FMEDA – Accurate Product Failure Metrics

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

November 2018

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

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

Introduction

The letters FMEDA form an acronym for "Failure Modes Effects and Diagnostic Analysis." The name was given by Dr. William M. Goble in 1994 to describe a systematic analysis technique that had been in development since 1988 by Dr. Goble and other engineers now at exida to obtain subsystem / product level failure rates, failure modes and diagnostic capabilities (Figure 1).

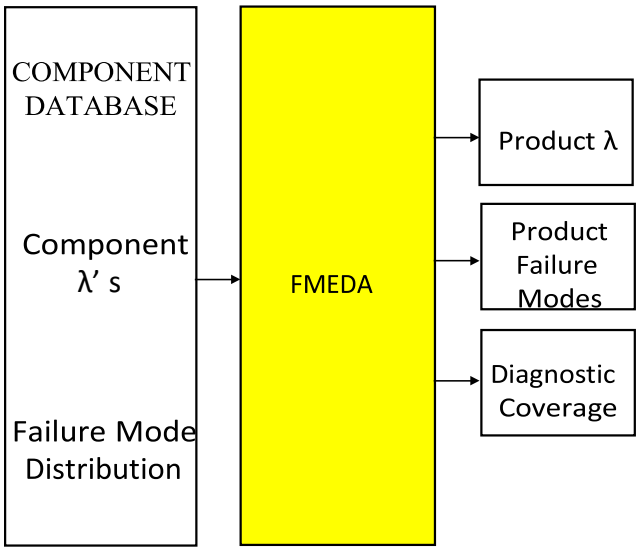


Figure 1: FMEDA Inputs and Outputs.

The FMEDA technique considers

- All components of a design,
- The functionality of each component,
- The failure rates of each component,
- The failure modes of each component,
- The impact of each component failure mode on the product functionality,
- The ability of any automatic diagnostics to detect the failure, The design strength (de-rating, safety factors) and
- The operational profile (environmental stress factors).

Given a component database calibrated with field failure data that is reasonably accurate [EXI06], the method can predict product level failure rate, failure mode and useful life data for a given application. The predictions have been shown to be more accurate [GOB14] than field warranty return analysis or even typical field failure analysis given that these methods depend on reports that typically do not have sufficient detailed information in failure records [GOB09].

FMEA/FMECA

A Failure Modes and Effects Analysis, FMEA, is a structured qualitative analysis of a system, subsystem, process, design or function to identify potential failure modes, their causes and their effects on (system) operation.

The concept and practice of performing a FMEA has been around in some form since the 1960s. The practice was first formalized in the 1970s with the development of US MIL STD 1629/1629A.

In early practice its use was limited to select applications and industries where cost of failure was particularly high. The primary benefits were to qualitatively evaluate the safety and reliability of a system, determine unacceptable failure modes, identify potential design improvements, plan maintenance activities and help understand system operation in the presence of potential faults.

The Failure Modes, Effects and Criticality Analysis FMECA, was introduced to address a primary barrier to effective use of the detailed FMEA results by the addition of a criticality metric. This allowed users of the analysis to quickly focus on the most important failure modes/effects in terms of risk. This allowed prioritization to drive improvements based on cost / benefit comparisons.

The automotive industry has strongly adopted FMEA as a standard design procedure in several variations. The SAE J1739 standard [SAE09] uses the term FMEA to describe the FMECA. It also describes design FMEA (DFMEA) and process FMEA (PFMEA). These are further variations of a fundamental method of detecting errors which is why these methods have proven to be so effective.

FMEDA Development

The Failure Modes, Effects and Diagnostic Analysis (FMEDA) technique was developed in the late 1980's by exida engineers based in part on a paper presented at the 1984 RAMS Symposium [COL84]. The initial FMEDA added two additional pieces of information to the FMEA analysis process. The first piece of information added in an FMEDA is the quantitative failure data (failure rates and the distribution of failure modes) for all components being analyzed. The second piece of information added to an FMEDA is the probability of the system or subsystem to detect internal failures via automatic on-line diagnostics. This is crucial to achieving and maintaining reliability in increasingly complex systems and for systems that may not be fully exercising all functionality under normal circumstances such as a low demand Emergency Shutdown System (ESD).

