Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26153-cd

Failure Mechanisms, Modes, Effects, and Diagnostics Analysis – a Novel Approach to Include Predictive Health Monitoring into Functional Safety

Jens Warmuth
Fraunhofer Institute For Integrated Circuits IIS, Germany. E-mail: jens.warmuth@iis.fraunhofer.de

This paper proposes a novel approach that integrates modern Reliability Engineering methods, specifically various types of Predictive Health Monitoring (PHM) into the Functional Safety analysis technique of Failure Modes, Effects, and Diagnostics Analysis (FMEDA). This new method is named Failure Mechanisms, Modes, Effects, and Diagnostics Analysis (FMMEDA). FMMEDA can serve as a drop-in replacement for FMEDA, delivering the same hardware-architectural metrics defined in IEC 61508 or ISO 26262. Although it is an open approach compatible with many techniques, this paper focuses on two primary types of PHM. The first type relies on Early Damage Detection. In this case, damage caused by a Failure Mechanism is already detectable before functional Failure manifests through the associated Failure Mode. The second type comprises Physics of Failure based approaches that use sensors to monitor stress parameters and model Remaining Useful Life (RUL). The FMMEDA for both types of PHMs is discussed as well as their principal advantages and limitations. Finally, example implementations of both PHM types are presented and abbreviated FMMEDAs are performed to illustrate the usage of this new analysis method.

Keywords: Safety, Reliability, Predictive analytics, Prognostics and health management, FMEA, FMEDA

1. Introduction

The Failure Mode Effects Analysis (FMEA) has been a staple of reliability engineering since its inception about eighty years ago. Barsalou (2024)

Generally FMEA is a qualitative approach, that does not take precise numbers into consideration. While a ranking of Failure Modes is possible it can never be absolute and only be used inside of a single FMEA or groups of similar FMEAs. IEC (2006)

With the publishing of the general functional safety standard IEC 61508 a quantification of the FMEA was born, now called the Failure Mode Effects and Diagnostics Analysis (FMEDA). The FMEDA was adapted in the automotive functional safety norm ISO 26262, that defined the FMEDA much clearer and provided flow charts for ease of application. IEC (2010), ISO (2018)

Unlike the general FMEA method, that can be used in a lot of different contexts e.g. design, process or software, the FMEDA is usually reserved for (electronics) hardware evaluation.

After publishing of the IEC 61508 in 1998, reliability engineering developed into new directions. Safety standards did not keep pace with these developments and included them very slowly if at all.

Reliability engineering research over the last decades has made significant advances in predicting Failure, the so called Predictive Health Monitoring (PHM). Modern computing power made it possible to use material science in combination with modeling and simulation software, to get much better predictions of reliability. Together with new highly integrated sensors and either edge computing or cloud based approaches, it became even possible to tailor reliability predictions individually during the lifetime of a specific system or detect damage before Fault can occur, thereby preventing Failure. These developments also included development of the FMEA into an Failure Mechanisms, Modes and Effects Analysis (FMMEA). However quantitative safety analyses such as the FMEDA were not considered. Pecht (2009)

This paper describes a new approach of including different modern reliability prediction techniques into the FMEDA. It shows that these techniques can make a significant contribution to the safety of systems and how such proactive approaches can be used to support, enhance, and in

part replace classic purely reactive Safety Mechanisms.

First, important terms of reliability engineering and functional safety used in this paper are explained and a brief description of generalized FMEA and FMEDA is given. The main part of the paper introduces the Failure Mechanism, Mode, Effects and Diagnostics Analysis (FMMEDA), the proposed extension of the FMEDA to include modern reliability prediction techniques. Next, highly abbreviated examples from current developments in predictive reliability will be used to illustrate the application of the new FMMEDA approach. Finally, the new approach is discussed regarding its potential and limitations.

