FMEDA – Accurate Product Failure Metrics

John C. Grebe
Dr. William M. Goble
exida
Sellersville, PA 18960 USA

Introduction

The letters FMEDA form an acronym for "Failure Modes Effects and Diagnostic Analysis." The name was given by one of the authors in 1994 to describe a systematic analysis technique that had been in development since 1988 to obtain subsystem / product level failure rates, failure modes and diagnostic capability (Figure 1).

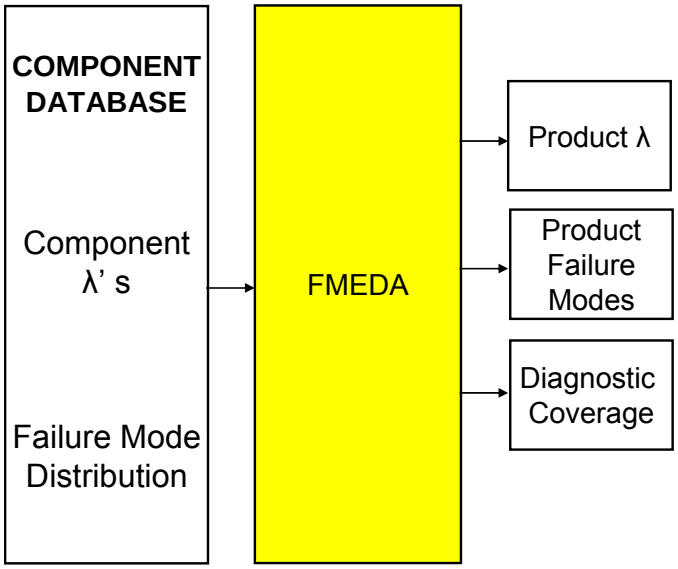

Figure 1: FMEDA Inputs and Outputs.

The FMEDA technique considers

- All components of a design,
- The functionality 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 that is reasonably accurate [EXI06], the method can generate product level failure rate and failure mode data that is more accurate than field warranty return analysis or even typical field failure analysis.

An FMEDA is an extension of the well proven FMEA technique and can be used on electrical or mechanical products [GOB03, GOB07].

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 1960's. The practice was first formalized in 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 is particularly high. The primary benefits were to qualitatively evaluate the safety 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 consequence but still did not address the likelihood or probability of the failure mode which is just as important in prioritization to drive improvements based on cost / benefit comparisons.

FMEDA Development

The Failure Modes, Effects and Diagnostic Analysis, FMEDA, technique was developed in the late 1980's based in part on a paper in the 1984 RAMS Symposium [COL84]. The 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 ability of the system or subsystem to detect internal failures via automatic on-line diagnostics. This is crucial to achieving and maintaining reliability in increasing 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 System.

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 1990's [GOB98a, GOBL98b, GOB99]. FMEDA techniques have been further refined during the 2000's primarily during IEC 61508 preparation work. The key changes have been:

1. IEC 61508 Failure Mode Definitions – New Definitions
2. Functional Failure Modes
3. Mechanical Component Usage

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

FMEDA – IEC 61508

The IEC 61508 standard officially recognizes the FMEDA technique and most IEC 61508 assessment bodies rely upon FMEDA results to verify that sufficient safety has been achieved for a particular application. Within the field of functional safety, standardized failure modes are also defined which also helped to improve the ease of performing the FMEDA and interpreting its results.

The official approval of IEC 61508, Part 2 in 2000 provided documentation on what is expected of a FMEDA and how to use the data in the area of functional safety. This has lead to significantly increased use of the FMEDA within the relevant industries and a rapid evolution of the methods and tools with the required component level failure rate and failure mode data.

IEC 61508 use of the FMEDA is focused on determination of two safety integrity measurements; the dangerous undetected failure rate and a metric known as the Safe Failure Fraction, SFF. The SFF represents the percentage of failures that are not dangerous and are detected. However, additional quantitative results important to system level modeling can also be easily derived out of the same FMEDA and this has driven further evolution of the process and enhanced the value of its results while remaining faithful to the original intent of the IEC 61508. Draft versions of future updates of the IEC 61508 standard are now working to capture some of these advancements.

IEC 61508 Failure Mode Definitions

IEC61508 Part 4 (1998) defines a dangerous failure as a failure which "has the potential to put the safety-related system in a hazardous or fail-to-function state." The standard also defines a safe failure as a failure which "does not have the potential to put the safety-related system in a hazardous or fail-to-function state." IEC61508 Part 2 further explains a "safe" failure as a failure leading to a safe shut-down or having no impact on the safety integrity of the E/E/PE safety-related system.

This significantly simplified and ambiguous definition of a safe failure, if followed, literally leads to results that do not provide data that is very relevant to applications and leads to multiple unanticipated interpretations of the standard. Some of these interpretations can provide unintended loop holes that result in circumstances where the addition of unrelated functionality to a product can improve the SFF metric without any improvement in safety integrity.

New Failure Mode Definitions

Key players in the industry, including exida, are dedicated to improvement of functional safety while remaining faithful to the original intent of IEC61508. exida has proposed multiple refinements to the failure mode definitions and began using those new definitions in 2003 when doing FMEDA analysis. The more refined failure mode definitions are expected to be included in subsequent versions of IEC 61508. To understand the required changes it is first necessary to better understand the ambiguity of the current official definition of "safe failure."