There is a clear need for a measurement of automatic diagnostic capability. This was recognized in the late 1980's [AME87]. In that context the principles and basic methods for the modern FMEDA were first documented in the book Evaluating Control System Reliability [Gob92]. The actual term FMEDA was first used in 1994 [MOR94] and after further refinement the methods were published in the late 1990s [GOB98a, GOBL98b, GOB99]. The method was explained to members of the IEC 61508 committee in the late 90s and included in the standard as a method of determining failure rate, failure modes and diagnostic coverage for products. FMEDA techniques have been further refined during the 21st century primarily during IEC 61508 preparation work. The key changes have been:

1. Use of Functional Failure Modes;
2. Mechanical Component Usage;
3. Prediction of manual proof test effectiveness; and
4. Prediction of product useful life.

With these changes, the FMEDA technique has matured to become more complete and useful.

Functional Failure Mode Analysis

In the early 2000s functional failure mode analysis was added to the FMEDA process by John C. Grebe. In early FMEDA work, component failure modes were mapped directly to “safe” or “dangerous” categories per IEC 61508. This was relatively easy since everything that was not “dangerous” was “safe” per the IEC 61508:2000 definition. With multiple failure mode categories now existing, direct assignment became more difficult. In addition, it became clear that the category assignment might change if a product were used in different applications. With direct failure mode category assignment during the FMEDA, a new FMEDA was required for each new application or each variation in usage.

Under the functional failure mode approach, the actual functional failure modes of the product are identified during an FMEA, for instance using exida’s ARCHx tool (Figure 2). During the detailed FMEDA, each component failure mode is mapped to a functional failure mode. The functional failure modes are then categorized according to product failure mode in a particular application. This eliminates the need for more detailed work when a new application is considered.

