20th IMEKO TC4 International Symposium and
18th International Workshop on ADC Modelling and Testing
Research on Electric and Electronic Measurement for the Economic Upturn
Benevento, Italy, September 15-17, 2014

Risk Analysis in Aviation: the Forensic Point of View

Ettore De Francesco[1], Ruggero De Francesco[1], Fabio Leccese[2], Marco Cagnetti[2]

[1] SeTeL s.r.l, via Casamari n.6, 00142, Roma, Italy, ettore.defrancesco@setelgroup.it, r.defrancesco@setelgroup.it
[2] Department of Science, Università degli Studi "Roma Tre", viale Marconi n.446, 00146 Rome, Italy, fabio.leccese@uniroma3.it, ing.marco.cagnetti@gmail.com

***Abstract* – An alternative process for the evaluation of the economic risk bound to the insurance of an aircraft is presented. Such process is built from two potentially complementary methodologies, used for risk and fault analyses (ERC and FMECA), combined with a cooperative agreement between flight and insurance companies, that meets the recent tendencies on aviation Safety Management Systems. This innovative procedure should allow the periodic update of the economic risk bound to the insurance while lowering the general costs for risk evaluation thus resulting in a lower insurance premium and increased competitiveness.**

Keywords—Risk Analysis; Avionic Insurance; FMECA; ERC; SMS; S3000L.

I. INTRODUCTION

It is possible to define Risk as a state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome [1,2].

Its quantification is essential in the insurance field because it allows to determine the insurance premium which, in the avionic sector, is determined by two factors:

- the risk of incurring reparation costs due to damages to persons and equipment,
- the costs that the insurance company must sustain in order to manage the insurance process and in particular the risk evaluation and update process (involving the acquisition of the costly historical data necessary for the evaluation).

The evaluation or estimation of the risk is composed by the combination of two elements: the severity of the event and the probability that the event happens.

The severity is an estimation of the damages that can derive from the effects of the event. Generally, in the aeronautical sector, severity is assessed through four classes that defines the level of damages brought by the event. Such categories are catastrophic, major, minor and negligible.

Probability can be managed in two different ways: it can be estimated by historical series data or, in absence of required data, it may be estimated using probability classes.

This risk estimation may be achieved through different approaches of which two well-known methodologies are the Failure Mode Effects and Criticality Analysis (FMECA) [3,4] and the Event Risk Classification (ERC) [5,6]. These two methods, following different strategies, may become a complementary approach that is not bound to the direct acquisition of aircraft historical data.

In this article, after a brief but complete description of these methodologies, the authors will show how their proactive use and integration inside the safety management and occurrence reporting systems of a flight company allows improving the risk analysis process. The approach should both improve the efficiency of the process and reduce the involved costs, for both the insurance companies and the flight companies in the form of a smaller insurance premium.

II. FMECA

Failure Mode, Effects and Criticality Analysis (FMECA) is a bottom-up, inductive analytical method applicable both to complex systems and to functional/operative procedures. This analysis is used to chart all the failure modes that may affect the system and to assess the probability of such failures against the severity of their consequences therefore defining the criticality of each charted failure. In the case of procedures, FMECA considers the effects of a failure on the subsequent functional blocks level while in the case of complex systems, it considers the effects of individual component failures. This last requires far more effort, but it is sometimes preferred because it relies more on quantitative data. The FMECA of complex systems is the one that interests us for the purposes of this article so the following paragraphs will focus on this aspect of the FMECA process.

FMECA analysis typically consists of the following logical steps:

ISBN-14: 978-92-990073-2-7

1. System definition

The completely complex system is fully defined and subdivided into a hierarchical structure that is made of a combination of subsystems, units or piece parts. Since the FMECA approach aims to guarantee the mission defined for the system, a functional descriptions that cover all operational modes and mission phases is provided in this step.

2. Ground rules and assumptions (optional)

Rules and assumptions are defined and agreed. This might include, for example: standardized mission profile with specific own associated time; sources for failure rate and failure mode data; identification of which faults the built-in test will be able to identify; definition of criteria (mission abort, safety, maintenance, etc.); procedures and systems for uniquely identifying parts or functions; severity category definitions. The definition of such elements allows for a more detailed implementation of the FMECA approach.

3. Block diagrams

A structure, normally a tree that links systems and subsystems, and even parts, viewed as functional blocks is built in order to highlight the information/failure flow between the different levels of the system hierarchy. This structure usually named RBD (Reliability Block Diagram) helps to identify critical paths and interfaces, and allows tracing the higher-level effects deriving from lower level failures.

