rates for each failure mode individually. FMEDA allows for the prediction of failure rates for new device designs and for existing devices when there is little or no quality FFD available for estimations.

OREDA data is based on (sub)systems containing multiple devices, not on individual devices. Further, there is no indication of the specific devices (manufacturers and models) nor their particular applications included in the (sub)system overall population. It is unlikely that failure rate estimates for individual devices and applications can be extracted from OREDA data. OREDA estimations are provided by failure mode for given severity levels. Only failure modes experienced and reported are included in the data. The failure mode descriptions are often insufficient to determine if the failure mode resulted in an actual field failure that was dangerous or safe since there is no way to know the specifics of the application. Extracting failure rate estimations for combinations of devices for specific applications is cumbersome and requires expert knowledge regarding what failure modes may be relevant to a specific application. Despite these limitations, it should be noted that OREDA data represents some of the best FFD available.

Therefore, it is reasonable to conclude that, when compared in an "apples-to-apples" fashion, for the equipment analyzed in this paper, the FMEDA predictions and OREDA estimations are quite comparable.

References

1. ANSI/ISA SP84.00.01 – 2004 (IEC 61511 Mod.), Application of Safety Instrumented Systems for the Process Industries, Raleigh, NC, ISA, 2004.
2. IEC 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems, Geneva, Switzerland, 2010.
3. Bukowski, J. V. and Goble, W. M., "Properly Assessing Mechanical Component Failure Rates," *2012 Proceedings Annual Reliability and Maintainability Symposium*, Reno, NV, January 2012, pp. 1-7.
4. Goble, W. M., and Brombacher, A. C., "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.
5. SINTEF, *OREDA Offshore and Onshore Reliability Data Handbook, Vol 1. – Topside Equipment and Vol. 2 – Subsea Equipment*, 6th Ed, OREDA Participants, 2015.
6. SINTEF, *OREDA Offshore Reliability Data Handbook, Vol 1. – Topside Equipment and Vol. 2 – Subsea Equipment*, 5th Ed, OREDA Participants, 2009.
7. SINTEF, *OREDA Offshore Reliability Data Handbook, Vol 1. – Topside Equipment and Vol. 2 – Subsea Equipment*, 4th Ed, OREDA Participants, 2002.
8. Bukowski, J. V. and Goble, W. M., "Validation of a Mechanical Component Constant Failure Rate Database," 2009 *Proceedings Annual Reliability and Maintainability Symposium*, Fort Worth, TX, January 2009, 338-343.
9. Amkreutz. R. and Stewart, L. *Safety Equipment Reliability Handbook*, 4th ed.,. exida, 2015, (in press).
10. Bukowski, J. V. and Gross, W. M., "A Proposed Framework for Incorporating the Effects of End-User Practices in the Computation of PFDavg," exida white paper, January 2014.
11. Bukowski, J. V., Gross, W. M., and van Beurden, I., "Product Failure Rates vs Total Failure Rates at Specific Sites: Implications for Safety," Proceedings *AIChE 11th Annual Global Conf on Process Safety – Process Plant Safety Symposium*, Austin, TX, April 2015.

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