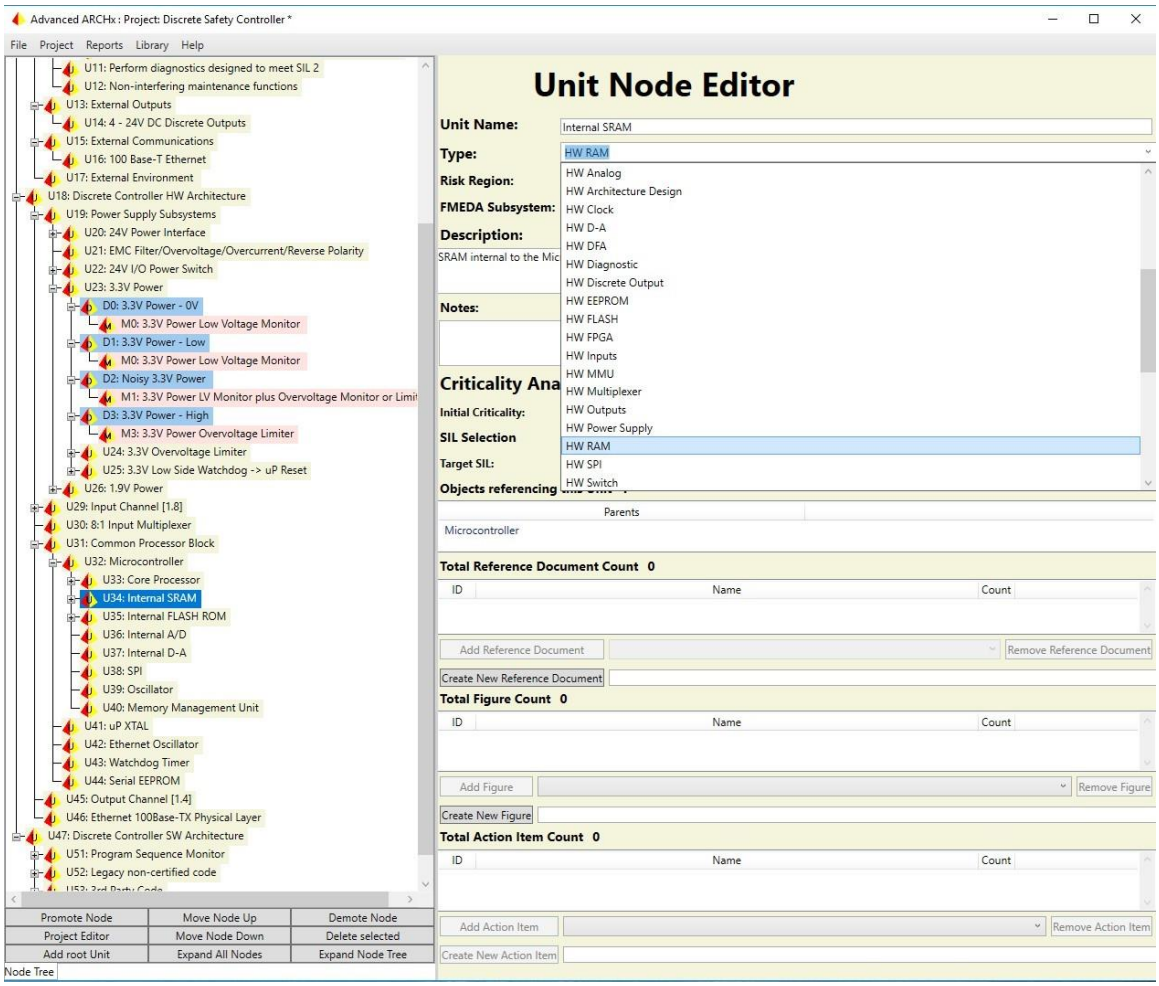


Figure 2: ARCHx architecture analysis tool used for FMEA.

Mechanical FMEDA Techniques

It became clear in the early 2000s that many products being used in safety critical applications had mechanical components and that in many cases these components were the largest contributors to the overall failure rate. An FMEDA done without considering these mechanical components was incomplete, misleading, and potentially dangerous. The fundamental problem in using the FMEDA technique was the lack of a mechanical component database that included part failure rates and failure mode distributions.

Using a number of published reference sources, exida began development of a mechanical component database in 2003 [Gob03]. After several years of research and refinement [GOB07], the database has been published [exi06]. This has allowed the FMEDA to be used on combination electrical / mechanical components and purely mechanical components.

Manual Proof Test Effectiveness

The FMEDA can predict the effectiveness of any defined manual proof test in the same way it can predict automatic diagnostic coverage. An additional column is added to the FMEDA and probability of detection for each component failure mode is estimated. The cumulative effectiveness of the proof test is calculated in the same way as automatic diagnostic coverage.

Product Useful Life

As each component within a product is reviewed, those with a relatively short useful life span are identified. One example of this is an electrolytic capacitor. Many designs have a useful life limitation of 10 years. Since constant failure rates are only valid during the useful life period, this metric is valuable for interpreting FMEDA result limitations.

Recent Developments EMCRH 4th Edition

The 4th edition of exida's Electrical and Mechanical Component Reliability Handbook [EXI13] includes more component types, updated component data, the latest semiconductor technology, and more application conditions.

Component failure rates and failure mode distributions have been derived by exida from the original IEC 62380 numbers modified by hundreds of comparisons with field failure data and root cause analysis of device failures.

The Component Database is validated with over 350 billion-unit field operating hours of equipment data from multiple applications and operating environments making it the global gold standard and ensuring the integrity of the FMEDA results.

The database includes environmental profiles for

Control Room;

Low Power Field Equipment (no self heating);

General Field Equipment (self heating);

Subsea;

Offshore;

Process Wetted Mechanical Components;

Automotive Engine Compartment; and Automotive Passenger Compartment.

These profiles are optimized for maximum accuracy in these common environments.

Site Safety Index

Comparisons of FMEDA results with field failure studies have shown that human factors, especially maintenance procedures, have an impact on the failure rates and failure modes of products. In order to take these factors into account exida has developed the Site Safety Index.

The SSI is a number from 0–4 that indicates the level of site activities and practices that contribute to the safety performance of safety functions on the site. SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site, and therefore there is no degradation in safety performance due to any enduser activities or practices. SSI 0 implies that not much proactive work is done to maintain the safety functions.

Several factors have been identified which impact the SSI. These focus on the quality of:

Commissioning and Safety Validation Testing

Proof Test Procedures, Planning, and Documentation of Tests

Failure Diagnostic and Repair Procedures

Modification Procedures (Making changes is the scariest part of functional safety)

Device Useful Life Tracking and Replacement Procedures

Decommissioning Procedures

FMEDAx™

The FMEDAx™ Tool incorporates the latest innovations in the evolutionary path of the FMEDA method.