2. Terms and Concepts

While some terms are often used in daily engineering parlance, they are not absolutely and clearly identically defined across standards. The definitions used in this paper derive mostly from the ISO 26262 and in part from the IEC 61508. Some terms that are idiosyncratic to the ISO 26262 standard have been abstracted to be more easily understood by non-experts in the ISO 26262 and to be more easily used in the context of this paper. IEC (2010), ISO (2018)

(i) **Diagnostic Coverage (DC)** Percentage of (potential) Faults that are detected and prevented from becoming Failures by the Safety Mechanism
(ii) **Element** System, Sub-System or component
(iii) **Failure** Termination of an intended behavior of a system, sub-system or component
(iv) **Failure/Fault Mechanism (FMech)** The physical process by which a Failure or Fault is caused
(v) **Failure Mode (FM)** Manner in which a system or sub-system or component fails to provide the intended behavior
(vi) **Failure Rate** λ Probability density of Failure divided by probability of survival for a hardware component. Normally given in units of FIT = 1 Failure / 10^9 hours (of operation). It is assumed to be constant in all functional safety standards and in this paper.
(vii) **Fault** Abnormal condition that can cause a component or system to fail
(viii) **Probability (or average frequency) of dangerous Failure per Hour (PFH)** Rate of Failures that are not covered or not prevented by a Safety Mechanism and manifest in the system leading to dangerous conditions for the life and health of humans or other things deserving protection.
(ix) **Safe Failure Fraction (SFF)** Ratio of safe as such, safe by design, or prevented Failures to the absolute expected Failure Rate without any design measures or Safety Mechanisms.
(x) **Safety Mechanism (SM)** Function that is implemented in an Element to detect Faults and prevent them from turning into Failures. Can be software, hardware, or a combination thereof.

3. FMEA and FMEDA

3.1. *FMEA*

An FMEA is the process of identifying the Failure Modes of parts of a system, i.e. sub-systems, components, or of the system as a whole. Once a Failure Mode is identified, its possible effects are determined. Normally, their severity, probability of occurrence and probability of detection are also assessed and assigned a (relative) numerical value. By combining these values into a single number, e.g. by multiplication, all Failure Modes of a system can be ranked. In addition, each Failure Mode can also be assigned one or more possible root causes and mitigation techniques or strategies. The technique can be applied to a multitude of systems in the broadest sense, e.g. functionalities, designs, processes, hardware, and software. The work is normally organized by and documented as a table. IEC (2006)

3.2. *FMEDA*

An FMEDA is a special application and extension of the normal FMEA for (electronic) hardware elements to specifically include diagnostics and get quantitative results. As with the FMEA, the FMEDA starts with parts of a system. However, now, Failure Rates (λ) for the individual Elements

λ_E are determined and assigned to them[a]. Like before, Failure Modes are assigned for the different Elements. Unlike in the FMEA however, each Failure Mode is now assigned a percentage of all the possible Failures of the Element. This percentage is designated $\mathrm{Dis_{FM}}$ The Failure Rate for each Failure Mode λ_{FM} can then be calculated.

For the safety critical Failure Modes[b], one or more Safety Mechanisms are assigned. A Diagnostic Coverage is derived as well. For each Failure Mode covered by Safety Mechanisms the prevented Failure Rate λ_{Prev} can be calculated from the Diagnostic Coverage of the Safety Mechanism(s) $\mathrm{DC_{SM}}$ and the Failure Rate for the individual Failure Mode λ_{FM}. Aggregated over all Failure Modes and divided by the Failure Rate of the Element, the derived number is the Safe Failure Fraction[cd]. Additionally, the Probability of dangerous Failure per hour (PFH) is calculated by subtracting the aggregated prevented Failure Rates from the base Failure Rate of the Element.

4. FMMEDA

The central topic of this paper is the introduction of the Failure Mechanism, Mode, Effects and Diagnostics Analysis. It starts in the same way as the FMEDA. Elements are analyzed as parts of a system. For each Element a Failure Rate is determined, as before.

From here, there are two ways to proceed.

4.1. *True Proactive Safety Mechanism*

The first approach is suitable for direct detection of an approaching Fault. One possible PHM technique for this is damage detection, discussed below. But there are other possibilities such as anomaly detection, that could be used here.

The process proceeds as in the FMEDA, determining and assigning Failure Modes, as well as the distribution of the Failure Rate of the Element amongst them. The individual Failure Modes are then assigned Failure Mechanisms. These Failure Mechanisms are in turn assigned a percentage of the Failure Rate of the Failure Mode. It is important to always set one Failure Mechanism as “unidentified Failure Mechanisms”. Part of the Failure Rate of the Failure Mode must be assigned here in order to account for unexpected Faults and Faults that cannot be explained by any Failure Mechanism. In practice, there are always Failures whose cause cannot be determined or that are caused by a Failure Mechanism not accounted for. Expert judgment or field statistics must be applied here. For safety’s sake, it is recommended to be conservative when assigning Failure Rate percentages to a Failure Mechanism other than ”unidentified Failure Mechanisms”, especially when using expert judgment by itself. The reason for this caution lies in the nature of the proactive Safety Mechanism. If the percentage of the Failure Rate assigned to a specific Failure Mechanism is too high, it can directly lead to a situation where the resulting SFF and PFH conform to the needed level but, in fact, the needed risk reduction is not reached.