4. Failure mode identification

Next, a complete list of failure modes is developed for each piece part or function covered by the analysis, therefore defining the list of all the failures that may affect the system.

FMECA's which analyzes a complex systems (like an airplane) usually build the list of failures modes through the use of failure historical data of the single parts/elements which compose the system or, in the absence of enough data, through the estimate of system engineers.

In both cases, the output of this phase is a first matrix that lists for each row the failures modes that may affect the system and the initial elements that are responsible for the failure.

5. Failure effects analysis

In this step, for each row of the FMECA matrix, failure effects are determined. Effects are described before for local, then for higher and end (system) levels. These effects may include: system failure, degraded operation, system status failure, no immediate effects.

The analysts, through engineering based judgment, estimate all failure effect categories, used at various hierarchical levels.

6. Severity classification

For each failure mode of each unique item, a severity classification is assigned based upon system level consequences. This information are therefore filled on the FMECA matrix. Severity levels may have from 3 to 10 steps, however in the avionic sector 4 levels are usually implemented: catastrophic, major, minor and negligible.

7. Probability Classification

The probability of the occurrence of each failure mode is determined. Such probability may be calculated using failure historical data of the failed item or using probability classes (usually bound to a certain code/level) and experts estimates (which compromises an higher uncertainty on the results).

8. Criticality ranking

Failure mode analysis could be qualitative or quantitative. The first case is applied when probability is estimated through classes. Using severity code as one axis and probability level code as the other, the failure mode may then be charted on a criticality matrix.

For quantitative assessment, for each failure mode of each item it is necessary to calculate C_m *(modal criticality number)*, and, for each item, C_r (*item criticality number)*. These numbers are computed as $C_m=\lambda_p\ \alpha\ \beta\ t$ and $C_r = \sum_{n=1}^{N}(C_m)_n$ considering the following values: basic failure rate λp, failure mode ratio α, conditional probability β, mission phase duration t and where λ_p derived from a failure rate prediction based on defined model, α is provided by a database source. Obviously, to correctly assign failure mode ratio for functional level FMECA, it is necessary an engineering judgment. β represents the conditional probability that the failure effect will result in the identified severity classification, given that the failure mode occurs. It represents the analyst's best judgment as to the likelihood that the loss will occur. Using either C_m or C_r on one axis and severity code on the other, a criticality matrix may be charted for graphical analysis.

9. Critical item/failure mode list

Once the criticality assessment is completed for each failure mode of each item, severity and qualitative probability level or quantitative criticality number may sort the FMECA matrix. This enables the analysis to identify critical items and critical failure modes for which design mitigation is desired.

10. Failure detection methods

The ability of the system to detect and report the failure in question is analyzed for each component and failure mode. Each row of the report (which defines a failure mode) will therefore contain information explaining if the failure is detectable and through which method can the

failure be detected (system diagnostic, operator inspection, sensorial signals, etc...).

11. Recommendations

The natural output of FMECA are recommendations that are made in this step to design to reduce the consequences of critical failures. The most common are the selection of higher reliability components, the reduction of the stress level at which a critical item operates and the adding of redundancy or monitoring to the system. Furthermore, it must be taken into consideration that Maintainability Analysis and Logistics Support Analysis of the system will require data from the FMECA.

12. FMECA report

At the end, the FMECA gives a report consisting of system description, base rules and assumptions, conclusions and recommendations, corrective actions to be tracked, and the attached FMECA matrix. The FMECA matrix lists all the information related to: the failure modes, their causes, their effects on the system, their detectability and the possible corrective actions.

The real strengths of FMECA include are surely: comprehensiveness, systematic establishment of relationships between failure causes and effects (which in our case will lead to reparation costs), its ability to point out individual failure modes for corrective action in design.

Unluckily this is paid as extensive labor required, large number of trivial cases considered and therefore implies great efforts and high costs.

III. ERC

The ERC is an approach applied to in field safety reports that aims to estimate the possible outcomes of the reported event. Therefore, its main objective is to act as the first screening of all incoming safety data and to identify when urgent action is necessary. The event risk classification should take place preferably within one or two days of the event and be carried out by a person with operational experience who has been trained in risk assessment, hereafter called the Safety Analyst.

The ERC approach is based on two questions:

- If this event had escalated into an accident, what would have been the most credible accident outcome?
- What was the effectiveness of the remaining barriers between this event and the most credible accident outcome?

