CRITICAL ANALYSIS OF RISK ASSESSMENT METHODS AND MODELS USED IN CIVIL AVIATION

Florin NECULA[1]

This paper presents the applicability of some reliability and risk assessment methods and models in aircraft engineering and operations. Such methods were identified, analysed in order to emphasize the advantages and disadvantages and applied to practical examples from aviation field. The work passes firsts through a series of concepts of reliability and probabilities which will later be used in the safety assessment models and reliability calculation. Further, a series of risk assessment methods which can be used in safety assessment of aircraft and aircraft operation are presented with their applicability to practical examples. The work ends with the author's conclusions related to the analysed methods.

Keywords: reliability, risk assessment, probability distribution, failure, safety assessment, aircraft safety.

1. Introduction

Air transport industry has an experience of about one hundred years and, as is shown by the statistics despite this not so long history is one of the safest ways of traveling. But even with this good safety record, the development of the technology and the society requires a higher level of safety. The scope of this paper is to analyse some generic methods and models used by aviation industry for safety assessment and to emphasise their applicability and limitations. The aim of this analysis is to provide a structured approach in description of the methods and how they can be applied in practice. The study coughs up the importance of the safety assessment in the day by day operation of the aircraft and its impact on the flight safety. The research structure is based on the industry literature review using approved sources such as regulations, accidents reports and engineering books. From the above mentioned materials can be noticed that at the same time with technology improvement, the methods used in safety assessment must be improved and extended to some others areas, like operations.

[1] PhD Student, University POLITEHNICA of Bucharest, Romania, e-mail: florin_necula2000@yahoo.com

2. Concept of probability and reliability theory

There are many situations when we have to understand how some situations can evolve or what possibilities we have for a system to change from a present status to future states. We use the probabilistic approach mainly because is impossible to predict future with certainty, because we don't know every single detail of the system we analyse and because we deal with imperfect systems. On the other hand, the more predictable we design a system, meaning more reliable in order to meet the design life goals, more costly it will be. Particularly, in aviation, in order to maintain the established design safety goals, the safety must be quantified. This offers us the confidence when we step on board of an aircraft that the event of a catastrophic failure is extremely improbable to occur during flight. Extremely improbable according to European Aviation Safety Agency (EASA) Certification Specifications for Large Aeroplanes (CS-25) means a probability smaller than 10^{-9} per flight hour [1]. In the remaining part of this section some well-known definitions of probability, joint probability and conditional probability will be briefly reminded since they will be used throughout the paper.
Probability by definition is *the extent to which an event is likely to occur, measured by the ratio of the favourable cases to the whole number of cases possible* [2].

$$P(A) = \frac{number\ of\ possible\ success\ cases\ in\ N\ trials}{N} \tag{1}$$

A probability space or event space represents the uncertainty regarding an experiment.

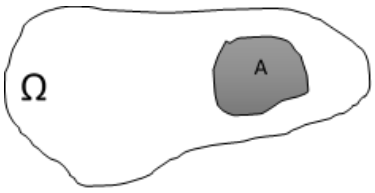

Fig. 1. Probability space

Ω = probability space
A = a subset included in Ω (A ⊂ Ω)

The probability of obtaining outcome A is denoted by P(A). The probability of event A not occurring (probability of the complement) is denoted by:

$$P(\bar{A}) = 1 - P(A) \tag{2}$$

For two independent events, the joint probability is equal to the product of the individual probabilities:

$$P(AB)=P(A\cap B)= P(A)\ P(B) \tag{3}$$

The conditional probability of event A to be obtained being given that event B occurred is denoted by $P(A \mid B)$.

In the case of two independent events, where P(A) and P(B) are unrelated to each other, the relation between the conditional probability of an event and complement probability of the other is:

$$P(A \mid B)= P(A \mid \bar{B})= P(A), \tag{4}$$

$$P(B \mid A)= P(B \mid \bar{A})= P(B)$$

The joint probability – P(AB) or $P(A\cap B)$ – for two dependent events is:

$$P(AB)=P(A\cap B)=P(A)\ P(B \mid A) = P(B)\ P(A \mid B) \tag{5}$$

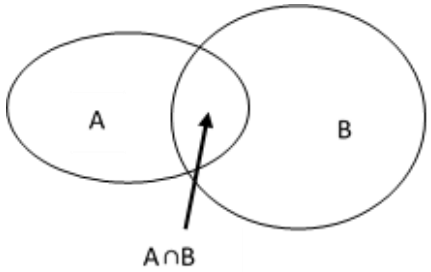

Fig. 2. Probability of dependent events

The probability of event A or B to occur is:

$$P(A + B)=P(A\ U\ B)=P(A) + P(B) – P(AB) \tag{6}$$

When A and B are two independent events, the above relation becomes:

$$P(A + B)=P(A\ U\ B)=P(A) + P(B) – P(A)P(B) \tag{7}$$

In case of two events A and B which cannot occur together (A and B are mutually exclusive) the following relations apply:

$$P(AB)=O \text{ and } P(A + B)=P(A) + P(B) \tag{8}$$

Reliability is the probability that an item will perform a required function without failure under stated conditions for a stated period of time [3]. Reliability is usually quantified in the probability of success of an item to perform its functions under specific operational and environmental conditions for a specified period of time. It is usually expressed as Mean Time Between Failures (MTBF).