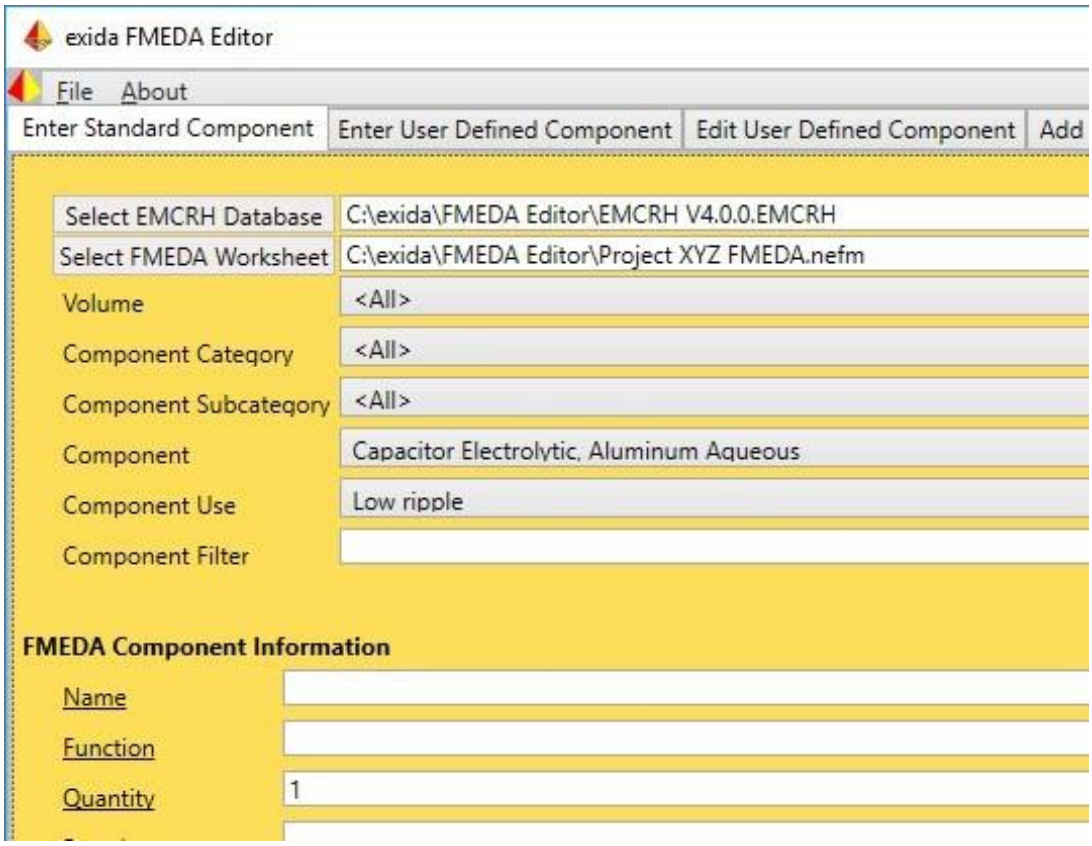


Figure 3: FMEDAx Component Entry Screen

FMEDAx™ uses a functional failure approach which allows design experts to perform the analysis in a realistic way without expert safety knowledge. The results can be categorized by an independent expert for safety usage. This approach also allows easy sensitivity analysis and supports easier FMEDA maintenance when design changes are made.