The first question is looking to identify the accident outcome **that is of most concern** when this type of incident occurs, or put another way 'what is the accident I am trying to avoid by having these incidents reported?' This question is not asking for the most probable outcome, as that is usually "nothing" and therefore ignores any risks that the event carries, but neither is it necessarily looking for the worst possible outcome, as the worst-case scenario would often not be the most obvious accident to expect.

There is likely to be some subjectivity between users in the answer to the first question depending upon how they consider the factors causing the event.

However that variation is dealt with in question two through consideration of the remaining barriers, and hence the probability of that accident outcome. The risk colors and values in the ERC are intended to ensure that any variation in approach produces similar outputs in terms of risk.

In the longer term, it is likely that organizations will identify the outcomes associated with types of events and hence remove the subjectivity associated with the first question for most incidents.

The second question only considers *remaining* barriers to estimate the probability of further escalation into the most credible accident outcome. The barrier, which stopped the escalation, will be counted in along with any others that are believed to remain. The already failed barriers will be ignored. In order to achieve such results however expert knowledge will still be required to make an accurate categorization.

Usually the reference in this analysis has to be an accident (event that resulted in major damage to the airplane or loss of life), meaning that the risk bound to every incident or generic safety report must be estimated in the optic of its possible **accident outcomes.**

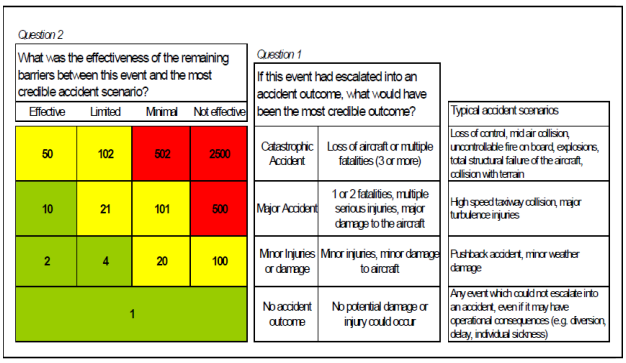

Fig. 1 Relationships between ASD SX000 standards.

The ERC has two outputs. **The first output** is a recommendation on what should be done about the event:

- Investigate immediately and take action.
- Investigate or carry out further Risk Assessment.
- Use for continuous improvement (flows into the

Database).

The second output of the ERC is a number, called the ERC risk index. This index gives a quantitative relative risk value and it is very useful in compiling statistics. During the evaluation of the event, often there are more possible scenarios that describe the accidents outcomes. A correct ERC process should evaluate each scenario and pick the one that gives the highest risk index.

IV. DISCUSSION

As explained in the previous paragraph, the ERC is considerable as a methodology that promptly gives early warnings on the system status. It is activated by experts in the field that notify that something in the aircraft may be break or may not properly function. From this point starts an analysis of what might happen. ERC is a cheap and quickly applicable methodology that however does not allow estimating the risk of incurring costs due to reparations.

On the other hand, the FMECA is an expensive process principally conceived for the design phase. The FMECA process can be applied in a way that allows estimating the "economic risks" bound to an aircraft insurance. The process can be applied also in recursive way but, depending on the circumstances, this would require the application of complex procedures related to the gathering and validation of in field maintenance data which must be compared with the system FMECA data. Such process allows to accurately estimating the "safety of the system" but implies the management of large quantity of data and implies high efforts and costs.

The idea is therefore to combine the two processes in order to achieve a continuous update of the risk analysis bound to the aircraft insurance while maintaining contained costs for such processes.

The combined process uses the FMECA analysis obtained from the design phase of the aircraft as a starting point; this data can be used to estimate the initial "economic risks" bound to the aircraft insurance performing a sort of "**Economic FMECA**" analysis. This FMECA design data usually needs to be acquired from the design organization responsible for the aircraft. However, design FMECA data acquisition can be costly, this has to be done only once for each aircraft type and therefore the general costs are scattered on all the insured aircraft of the same type and for all the lifespan of each aircraft. This leads to an extremely low effective cost on the insurance premium.

From this point, the FMECA data of the aircraft, which allows the "economic risk" estimate, must be periodically updated in order to update the insurance premium.

However, such update would involve high costs for the insurance company since processes as the continuous update of FMECA data are not performed inside the civil aeronautical sector. This is due to various reasons such as high costs for the management of high quantities of data and the need to involve design organizations in the process.