$$MTBF = \frac{Total\ time}{Number\ of\ failures} \tag{9}$$

The relation between failure rate (λ) and MTBF is:

$$\lambda = \frac{1}{MTBF} \tag{10}$$

Aircraft designers and manufacturers use the reliability engineering in order to improve the maintenance tasks and intervals. Reliability data as failure rates, data resulting from analysis of failed components and data resulting from testing are used to support the prediction of maintenance intervals, the safety assessment process and finally to prove the safety goals of the aircraft.

Being given a constant failure rate (λ) of a component, the failure probability within a specified time interval (t) can be calculated using the formula [3]:

$$P = 1 - e^{-\lambda t} \tag{11}$$

The reliability of a series system is lower than the value of the most reliable component in that series. Because the reliability of the system (R_S) equals the product of the reliability of individual components, adding components to the system will decrease the system reliability.

$$R_S = R_1\ R_2\ R_3 \ldots \tag{12}$$

When parallel systems are considered, the higher the number of components, the higher the overall reliability of the system [3].

$$Rp = 1 - (1 - R_1)\ (1 - R_2)\ (1 - R_3) \ldots \tag{13}$$

In the above relation $(1 - R_i)$ is the failure probability of component "i". Because the components are in parallel, the system will fail when all the components will fail.

During reliability predictions and especially during safety assessment of aircraft systems different types of failure have to be considered. These failures include: single active, passive/ latent, multiple independent, common mode,

cascade and environmental. Reliability engineering in aviation is used both for designing process and for operation of the aircraft during its life cycle. The following are examples were reliability analysis supports the operation: maintenance and overhaul intervals, dispatchability (Minimum Equipment List), spare parts management, modification of the aircraft, safety data (e.g. Airworthiness Directives and Service Bulletins) and last but not least economical operation.

An example of reliability calculation and prediction method is Markov Analysis. Markov Analysis models systems which show strong dependencies between components failures [4].

A Markov model consists of a combination of possible states of a specific system. Considering any given system, Markov model consist of a series of possible states of that system, the transition paths between these states and the rate parameters for these transitions. For reliability analysis, the transitions represent failures and repairs. The following representation is usually used to depict the system states. Considering the system has two components, and each component has two states only, working or failed, then from the possible combination of the two components results four possible states of the system.

Table 1

Possible states for a two-component system

State	Component A	Component B
0	working	working
1	working	failed
2	failed	working
3	failed	failed

Considering one system consisting of one component with a failure rate λ_a, then the system can have the following states: working or failed. At the beginning, in state 0, when the system is working $P_0(0) = 1$. The probability of failure during the interval $\Delta t \; is \; \lambda_a \Delta t$. Then the probability of the system to move to state 1 (failed) during a time interval Δt is:

$$P_1(t + \Delta t) = P_1(t) + P_0(t)\lambda_a \Delta t \tag{14}$$

This equation can be interpreted that the system was already in state 1 at time t or the system was in state 0 and failed during time interval Δt. The above equation can be rearranged:

$$\frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} \approx P_0(t)\lambda_a \tag{15}$$

When Δt tends to 0, the equation can be re-written as follows:

$$\frac{dP_1(t)}{dt} = \lambda_a P_0(t) \tag{16}$$

It is also known that at time t, $P_0(t) + P_1(t) = 1$, this means:

$$\frac{dP_0(t)}{dt} = -\frac{dP_1(t)}{dt} \tag{17}$$

Substituting this in equation (16) is obtained: $\frac{dP_0(t)}{dt} = -\lambda_a P_0(t)$ and integrating both sides:

$$\int \frac{1}{P_0(t)} dP_0(t) = -\int \lambda_a dt \text{ resulting ln } P_0(t) = -\lambda_a t + C$$

But from the condition that the system is working in the initial state:

$P_0(0) = 1 => C = 0$ and in this case $P_0(t) = e^{-\lambda_a t}$ which is actually the reliability of the system at time t.

