17th IMEKO TC 10 and EUROLAB Virtual Conference
"Global Trends in Testing, Diagnostics & Inspection for 2030"
October 20-22, 2020.

FMEA analysis and metrology: a beneficial synergy

Loredana Cristaldi[1], Marco Faifer[1], Alessandro Ferrero[1] , Roberto Ottoboni[1]

[1] *Politecnico di Milano, DEIB Department Milano, Italy, Loredana.cristaldi@polimi.it*

***Abstract*—Failure Mode and Effects Analysis (FMEA) is a procedure that is often skipped or not completed generally because of time of financial constraints, despite its proper use during the different steps of the product life cycle (design, development, manufacturing and maintenance) makes it possible to identify and possibly solve potentially critical problems. The most often skipped part of the FMEA procedure is that related to the sensing and measuring equipment, when present. Even when they are considered, the analysis is confined to the possible effects of failures that make them unavailable, while also the deviation from the expected metrological performance (larger uncertainty, as well as unexpected bias) may cause severe malfunctions in the whole system. This paper proposes a possible way to consider also the metrological performance of the sensing elements in the FMEA analysis and shows, also with a practical example, how they can be taken into account.**

Keywords— FMEA, Measurement uncertainty, Target uncertainty, Errors, Failures

I. INTRODUCTION

The Failure Mode and Effects Analysis (FMEA) [1] is an analysis method aimed at supporting designers in defining the characteristics of the system under development, and is based on the systematic analysis of the failure modes with the final goal of improving the intrinsic reliability of the whole system. Actually, it is an iterative method aimed at identifying, since the design stage, the failure modes and showing the potential effects on the system, so that the causes can be detected and the suitable corrective actions can be implemented.

It is also possible to classify the failure modes according to their severity (known also as fault severity) and the occurrence probability, thus obtaining a criticality index that changes a qualitative tool (the FMEA) into a quantitative tool: the FMECA, or the Failure Mode, Effects and Criticality Analysis. It can be readily perceived that the information provided by the FME(C)A can be usefully exploited in setting the operative constraints and the preventive maintenance operations, and fault and malfunction risk minimization is its most significant outcome. When the costs of a missing process quality are considered, not applying this process may have a cost that can easily offset the cost, both financial and in terms of dedicated time, of applying it [1]–[3].

An important and often critical components of nowadays complex systems is the sensing element or, more in general, the measuring equipment that provides field data to the system. It is crystal clear that if such a component fails in providing data, the whole system may fail.

On the other hand, it is also known that a measuring equipment cannot provide the true value of a measurand, that is the measured quantity, but only an approximation of this value, approximation that is quantified in terms of measurement uncertainty [4]. It is also known that a measuring equipment can operate, in an apparently safe way, outside the uncertainty range provided by the manufacturer or by a calibration [5]. When this happens, the whole system processes data that may differ from the true measurand value for more than expected on the basis of the measuring equipment specifications, thus causing the system to possibly operate incorrectly.

From the system's point of view, this should be treated as a possible failure, whose severity depends on how sensitive is the whole systems to input data outside the expected accuracy range. However, the traditional FME(C)A does not take into account, to the authors' knowledge, this kind of failures, limiting itself to consider the effect of a complete out-of-order situation for the measuring equipment. It is quite evident that neglecting this metrological aspect of the analysis may lead to situations that are potentially as critical as the situations related to missing data.

This paper is therefore aimed at exploring how out-of-calibration situations can be considered in FMECA, as well as out-of-order situations, and how they can be suitably considered in the different stages of the analysis.

The aim of this paper is hence to discuss how the fundamental concepts of metrology can be suitably and properly encompassed in the traditional FMECA analysis to keep into account also the malfunctions that may be originated by measurement equipment working outside their state of metrological confirmation [6].

The paper is organized as follows: Section II covers the basis of the FMECA anlysis that are generally not familiar to the metrology experts; Section III provides some novel guidance on how to detect sensing elements that are out of calibration, and, finally, Section IV provides a numerical example.

II. THE STEPS

A well-assessed concept, in FME(C)A, as well in RAM (Reliability, Availability, Maintainability) analysis, states that all processes involved in the analysis must follow the design stages quite closely, so that all choices can be properly addressed, from those related to system architecture, to the employed technology, the test procedures and logistics [2], [3], [7], [8].

Several variations of this analysis can be found, according to the design and implementation stage they are applied: the Design FMEA (DFMEA) and the Process FMEA (PFMEA) are the most known and used. It is also worth mentioning the Failure Recording and Corrective Action System (FRACAS) [9], developed by the US Navy, that, starting from the analysis of the fault history, provides a method to identify and implement suitable corrective actions.