To avoid such outcome, a "filtering process" is applied which is represented by the use of the ERC analysis. The ERC analysis allows to obtain two main contributes: the first is the identification of the events that have the greater urgency to be investigated (therefore the ones having the higher risks) and the second consists in the fact that a first estimate of the level of risk associated to these events is provided.

The responsibility of this step in the process belongs to the CAMO (Continuous Airworthiness Management Organization) of the flying company which operates the insured aircraft. The CAMO have therefore the task to use the safety reports deriving from occurrence reporting to perform an ERC analysis which results must be made available to the insuring company.

It is important to take notice that performing an ERC does not involve high costs for flight companies and furthermore ERC is becoming a requisite of the SMS (Safety Management System) which is mandatory for such companies.

At this point, the data deriving from the ERC and made available by the insuring company are used to aim the updating iteration of the "Economic FMECA" which, starting from the more critical events and by using the ERC estimated risk levels, allows to estimate the new "economic risks" bound to the aircraft insurance.

Fig. 2 shows the idea of the Block scheme of the Continuous Insurance Risks evaluation process.

The application of the ERC process allows aiming the execution of the FMECA on a reduced list of critical items or functions allowing the reduction of the quantity of data managed, of the involved costs and generally simplifying the whole process. However, in order to achieve such a process, two things must be taken into consideration. The first is the necessity to perform an "economic FMECA" which may be considered an alteration of the common FMECA, which is not focused on predicting the system failure modes, but the costs derived from such failures. The second is the necessity to stipulate a common agreement (by contract) between the insurance company and the flight company in order to guarantee the access to ERC data in return for a decrease

in the insurance premium (which is covered by lower costs in risk evaluation).

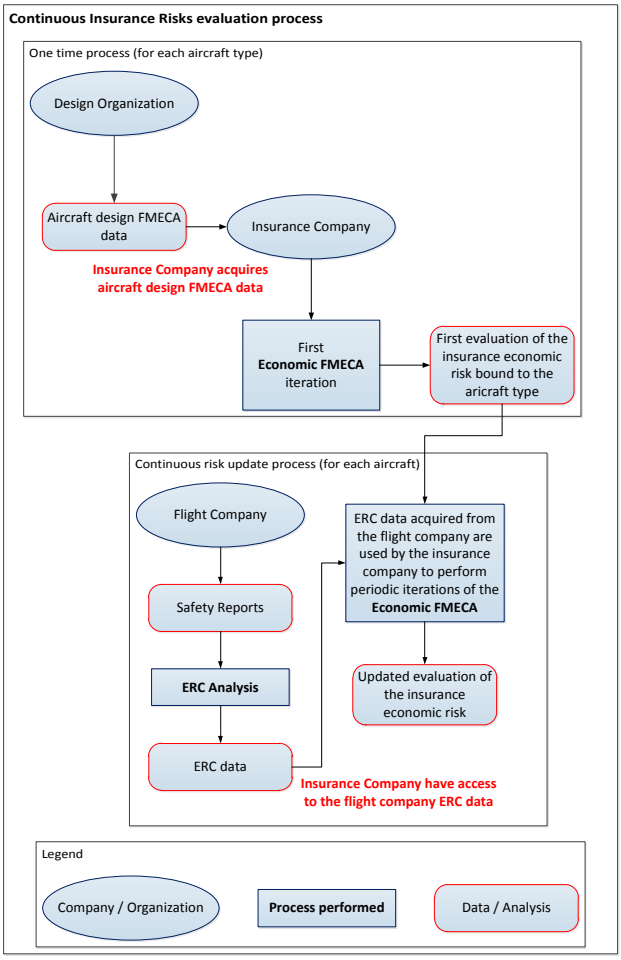

Fig. 2 Block scheme of the idea of the Continuous Insurance Risks evaluation process.

V. A SIMPLE MATHEMATICAL MODEL

What is now presented is a hypothesis for a possible variation of the FMECA process that leads to an estimate of the cost incurred in insuring a system, which can then be used as a basis to define the insurance premium. This model follows the standard FMECA process up to the definition of the system components C_m, at which point it adds another step, the economic cost estimate. Since each failure mode is linked to an end effect, the incurred cost in case of that failure mode occurrence is easily identifiable. This will be referred as the expected failure mode cost (E_m). Each C_m is now multiplied by the expected incurred cost for that failure mode to obtain the failure mode average cost (A_m):

$$A_m = C_m \cdot E_m$$

This number represents the fact that the presence of that failure mode on a component of the insured system has raised the expected cost of the whole system of A_m for the insuring company. Since the FMECA analysis is already weighted in terms of failure mode probabilities and item failure rates, and since the item failure rates considered are already comprehensive of the items multiplicity, by converting the leafs of this tree like analysis approach that is the FMECA into a cost voice it is possible to obtain the final cost of the system by simply summing all the voice costs of those leafs.

$$Total\ system\ cost = \sum_{i=1}^{M} \sum_{n_i=1}^{N_i} (A_m)_{n_i}$$

As shown, the FMECA analysis is a great starting point to quantify the cost in which an insuring company will incur for that system. The process requires only doing some estimations of the economic damage for the different failure modes, while providing a result that is possibly more accurate than the historical data.