As currently defined a safe failure includes all failures not considered dangerous. This includes "failure leading to a safe shut-down or having no impact on the safety integrity of the E/E/PE safety-related system." A failure that has no impact on the safety integrity function would most likely not even be noticed by a user of the product and can fall into two general categories.

No Impact – Category 1, No Effect

Most components have multiple failure modes and these failure modes are more or less important depending on how they are used within a particular design. For instance failure modes of a resistor include change in value within the range of one-half to two times its original value, open circuit and short circuit faults. If this resistor is used as part of an analog circuit monitoring a particular voltage or current level, the drift failure mode will directly result in a significant error in measurement and most likely be dangerous.

If the same resistor was used in series with the base of a transistor used to drive an on-off relay coil, the product would most likely continue to operate and produce the desired output state even if the resistor drifts over this relatively wide range of values. Resistor drift in this application has no effect of the functionality. Therefore this failure mode is called **"No Effect"** as although the component is part of the desired function this particular failure mode has no effect on the desired function. If this resistor were to fail open circuit there would be an impact on the function so all failure modes of the component cannot be ignored.

No Impact – Category 2, Not a Part

The purpose of some components is to support human interface display and auxiliary functions that are not part of the circuitry providing the functionality of the product being relied upon for the application. For instance a resistor can be used to set the current level for an indicating LED that lights up when

communications are taking place so that it can be easily seen if communications are active. Failure of the resistor such that the LED does not light up during communications has no impact on the normal operation of the product. In fact any of the failure modes of the resistor are unlikely to impact performance of the function of the product. This category of components are referred to as **"Not a part"** since they are not a part of the implementation of the desired function.

New Definition of "Safe" Failures

Note that "no effect" refers to one particular failure mode of a component that is used by the desired function (and other failure modes of that part will lead to loss of function) and "not a part" refers to an entire component that is not necessary or used in the implementation of the desired function but both can be considered "safe" by the current IEC61508 definition.

A more useful and non-ambiguous definition of a safe failure in the context of a safety system is one that leads to a false trip (in the absence of a fault tolerant architecture) which is clearly the opposite of a dangerous failure (failure to perform the safety function or inability to trip when needed). This definition of "safe" also has the additional benefit of providing an estimated false trip rate for a safety product which is also very important to a potential user of the product as it typically leads to lost production and is possibly an initiating event for another hazard scenario.

Safe Failure Fraction calculation

The remaining question is how the "No Effect" and "Not a part" failure rates are used (or not used) in the calculation of the SFF. The most conservative method is to exclude both from the calculation which provides the lowest SFF estimate for a product. This approach only considers the safe and dangerous failures as those that directly impact the desired safety function. This policy was followed by conservative vendors including exida once the problem was recognized in the time period approximately represented by the years 2000 through 2002.

It is clearly bad policy to count the "Not a part" failures as "safe." This is because a product designer with a design that is close to a particular SFF threshold could potentially reach that threshold by adding extraneous components which provide no improvement for safety functionality.

Around the year 2003 the consensus of the key industry experts in this area settled on interpretation of the original "safe failures" as the newly defined safe failures plus No Effect but excluding Not a Part failures. The results in the sum of the newly defined safe failure and the no effect failures being used for the safe failure portion of the SFF calculation and the "Not a part" failure rates are not considered relevant to safety calculations. FMEDA result reports began publishing numbers for the additional failure rate categories.

The result of this change is that the total failure rate reported by the FMEDA represents the total failure rate for all the components even if some of those failure rates do not lead to an observable failure at the product level. Observed failure rates at the product level are predicted by the total failure rate minus the no effect failure rate because the no effect failures would, in most cases, only be discovered by full parametric testing of the individual components.

Functional Failure Mode Analysis

Also in the early 2000's functional failure mode analysis was added to the FMEDA process. 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." 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 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.

Mechanical FMEDA Techniques

It became clear in the early 2000's that many products being used in safety critical applications had mechanical components. An FMEDA done without considering these mechanical components was incomplete and potentially misleading. 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 a few 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.

The Future

This paper explains how FMEDA techniques have evolved over the past decade since the first efforts to define the process were made. One result of this is that

older FMEDA reports (2002 and before) should not be used and should never be compared to newer work.

It is clear that further refinement of the component database with selective calibration to different operation profiles is needed. In addition, 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. As more data becomes available, these factors can also be added to FMEDA analysis.

References

[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.

[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.

[GOB92] Goble, W.M., Evaluating Control Systems Reliability, Techniques and Applications, NC: Research Triangle Park, Instrument Society of America, 1992.

[MOR94] FMEDA Analysis of CDM (Critical Discrete Module) – QUADLOG, Moore Products Co., PA: Spring House, 1994.

[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.

[GOB98b] Goble, W.M., Control Systems Safety Evaluation and Reliability, second edition, NC: Research Triangle Park: ISA, 1998.

[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.

[GOB03] W. M. Goble, "Accurate Failure Metrics for Mechanical Instruments," Proceedings of IEC 61508 Conference, Germany: Augsberg, RWTUV, January 2003.

[EXi06] Electrical & Mechanical Component Reliability Handbook, exida, PA: Sellersville, 2006. See www.exida.com

[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.

Revision History

Rev. 1.0,	Goble, Grebe	Initial release, February 19, 2007
Rev. 1.1,	Goble, Grebe	Review results included, February 19,2007