Now, the Safety Mechanisms for the Failure Modes and Failure Mechanisms are assigned. Assuming that they are functionally independent, their Diagnostic Coverage values can be treated as probabilities, and their combined probability can be calculated as such.

In practice, it has shown itself to be useful to start with the DC of the Safety Mechanisms for the Failure Modes, since each Failure Mode itself is also assigned first and then divided again into different contributing Failure Mechanisms. This makes it easier to work in the familiar table-format used for FME(D)A. However, it is worth noting that a second possibility is to flip the whole process and determine the Failure Mechanism first, directly after assigning the Failure Rate of the Element. The individual Failure Mechanisms are then divided into the Failure Modes. This can be beneficial if it is known, that a Failure Mechanism is contributing to many Failure Modes at the same time. An overview of this approach to the FMMEDA is shown in Figure 2.

[a] Most often on component basis

[b] In this paper all Failure Modes are assumed to be safety critical

[c] Some standards like the ISO 26262 use slightly different metrics based on the same principles. ISO (2018)

[d] It is also possible to analyze multi-point Failures in an analogous way ISO (2018)

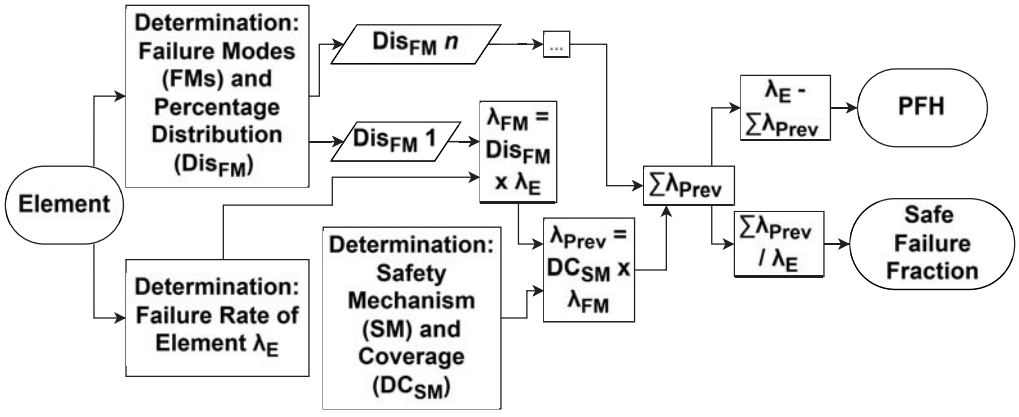

Fig. 1. Flowchart of a simple FMEDA including only one Element.

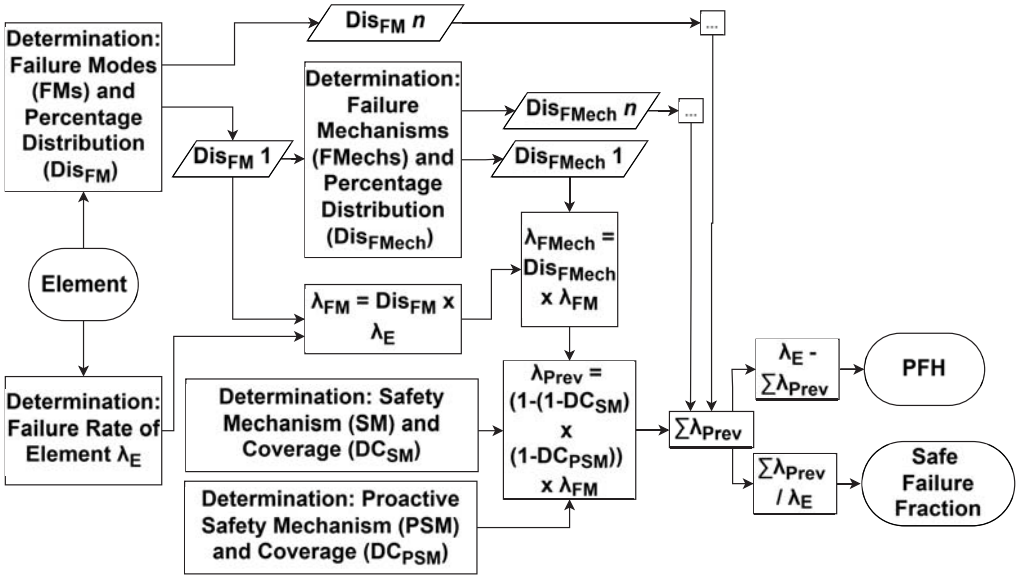

Fig. 2. Flowchart for an FMMEDA including a true proactive Safety Mechanism as well as a classic reactive Safety Mechanism.