A. DFMEA and PFMEA: two similar, but different methods

Several documents [10] and Standards [11], [12] have covered the FMEA process and its declination into the DFMEA and PFMEA and have represented milestones in implementing a Quality Management System (QMS) meeting the ISO 9001 [13] requirements, since they clarify how to perform a correct risk analysis.

Two factors contribute to risk: the consequences of the event, and the probability that the event occurs. Therefore, to reduce risk, consequences must be mitigated and the occurrence rate reduced, according to ISO 9001 that recommends to monitor the following risk sources:

- incomplete or wrong definition of the design input elements;
- definition of design output elements that do not meet specifications;
- production that does not meet design specifications.

DFMEA and PFMEA meet these requirements, since they are aimed at analyzing the possible failure modes starting from the design stage, investigating on the failure causes and consequences. This investigation requires also to analyze the possible ways the different parts of the design interface with each other [14].

A critical issue with this analysis and the way it is implemented when the analyzed system uses measurement results coming from measuring equipment that are part of the system is that the traditional DFMEA and PFMEA analysis consider the measuring equipment - sensors, instruments ... - as if they were just components with only two possible ways to operate: normal and faulty.

The problem, when measurements are concerned, is that the employed measuring equipment may look perfectly working, although it is providing non-pertinent information because it started working outside the metrological specifications.

The correct definition of the metrological specifications that must be met to ensure that the whole system may work inside its own specifications is, hence, of critical importance. The keywords, in this case, are target uncertainty, of course, but also, according to the performance required to the whole system, repeatability, maximum admissible drift, ...

Once the expected metrological performance has been correctly defined and specified, any operating condition outside the assigned metrological performance should be considered as a possible failure mode.

This is not a trivial operation. Indeed, it is well-known that any operating mode outside the metrological specification can be detected by calibrating the instrument. On the other hand, it is quite obvious that the measuring equipment may have started working outside specification well before calibration and that calibration cannot tell us when misoperations have started.

A method is then required to detect such situation (which is actually a failure) as soon as it occurs. DFMEA and PFMEA are the key elements to this, because they shall consider the effects of apparently correct measurement results, that are actually delivered outside the metrological specifications. This may occur, for instance, when the actual measurement uncertainty exceeds the target uncertainty.

If the criticality of this kind of failures is also considered and evaluated, under a strict metrological perspective, for instance by considering how uncertainty propagates to the final result and how it may change the risk of wrong decisions or incorrect operations, it is also possible to identify the most effective, also from the economical point of view, actions to deactivate potentially critical situations.

TABLE I ELEMENTS TO CONSIDER IN THE DFMEA

	Design require-ments	Failure modes	Effects	Severity	Main causes	Preliminary checks (design stage)	Occurrence	Detectability	RPN (Risk Priority Num- ber)
Metrological require-ments									

TABLE II ELEMENTS TO CONSIDER IN THE PFMEA

	Object / Func-tionality	Failure modes	Effects	Severity	Potential causes	Occurrence	Process control	Detectability	RPN (Risk Priority Num- ber)
Metrological require-ments									

Since the DFMEA considers the design requirements to obtain the specified performance, it appears to be the best stage of the analysis where to consider also the metrological performance. Table I represents a sort of checklist of the elements to consider in the DFMEA.

It is advisable to add a line, in this table, dedicated to the above mentioned measurement requirements, as shown in Table I, so that the related design requirements can be taken into account as well as the possible failure modes, their potential effects and their estimated criticality. The presence of a measurement expert in the team that performs the DFMEA would be highly advisable.

On the other hand, the PFMEA is aimed at considering the failure modes that might be originated during the production stage, assuming that the design is fully compliant with the required specifications.

In other words, the PFMEA is specifically related to monitoring the production process and identifying the failure modes in this process that may affect the performance of the final product. Here too the impact of the performance of the measuring equipment used to monitor the production process is quite significant and a degraded metrological performance should be seen as a failure.

Similarly to the DFMEA, Table II represents a sort of checklist of the elements to be considered in the PFMEA. Also in this table, it is advisable to add a line dedicated to the above mentioned measurement requirements, as shown in Table II, so that the related requirements can be taken in account as well as the possible failure modes, their potential effects and their estimated criticality.

It can be concluded that DFMEA and PFMEA act as complementary analysis also from the metrological point of view, since the DFMEA aims at identifying and correcting design weaknesses that may cause failures, while the PFMEA aims at identifying and correcting weaknesses in logistics and production processes that may affect the final product quality. The main differences in the object and context of the two analysis are highlighted in Table III, while the synergistic interaction between them is graphically shown in Fig. 1.