The greatest selling point of this method though is related to the possibility of rapidly estimating a premium insurance for newly designed systems, for which there is no historical data. Naturally, like all models of this kind it needs corrective actions during its employment, to correct the possible erroneous assumptions that were made in the first estimation. This is where this model becomes too cumbersome to be effectively used and where the ERC analysis intervenes as a solution.

Periodically updating a FMECA analysis with all the data incoming from the field is a daunting task, which also means costly. Since the insurance premium is based not solely on the expected costs deriving from the insured system, but also takes in consideration a cost derived from the administrative costs related to keeping up the insurance service, this cost derived from updating the FMECA would negatively impact on the premium.

By filtering, the updating process only to the items highlighted by the ERC process this cost can be considerably lowered and the model can be effectively used as a mean to evaluate the premium. This can be done since the items highlighted by the ERC process are the same ones that cause the major costs contributions to the system.

This shows that by sharing the FMECA and ERC analysis between the air company and the insurance company can lead to a more accurate and continuous esteem of the premium and do so at low costs.

VI. CONCLUSION AND PERSPECTIVES

The process proposed in this article shows that the combination of the ERC and of a cost oriented FMECA with the cooperation between flying and insurance companies holds the opportunity to both:

- continuously maintain the alignment between the insurance premium and the real risks involved by the aircraft insurance;
- decrease the component of the insurance premium determined by risk evaluation.

In this process, the reduction of the costs, shouldered by the insurance company, is determined by many factors such as: smart data management, quick interactions (based on a predetermined process) between flying and insurance companies and the capability to estimate the risk value without the continuous acquisition of aircraft historical data.

For such reasons this process acquires the greatest efficiency when combined with standardized data management structures and databases which takes into considerations the possible interactions between different organizations.

This suggests that a good vector for enhancing the performance of the proposed process could be the new Aerospace and Defense S3000L standard [7] that represents the new frontier related to logistic database management.

ASD S3000L describes a standardized database structure that, among different advantages, allows smart FMECA data management and provides shared formats to exchange such data between different organizations. This potentially leads to quicker and more efficient interactions between different organizations resulting in lower cost for data exchange and data exchange error correction.

REFERENCES

[1] D.W. Hubbard: “How to Measure Anything: Finding the Value of "Intangibles" in Business,” John Wiley & Sons Inc; 2nd ed., 19 April 2010, ISBN-10: 0470539399, ISBN-13:978-0470539392.

[2] C. Starr, R. Rudman, C. Whipple: “Philosophical Basis for Risk Analysis,” Annual Review Energy, 1976, Electric Power Research Institute, Palo Alto, California 94303, Available at: http://www.annualreviews.org/doi/pdf/10.1146/annurev.eg.01.110176.003213.

[3] E. De Francesco, F. Leccese: "Risks analysis for already existent electric lifelines in case of seismic disaster," *Environment and Electrical Engineering (EEEIC), 2012 11th International Conference on*, vol., no., pp.830,834, 18-25 May 2012doi: 10.1109/EEEIC.2012.6221490

[4] FMECA definition, Available at: http://en.wikipedia.org/wiki/Failure_mode,_effects,_and_criticality_analysis#cite_ref-0.

[5] P.C. Cacciabue, V. Licata, A. DE COL, “Un approccio pratico alla valutazione del rischio per il Safety Management System in campo aeronautico: il caso studio delle perdite di separazione in volo,” 2012, Politecnico di Milano, Available at: http://www.kitesolutions.it/WPSITEOLD/wp-content/uploads/2012/12/2012_12_DeCol.pdf.

[6] ARMS, “The ARMS Methodology for Operational Risk Assessment in Aviation Organizations,” 2007-2010. Available at: http://www.skybrary.aero/bookshelf/books/1141.pdf.

[7] ASD S3000L "International procedure specification for Logistic Support Analysis LSA". Apr.1, 2010.