For example, being given the generator of an Auxiliary Power Unit (APU), working two hours during a turnaround and knowing that the failure probability is 0,09 per operating hour and the repair probability is 0,7 for the same interval of time, using the Markov analysis the probability of the generator to be functional after the two hours is:

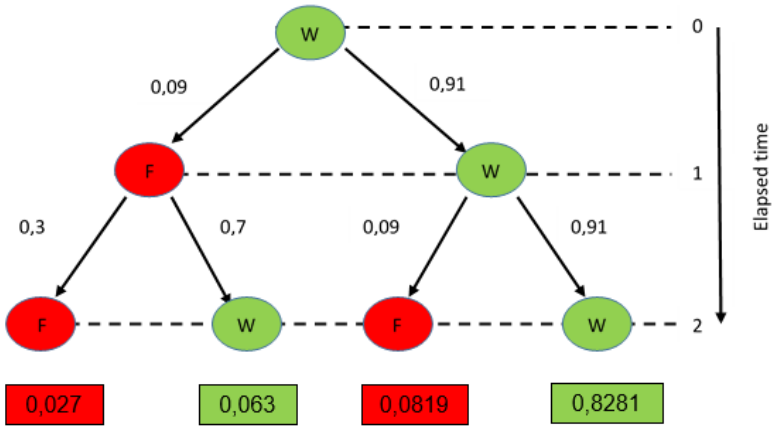

Fig. 4. Probability of the generator to be functional after two hours of operation using Markov representation

From the above graph one can notice that the probability of the generator to be working after two hours is P(W)= 0,063 + 0,8281 = 0,8911, while the probability of failure is P(F) = 0,027 + 0,0819 = 0,1089.

Proofing of the calculation can be done as follows:

$$P(W) + P(F) = 0,8911 + 0,1089 = 1$$

3. Risk assessment methods and models

Functional Hazard Assessment (FHA)

Aircraft involved in commercial air transport are complex systems and to assure an accepted level of safety, every aircraft, its systems and subsystems must be assessed from safety point of view. One of the ways this can be done is the FHA.

Hazard identification is not a new concept in aerospace industry, at early stages is was performed through use of hazard checklists and today is increasingly recommended by standard practices as a mean of performing hazard identification [5].

"Functional Hazard Assessment" is defined as one of the preliminary activities in the safety assessment process. FHA is first carried out for the whole aircraft, working from a description of aircraft functions. Then, following allocation of functions to aircraft systems, FHA is performed again for each subsystem [5].

When we consider aircraft systems we are looking at hazards involving possible failures like failure to operate, operating incorrectly, operating inadvertently, operating at wrong time (i.e. too early or too late), component is damaged by other components in its vicinity (e.g. hydraulic leak affecting a landing gear switch), component receives or send erroneous data, conflicting information (e.g. two different values sent by two different radio altimeters installed on aircraft) etc. A typical aircraft system hazard analysis comprises of identifying the system or subsystem to be assessed, identifying the functions of the assessed system or subsystem, identification of the possible hazards and their effects for all the system functions, the causal factor for each identified hazard and the Risk Index (product of Probability and Severity). Risk Index (RI) is calculated based on the following assumptions:

Probability	**Severity**
A - Frequent	1 - Catastrophic
B - Probable	2 – Critical
C - Occasional	3 - Marginal
D - Remote	4 - Negligible
E - Improbable	

Failure Mode and Effect Analysis

Failure Mode and Effect Analysis (FMEA) is a widely used tool to assess systems safety, not only in aircraft industry, but also in nuclear industry for

example. The FMEA process determines what can go wrong with each individual component of a system and what effects these particular failures have [6].

This systematic group of activities is aimed to identify possible hazard situations resulting from potential effects of failures of system's components or processes in order to be able to implement proper barrier to avoid or diminish possible undesirable outcomes. Breaking down the term FMEA in its two main components ("Failure Mode" and "Effect Analysis") it also can provide a suggestive idea about the logic behind this analysis. "Failure Mode" refers to the way in which something might fail while "Effect Analysis" approaches the possible consequences of all failure modes, mainly in order to establish the consequences.

The basic steps of a FMEA process are represented by passing through a series of questions [7]:

1/. What can fail?
2/. How does it fail?
3/. How frequently will it fail?
4/. What are the effects of the failure?
5/. What is the safety consequence of the failure?