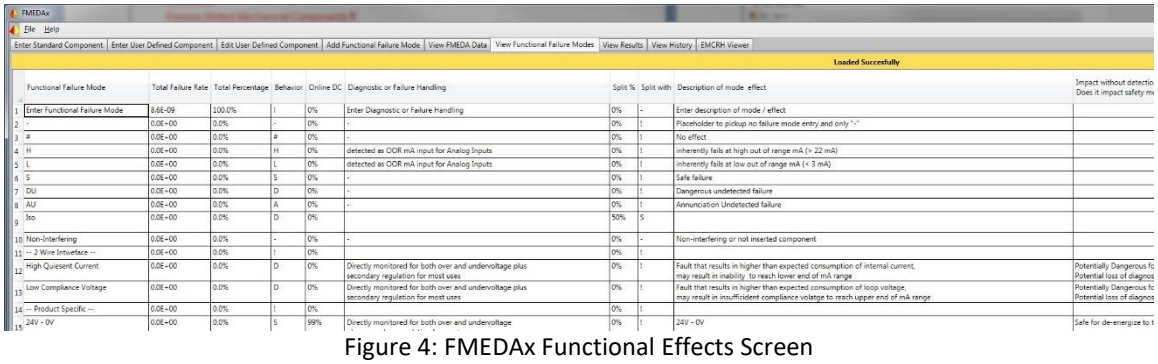
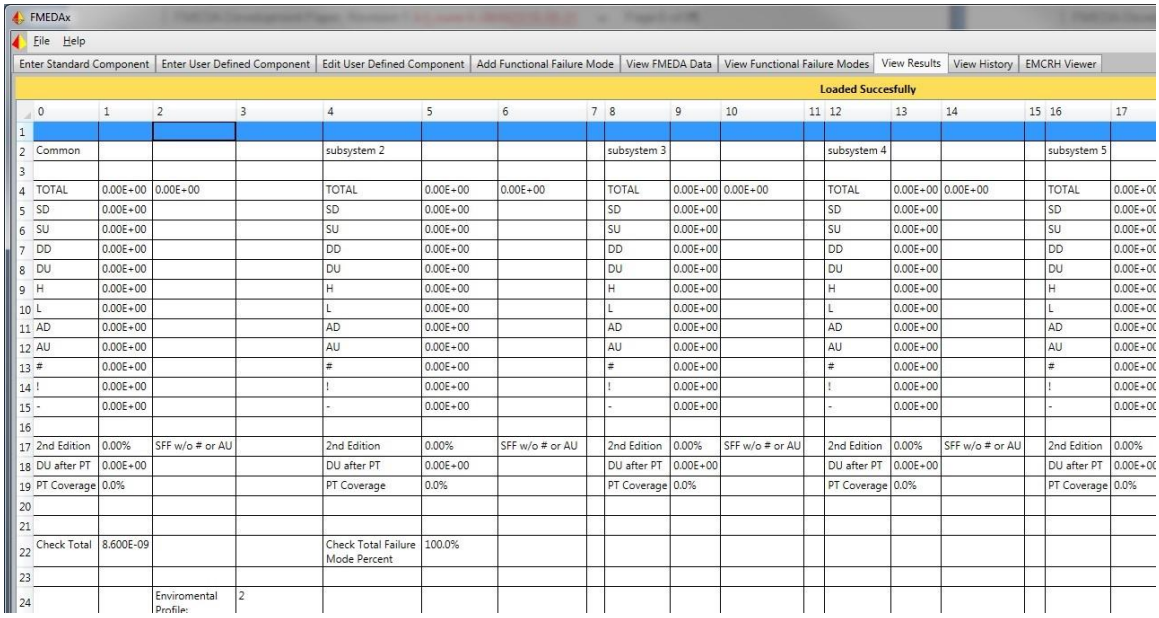


Figure 4: FMEDAx Functional Effects Screen

FMEDAx™ supports separate subsystem analysis. After analysis, subsystems can be combined into a system result. This feature is valuable to reduce rework after a design change and allows different subsystems to be grouped to account for option differences in a product.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1																		
2	Common				subsystem 2				subsystem 3				subsystem 4				subsystem 5	
3																		
4	TOTAL	0.00E+00	0.00E+00		TOTAL	0.00E+00	0.00E+00		TOTAL	0.00E+00	0.00E+00		TOTAL	0.00E+00	0.00E+00		TOTAL	0.00E+00
5	SD	0.00E+00			SD	0.00E+00			SD	0.00E+00			SD	0.00E+00			SD	0.00E+00
6	SU	0.00E+00			SU	0.00E+00			SU	0.00E+00			SU	0.00E+00			SU	0.00E+00
7	DD	0.00E+00			DD	0.00E+00			DD	0.00E+00			DD	0.00E+00			DD	0.00E+00
8	DU	0.00E+00			DU	0.00E+00			DU	0.00E+00			DU	0.00E+00			DU	0.00E+00
9	H	0.00E+00			H	0.00E+00			H	0.00E+00			H	0.00E+00			H	0.00E+00
10	L	0.00E+00			L	0.00E+00			L	0.00E+00			L	0.00E+00			L	0.00E+00
11	AD	0.00E+00			AD	0.00E+00			AD	0.00E+00			AD	0.00E+00			AD	0.00E+00
12	AU	0.00E+00			AU	0.00E+00			AU	0.00E+00			AU	0.00E+00			AU	0.00E+00
13	#	0.00E+00			#	0.00E+00			#	0.00E+00			#	0.00E+00			#	0.00E+00
14	!	0.00E+00			!	0.00E+00			!	0.00E+00			!	0.00E+00			!	0.00E+00
15	-	0.00E+00			-	0.00E+00			-	0.00E+00			-	0.00E+00			-	0.00E+00
16																		
17	2nd Edition	0.00%	SFF w/o # or AU		2nd Edition	0.00%	SFF w/o # or AU		2nd Edition	0.00%	SFF w/o # or AU		2nd Edition	0.00%	SFF w/o # or AU		2nd Edition	0.00%
18	DU after PT	0.00E+00			DU after PT	0.00E+00			DU after PT	0.00E+00			DU after PT	0.00E+00			DU after PT	0.00E+00
19	PT Coverage	0.0%			PT Coverage	0.0%			PT Coverage	0.0%			PT Coverage	0.0%			PT Coverage	0.0%
20																		
21																		
22	Check Total	8.600E-09			Check Total Failure Mode Percent	100.0%												
23																		
24			Enviromental Profile:	2														