4.2. *Failure Rate Lowering Mechanism*

The second approach is suitable for long term and indirect prediction methods. The example method in this paper is using a Physics-of-Failure model of the Element in combination with sensors in the real Element to get an estimate of the Remaining Useful Life (RUL) or the Failure Rate of the component in real time.

This method and others like it should not be used as a Safety Mechanism in a classical sense but rather as a Failure Rate capping technique. It is used to mitigate the need of high safety margins in the Failure Rate. The Failure Rate can be set at a lower level as long as the stress based real time estimation evaluates it accordingly. If measured stress in the field leads the simulation models to conclude higher Failure Rates or a shorter RUL as assumed at design time, measures have to be

taken, e.g.indicate to the operator of the system to do professional maintenance earlier and/or more frequent, to replace parts and keep the Failure Rate caused by specific Failure Mechanisms low. The Failure Rate assigned to the "unidentified Failure Mechanisms" is not influenced by this.

The FMMEDA in this approach always starts with the Failure Mechanisms. All known Failure Mechanisms for the Element are derived and assigned a percentage of the Element's Failure Rate. As before, the "unidentified Failure Mechanisms" Failure Mechanism has to be present and assigned part of the Failure Rate. Afterwards, the Failure Mechanisms are assigned predictive Safety Mechanisms. In contrast to the first FMMEDA approach, these predictive Safety Mechanisms are not combined with the reactive Safety Mechanisms. They rather cut the Failure Rate to a level of the expected environmental and load conditions in the application without using overly high safety margins for edge cases. This is best done by assigning them a DC. This DC is calculated from the Elements base Failure Rate at expected conditions compared to the edge-case conditions previously used for the analysis. By using this DC, it becomes possible to easily calculate the remaining Failure Rates for the covered Failure Mechanisms but leaving the not-covered or unidentified Failure Mechanisms at the level with greater safety margin. Figure 3 shows an overview of the procedure.

5. Application Examples

5.1. *True Proactive Safety Mechanism via Damage Detection*

The example system is a simple power amplifier. It's base concept was developed as a project-showcase for damage detection techniques by a multi-company and research institution consortium Reitz and Warmuth (2023). The FMEDAs and FMMEDAs in this and the following section were done by the author based on the documented work of the project and his own experience. The power amplifier contains as the central component a power MOSFET as a Surface-Mounted Device. The exposed pad in this particular arrangement serves both as a path for heat dissipation as well as the drain connection. For this deliberation, the continuous power supply is safety-critical. The off-state is not per se a safe state but requires other conditions. Hence, the resulting power loss from an open connection is a safety-critical Failure. Table 1 shows an abbreviated FMEDA table for this component. While the Failure Mode open drain-source is already covered by the Safety Mechanism of simple redundancy, this is not enough to reach the desired Safe Failure Fraction of 95%[e].

The Failure Mechanism of exposed pad solder delamination has a considerable contribution to the Failures in the Failure Mode open drain-source[f]. It is therefore to be covered by a dedicated proactive Safety Mechanism. Thermal On-Board Spectroscopy is used. This is a technique making use of changes in thermal impedance to detect damage in the heat conducting path of electronics packaging. Reitz and Warmuth (2023)

If implemented properly, it can reliably show growing damage days before functional Failure occurs and is therefore suitable to be a proactive Safety Mechanism. The confidence level of such a prediction has to be substantiated with extensive tests as with all Safety Mechanisms. However, because of its predictive nature, normally more extensive tests are required. The confidence level here has been chosen very conservatively but gets the Safe Failure Fraction above the required level. Table 2 shows the FMMEDA for the Failure Mode open drain-source with the Safety Mechanism for the exposed pad delamination in place yielding an acceptable Safe Failure Fraction.

Note that this example shows only a small part of the safety case. It also uses a very conservative approach.