Table III OBJECTIVES AND CONTEXT OF DFMEA AND PFMEA

	Objective	**Context**
DFMEA	product elements	- Interactions between elements - Interactions with external entities - ...
PFMEA	- Operation modes - Process stages - ...	- Interactions between elements - Interactions between stages - Interactions between systems

B. Exploiting synergy

According to the IEC 60812 Standard [1], the following 11 steps must be accomplished to perform an FME(C)A.

- Step 1 – System definition
- Step 2 – Block-diagram processing
- Step 3 – Definition of the base principles

- Step 4 – Failure mode definition Step
- Step 5 – Failure cause identification
- Step 6 – Failure effect identification
- Step 7 – Definition of methods and actions to identify and isolate failures
- Step 8 – Prevention of undesired events
- Step 9 – Classification of severity on the final effects
- Step 10 – Multiple failures
- Step 11 – Recommendations

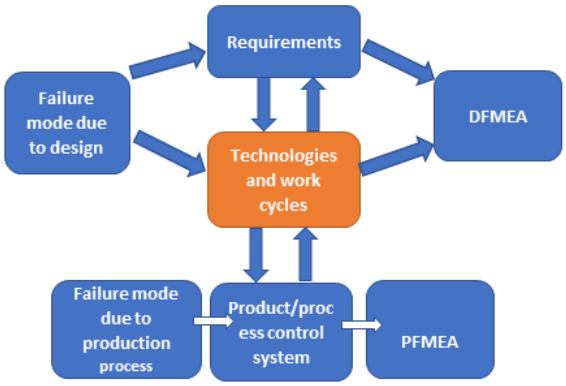

Fig. 1 . Interactions between DFMEA and PFMEA

The synergistic inclusion of the metrological concepts con- sidered in the previous sections can be located in Steps 6 and 9 of the above list, when the failure mode effects on the final result and their severity shall be considered.

As already mentioned, the traditional FMEA, at the DFMEA stage, tends to consider that a measuring equipment operates correctly if it has been calibrated. However, calibration is a necessary, but not sufficient condition to ensure the correct metrological performance, since this depends also – and sometimes mainly – on the actual operating conditions and the possible degradation that the same equipment may have suffered in time.

An example of the effects, on the measured value, of the possible degradation suffered by the measuring equipment is shown in Fig. 2. Let us suppose that the measured value M, represented by the probability distribution of the possible values that can be attributed to the measured quantity, according to the evaluated measurement uncertainty, has to be compared with a threshold value T, also represented by a probability distribution. The normal situation is the one depicted by the distributions in the left side of the figure, where the measured value is 100% below the threshold.

However, due to a drift over time of the measuring equipment, the measured value shifts in time towards the threshold value, until it reaches the rightmost situation in Fig. 3. In this situation, a probability exists, quantified by the red surface, that the measured value is considered above the threshold and a wrong decision is taken by the considered system.

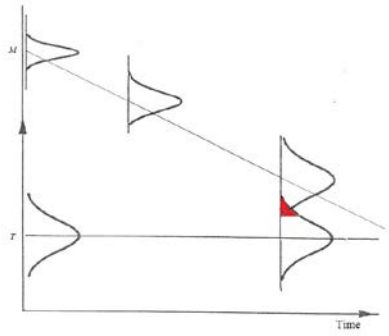

Fig. 2 Possible effect of a metrological degradation when the measured value has to be compared with a threshold value.

III. THE DETECTABILITY PROBLEM

Considering the problem of the possible deviations from metrological specifications in the FME(C)A allows one to consider them as possible failures, and analyze their effects on the final product or system. Therefore, also their criticality can be correctly estimated.

Nevertheless, this leaves a problem open: how can such a deviation be detected? The most immediate way is that of adding redundancy, which means, in the most critical situations, to implement also a voting system, such as a n − 1 over n system.

The main drawback of such a strategy is the cost, especially when an expensive measuring equipment needs redundancy. Hardware redundancy, however, is not always strictly required, if:

1) other sensors are available to measure different quanti- ties, and

2) a model is also available that relates these other quantities to the quantity measured by the measuring equip- ment that should be duplicated.

This strategy can usefully provide a so-called *pseudo-measurement or virtual measurement*, that is a value that is not directly measured, but is inferred from other sets of information available in the process to which the measuring equipment is dedicated. The uncertainty value associated with the pseudo-measurement will likely be larger than the uncertainty value associated with the measurement result provided by the dedicated measuring equipment. However, if suitably defined at the design stage and correctly considered when comparing the pseudo-measurement with the other values provided by the voting system – coming from other pseudo-sensors or actual sensors – uncertainty helps in detecting whether the actual sensor is operating inside its metrological specifications or not. Indeed, if the result provided by the actual sensor and the one provided by the

pseudo-sensor are metrologically compatible, according to their respective uncertainty values, the sensor can be considered as healthy. In the other case, it will be tagged as faulty.