Figure 5: FMEDAx Results Screen

The Future

As more data become available, the component database can be refined and updated [EXI12, EXI13] as required by new technology and new knowledge. The success of the FMEDA technique is supplying needed data in a relatively accurate way has facilitated the success of the probabilistic performance approach to design.

References

1. [SAE09] J1739 Surface Vehicle Standard, PA: Warrendale, SAE International, January 2009.
2. [Col84] Collett, R. E. and Bachant, P. W., “Integration of BIT Effectiveness with FMECA,” 1984 Proceedings of the Annual Reliability and Maintainabiltiy Symposium, NY: New York, IEEE, 1984.
3. [AME87] H.A. Amer,and E. J. McCluskey, “Weighted Coverage in Fault-Tolerant Systems,” 1987 Proceedings of the Annual Reliability and Maintainabiltiy Symposium, NY: NY, IEEE, 1987.
4. [BUK07] J. V. Bukowski, “Results of Statistical Analysis of Pressure Relief Valve Proof Test Data Designed to Validate a Mechanical Parts Failure Database,” exida, PA: Sellersville, http://www.exida.com/resources/whitepapers.asp
5. [GOB92] Goble, W.M., Evaluating Control Systems Reliability, Techniques and Applications, NC: Research Triangle Park, Instrument Society of America, 1992.
6. [MOR94] FMEDA Analysis of CDM (Critical Discrete Module) – QUADLOG, Moore Products Co., PA: Spring House, 1994.
7. [GOB98a] 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.

8. [GOB98b] Goble, W.M., Control Systems Safety Evaluation and Reliability, second edition, NC: Research Triangle Park: ISA, 1998.
9. [GOB99] 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.
10. [GOB03] W. M. Goble, "Accurate Failure Metrics for Mechanical Instruments," Proceedings of IEC 61508 Conference, Germany: Augsberg, RWTUV, January 2003.
11. [GOB07] W.M. Goble and J.V. Bukowski, "Development of a Mechanical Component Failure Database," 2007 Proceedings of the Annual Reliability and Maintainabiltiy Symposium, NY: NY, IEEE, 2007.
12. [GOB09] W. M. Goble, "Field Failure Data – the Good, the Bad and the Ugly," exida, PA: Sellersville, http://www.exida.com/resources/whitepapers.asp
13. [GOB14] W.M. Goble and Iwan van Beurden, "Combining field failure data with new instrument design margins to predict failure rates for SIS Verification," exida, PA: Sellersville, Proceedings of the 2014 International Symposium - BEYOND
14. REGULATORY COMPLIANCE, MAKING SAFETY SECOND NATURE, October
15. 28-30, 2014, Hilton College Station-Conference Center, College Station, Texas [EXI06] Electrical & Mechanical Component Reliability Handbook, exida, PA: Sellersville, 2006. See www.exida.com
16. [EXI08] Electrical & Mechanical Component Reliability Handbook, Second Edition, exida, PA: Sellersville, 2008, ISBN-13: 978-0-9727234-6-6, See www.exida.com
17. [EXI12] Electrical & Mechanical Component Reliability Handbook, Third Edition, exida, PA: Sellersville, 2008, ISBN-13: 978-1-934977-04-0, See www.exida.com
18. [EXI13] Electrical & Mechanical Component Reliability Handbook, Fourth Edition, exida, PA: Sellersville, 2018, Database available with the FMEDAx tool, See www.exida.com

Revision History

Authors: John Grebe, Dr. William M. Goble, Rudolf Chalupa

Revision History

Rev. 1.0,	Goble, Grebe	Initial release, February 19, 2007
Rev. 1.1,	Goble, Grebe	Review results included, February 19,2007
Rev. 1.2,	Goble, Grebe	Update, October 22, 2009
Rev. 1.3,	Goble	Update, June 4, 2015
Rev. 1.5,	Chalupa	Added ARCHx and FMEDAx, 2018-09-04
Rev 1.6,	Chalupa, Goble	Added screen shots SAE ref., 2018-11-27

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