[e] While redundancy is often assigned a 99% Diagnostic Coverage, simple homogeneous redundancy should be treated more conservatively. The Failure Modes (and Mechanisms) are the same for both redundant components. Triple redundancy could be used but would lead to considerably more weight, volume, and cost. ISO (2018)

[f] there are of course other Failure Mechanisms like thermal runaway. They can also interact or even cause the delamination. To keep the paper focused and in scope, this will not be taken into consideration here

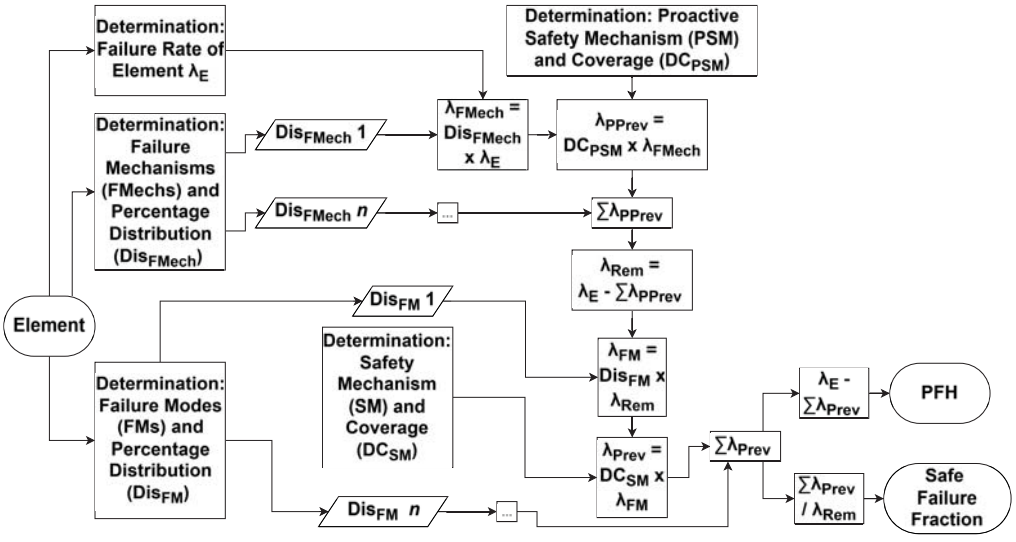

Fig. 3. Flowchart for an FMMEDA including a Failure Rate lowering Safety Mechanism as well as a classic reactive Safety Mechanism.

Table 1. Abbreviated FMEDA for the power amplifier including only the Power MOSFET component. As normal for an FMEDA only reactive Safety Mechanisms are applied.

Element	λ_E	FM	Dis $_{FM}$	λ_{FM}	SM	DC $_{SM}$	λ_{Prev}
Power MOSFET	60	Open drain-source	0.8	48	Simple redundancy	0.9	43.2
		Short drain-source	0.1	6	Simple redundancy	0.9	5.4
		Other	0.1	6	Simple redundancy	0.9	5.4
SUM	60						54
SFF							0.9
PFH							6

5.2. *Failure Rate Lowering Mechanism via Digital-Twin*

Taking the same power amplifier from above we assumed it to have a Failure Rate of 60 FIT. However, field studies on the target application have concluded that some devices experience much harsher environments. They age faster reaching the end of their useful life earlier and the assumed constant Failure Rate also has to be increased. It would be possible to use more resilient devices but this would make large design changes necessary and increase not only unit weight, volume and cost but also reduce performance and effectiveness of the product as a whole. Therefore alternative ways are considered. Temperature sensors are installed in the module containing the power amplifiers at determined spots and a digital twin is built that uses a functional and an FEM model parameter-

Table 2. Abbreviated FMMEDA for the power amplifier including only the Power MOSFET component. Includes both a reactive and a proactive Safety Mechanism.

Element	λ	FM	λ_{FM}	DC_{SM}	FMech	Dis_{FMech}	λ_{FMech}	PSM	DC_{PSM}	$DC_{PSM\&SM}$	λ_{Prev}
Power MOS FET	60	Open drain-source	48	0.9	Delamination of exposed pad solder or pad itself	0.8	38.4	On-Board Thermal Spectroscopy	0.8	0.98	37.6
					Other	0.2	9.6	-	-	0.9	8.6
		Short drain-source	6	0.9							5.4
		Other	6	0.9							5.4
SUM	60										57
SFF											0.95
PFH											3

ized by the sensor data and the electronic load data. With it, first, the remaining useful life can be predicted and the components or whole system replaced before its end is reached. Second, the components Failure Rate from the Failure Mechanisms in the model can be assumed at the level for the actual expected conditions without an overly large safety margin. If they go out of bound, repair or maintenance schedules can be ramped up. Leaving only the Failure Rate resulting from the unidentified Failure Mechanisms to remain at the level used with the higher safety margin[g]. Table 3 and Table 4 show the FMMEDA for this example. Here, the Failure Rate initially is defined to include 100% of observed conditions and still have a safety margin. If the Failure Rate for certain Failure Mechanisms can be assumed to be lower because of on-line monitoring, the overall Failure Rate can be lowered significantly.