The most interesting outcome of this approach is that the system may become fault-tolerant also with respect to failures caused by a measuring equipment working outside its metrological specification by exploiting the whole available information, thus limiting the extra cost of full hardware redundancy.

IV. Examples

A. The B737MAX example

The recent accidents occurred to two Boeing B737 MAX aircraft, one of the Indonesian Lion Airlines and one of the Ethiopian Airline, cane be seen as a clear case in which the metrological performance of a sensor – the angle-of-attack sensor – has not been properly taken into account during the DFMEA.

The final report for the Lion Airlines is already available [15] and has not left doubts on the cause of the accident. While the final report for the Ethiopian Airline is not yet available, there is little doubt that the cause of the accident was the same. The origin of the problem is the tendency of the new B737 MAX to nose up at low speed and high thrust, due the different position and size of the engines with respect to the previous versions of this same aircraft. The FMECA analysis showed this as a highly critical element, since it may cause the aircraft to stall in critical phases of the flight (take-off and initial climb). Therefore, the Maneuvering Characteristic Augmentation System (MCAS), already present in the previous versions, was considered a critical element and was duplicated. The original, single MCAS, processed the angle-of-attack values coming from both sensors installed on both sides of the aircraft, and could check whether their readings were in agreement or not. After duplication, each new MCAS system is now processing the angle-of-attack reading coming from only one sensor, the one on the same side as that of the pilot flying. Therefore, there is no more redundancy on this element, that proved to have become the most critical element in the system, since incorrect readings led two aircraft to crash.

Could this be avoided, without adding two more angle-of-attack sensors, one on each side of the aircraft, so that each MCAS could process two independent measured values? It is known that the information provided by the angle-of-attack sensor can be retrieved also by processing the airspeed and the aircraft attitude, provided by the artificial horizon. Therefore, it was possible, adding some processing capability to the MCAS, to implement a pseudo sensor to measure the angle of attack, and compare its output with that of the real sensor. A DFMEA performed considering also the metrological specification of the sensor, the severity of operations outside these specifications (as those occurred to the two unfortunate B737 MAX), and the detectability by means of a pseudo sensor would have, probably, avoid two mournful disasters.

B. IGBT Heat-Sink temperature monitoring

Another example, still under development, is related to monitoring the temperature of the heat sink of an IGBT employed in the control board of an inverter dedicated to the connection of photo-voltaic (PV) panels to the AC grid. This temperature needs to be monitored since variations in its values or values exceeding the normal operating conditions may cause damages in the inverter control.

However, the economical value of the whole device leaves little margin to add expensive hardware redundancy. A pos- sible model that relates the heat sink temperature to other parameters of the board that are already monitored has been investigated and is schematically shown in Table IV.

The monitored parameters are the CPU temperature, the DC cabinet output temperature, the output power Pu, the output current Iu and the DC voltage Vdc. A non-linear relationship linking these quantities to the heat-sink parameters is shown in the bottom row of Table IV. The βi weights assigned to each quantity inside this relationship are reported in the top line of the same table. The result provided by the relationship shown in the bottom row of Table IV implements a pseudo sensor for the IGBT heat-sink temperature.

Fig. 3 shows a comparison between the temperature measured by a real temperature sensor (red line) and the temperature returned by the pseudo sensor shown in Table IV. Although these are preliminary results, the agreement between the two values over time is quite good, and shows that the implemented pseudo-sensor can be efficiently employed as a redundancy for the temperature sensor.

V. Summary

This paper has shown how the FME(C)A process can be usefully and fruitfully completed by a thorough metrological analysis of all measuring devices that are part of a product or system. It has been shown that failures, in a measuring equipment, are not of on/off kind, and the most critical ones are, probably, those involving apparently correct oper- ating conditions that are, actually, outside the metrological specifications: in other words, the reliability of the provided measurement results is not the expected one.

The most suitable steps of the FMEA, and specifically the DFMEA, have been identified to implement the metrological analysis and identify the best corrective actions to detect possible failures and mitigate their effects.

Redundancy has been considered as the most effective way to reduce the risk of incorrectly operating measuring devices, and it was shown how the whole available information can be exploited to avoid expensive hardware redundancy by implementing pseudo-measurements.