6. Discussion

In this paper a novel technique for including Failure Mechanisms into the safety analysis technique FMEDA have been introduced, the Failure Mechanism, Mode, Effects and Diagnostics Analysis. Two different approaches to this FMMEDA useful for either direct detection of approaching Faults or long term indirect prediction of Faults and Failures have been discussed in general and in relation to different prognostic health management techniques. Additionally, their use has been shown in minimal application examples.

The FMMEDA can be included into any safety analysis replacing the FMEDA without disrupting the results of the familiar method. It is therefore possible to introduce this new safety tool gradually into the safety process with minimal effort and only use its full capabilities where suitable. If a certification is deemed contingent on the use of the classic FMEDA by the certification body, the results of both methods are easily output separately without having to do different analyses since the FMMEDA already includes the FMEDA.

This ability to be included into a standard-compliant safety analysis without using a completely different analysis method and still doing an FMEDA sets apart this new approach from existing methods like Event Tree Analysis or Markov Chains. Fault Tree Analysis can also be used to include Failure Mechanisms. However it is an inductive method and not used to derive the Hardware Architectural Metrics such as SFF or PFH. This leads to additional overhead if predictive Safety Mechanisms are to be included in their calculation by using the listed or known possible

[g] A certain safety margin will still be necessary and it is always advisable to be on the side of caution in matters of safety

Table 3. Part of an abbreviated FMMEDA for the power amplifier including only the Power MOSFET component. Only the predictive Failure-Rate lowering Safety Mechanism is included. Continues in Table 4.

Element	λ_{E}	FMech	Dis $_{FMech}$	λ_{FMech}	PSM	DC $_{PSM}$	λ_{Prev}	$\Sigma\lambda_{Prev}$	$\lambda_{E,rem}$
Power MOS FET	140	Solder fatigue, delamination and similar	0.8	112	Model-based live Failure Rate prediciton	0.5	56	56	84
		Other	0.2	28	-	0	0		

Table 4. Part of an abbreviated FMMEDA for the power amplifier including only the Power MOSFET component. Continues from the result from Table 3 and concludes like a normal FMEDA.

Element	$\lambda_{E,rem}$	FM	Dis $_{FM}$	λ_{FM}	SM	DC_{SM}	λ_{Prev}
Power MOSFET	84	Open drain-source	0.8	67.2	Simple redundancy	0.9	60.48
		Short drain-source	0.1	8.4	Simple redundancy	0.9	7.56
		Other	0.1	8.4	Simple redundancy	0.9	7.56
SUM	84						75.6
SFF							0.9
PFH							8.4

methods other than the FMMEDA.

While the FMMEDA is easy to include in a safety design, the method has to be developed further and tested on more real life examples. In the current time of rising complexity of electronic systems and their ubiquitous use in safety relevant applications the reactive Safety Mechanism with its usual large overhead needs to be scaled back. New ways of proactively and predictively preventing Failure are developed and put to use constantly. Especially with AI pattern and anomaly detection, this development will only increase in the next years. Until now, it was not possible to include these predictions in a classic safety assessment. Their use in safety critical applications therefore remained low. The FMMEDA introduced in this paper solves this challenge by providing a framework for including these modern prediction techniques in classic safety assessment.

References

Barsalou, M. (2024). 75 Years of FMEAs: 1949–2024.

IEC (2006). *IEC 60812:2006*. International Electrotechnical Commission.

IEC (2010). *IEC 61508:2010*. International Electrotechnical Commission.

ISO (2018). *ISO26262:2018*. International Organization for Standardization.

Pecht, M. (2009). Failure modes, mechanisms, and effects analysis. In *Product Reliability, Maintainability, and Supportability Handbook*, pp. 203–218. United States: CRC Press.

Reitz, S. and J. M. Warmuth (2023). Automated early damage detection for power mosfets using on-board thermal spectroscopy. In *Proceedings of ITherm 2023*. IEEE.