The recent dramatic accidents involving two Boeing B737 MAX aircrafts have been considered as a good example of the problems that can be caused by not considering the criticality of a sensor when it drifts out of the specified metrological performance.

An example has been also proposed on how to implement a good and efficient redundancy, through a pseudo-sensor, to sensors monitoring the temperature of an IGBT heat sink. The preliminary experimental tests show that the value measured by the sensor and estimated by the pseudo-sensor are in good agreement.

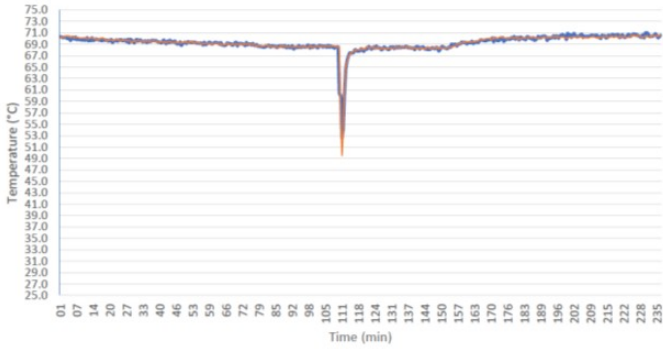

Fig. 3 IGBT heat-sink temperature. Red line: measured temperature. Blue line: temperature estimated by the pseudo sensor.

REFERENCES

[1] IEC60812-2018, Failure modes and effects analysis (FMEA and FMECA), IEC 60812, 2018.

[2] M. Catelani, L. Cristaldi, M. Lazzaroni, L. Peretto, and P. Rinaldi, *Reliability Engineering: Basic Concepts and Applications in ICT*. New York, NY, USA: Springer, 2011.

[3] M. Rausand and A. Hoyland, *System Reliability Theory: Models, Statis- tical Methods, and Applications*, 2nd ed., ser. Wiley Series in Probability and Statistics. Hoboken, NJ, USA: J. Wiley & Sons, 2004

[4] A. Ferrero and D. Petri, Modern Measurements: Fundamentals and Applications. Hoboken, NJ, USA: J. Wiley & Sons, 2015, ch. Measurement models and uncertainty, pp. 3 – 46.

[5] A. Ferrero, "The pillars of metrology," IEEE Instrumentation Measure- ment Magazine, vol. 18, no. 6, pp. 7–11, December 2015.

[6] Measurement management systems – Requirements for measurement processes and measuring equipment, ISO EN 10012, 2013.

[7] R. M. Herman and K. M. Janasak, "Using fmeca to design sustainable products," in 2011 Proceedings - Annual Reliability and Maintainability Symposium, Jan 2011, pp. 1–6.

[8] K. Bowman, D. Huffman, and J. Akers, "Emerging trends in risk assessment and evaluation," in 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), Jan 2013, pp. 1–4.

[9] Z. Li and M. Mobin, "A dfmea-based reliability prediction approach in early product design," in 2018 Annual Reliability and Maintainability Symposium (RAMS), Jan 2018, pp. 1–7.

[10] AIAG, Potential Failure Mode & Effects Analysis (FMEA-4), Automo- tive Industry Action Group - AIAG, 2008.

[11] MIL-STD-1629a, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, US Department of Defense, 1980.

[12] SAE-J1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA), SAE, 2002.

[13] ISO 9001, Quality management systems. Requirements, ISO, 2015.

[14] B. Haughey, "Product and process risk analysis and the impact on product safety, quality, and reliability," in 2019 Annual Reliability and Maintainability Symposium (RAMS), Jan 2019, pp. 1–5.

[15] Komite Nasional Keselematan Transportasi – Republic of Indone- sia, Aircraft Accident Investigation Report. PT.Lion Mentari Airlines, KNKT.18.10.35.04, 2019.4.

TABLE IV
NON-LINEAR REGRESSION MODEL TO USE AS HEAT-SINK TEMPERATURE SENSOR REDUNDANCY

β_1 $-2.20 \cdot 10^{3}$	β_2 $2.35 \cdot 10^{-1}$	β_3 $8.34 \cdot 10^{-1}$	β_4 $5.95 \cdot 10^{-2}$	β_5 $2.10 \cdot 10^{-4}$	β_6 -1.84
Input	X_1	X_2	X_3	X_4	X_5
	CPU temperature [°C]	DC cabinet output temperature [°C]	P_u [kW]	I_u [A]	V_{dc} [V]
$HS_{pm} = \beta_1 + \beta_2 \cdot X_1 + \beta_3 \cdot X_3 + \beta_4 \cdot X_3 + \beta_5 \cdot X_4^2 + \beta_5 \cdot X_5$					