The answers to the questions above are usually organized in a worksheet as the example below:

Table 2

Example of FMEA worksheet

Component	Failure Mode	Failure Rate	Causal Factors	Effect of Failure	Risk Priority Number (RPN)

Risk Priority Number (RPN) equals the product of Severity, Occurrence and Detection. Two types of scales are can be used for the values that can be taken by each of the product terms: 1-5 or 1-10. The 1-5 scale makes it easier decide on scores. The 1-10 scale may allow for better precision in estimates and a wide variation in scores. Commonly accepted values for the three components of the RPN are:

Severity: 1 = Not Severe, 10 = Very Severe
Occurrence: 1 = Not Likely, 10 = Very Likely
Detection: 1 = Easy to Detect, 10 = Not easy to Detect

Dependence Diagrams

Dependence Diagrams are simply schematic representation of failures and combination of failures which can lead to a specific undesirable event (e.g. engine failure, flight controls failure, hydraulic system failure etc.). This schematic

representation can also be used to calculate the probability of the given failure condition as a combination of failure probabilities of the system components. As opposite, if the failure probabilities are replaced by reliability data, the reliability of the system can be calculated, and, in this situation, the Dependence Diagrams are named Reliability Diagrams. Representation of both of them is done by rectangular boxes connected by lines and arranged in series or in parallel, depending by system configuration. Series representations are "OR" conditions and the failure probabilities are added (i.e. for a total system failure is enough at least one of the components to fail).

$$Failure\ probability = A\ OR\ B\ OR\ C = A+B+C$$

Parallel representations are "AND" conditions and the failure probabilities are multiplied (i.e. for a total system failure there must be at least a component failure on each branch of the representation).

$$Failure\ probability = A\ AND\ B\ AND\ C = A\ x\ B\ x\ C$$

An example is approached next on a possible aircraft system configuration in order to show the applicability of the Dependence Diagram. The aircraft system is the landing gear and the failure event under analysis is failure of the landing gear to be lowered and locked in the down position. Every single rectangular box in the representation can be divided in more detailed components, but for simplicity the system is represented as follows:

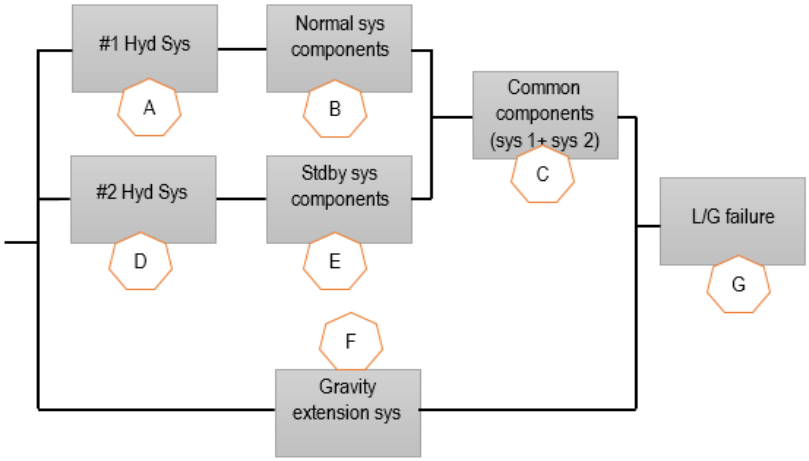

Fig. 5. Example of Dependence Diagram for aircraft system

The probability of landing gear failure to extend is:

$$P(G) = \{[P(A)+P(B)]\ x\ [P(D)+P(E)] + P(C)\}\ x\ P(F) \quad (18)$$

Fault Tree Analysis

The *fault tree* is a graphical method expressing the logical relationship between a particular failure condition and the failures or other causes leading to the particular failure condition [8]. The Fault Tree Analysis (FTA) is a technique used in reliability and design which focuses on certain individual failures or on combination of failures which can lead to a so named *top event*. FTA graphically shows the logics between failures and their connection with event under analysis (top event). As was previously shown on the Dependence Diagrams, the failure probabilities for the top event can be calculated using almost the same methodology. What is necessary to be known, are the failure probabilities of individual or combined failures of the lower levels in the fault tree. Some standard symbols are used to construct the fault trees, most common of them are found in table below:

Table 3

Standard symbols used in Fault Tree Analysis

	Basic fault event that requires no further development. Is independent of other events.
	Undeveloped event (basic event which is no further developed). Is dependent upon lower events but not developed downwards.
	Transfer symbol. Indicates a transfer continuation to a sub-tree.
	AND gate. Failure on the higher level will occur if all inputs fail.
	OR gate. Failure on the higher level will occur if any input fails.
	Inhibit gate. The input event occurs if all input events occur and an additional conditional event occurs.
	Priority AND. The output event occurs if all input events occur in a specific sequence.

Example below shows a simplistic FTA where the top event is loss of control of an aircraft due to mechanical failures resulting in aircraft crash. The accident under analysis is United Airlines Flight 232 which suffered a catastrophic failure in 1989 when the tail engine had an uncontained failure resulting in loss of all three hydraulic systems and consequently loss of flight controls. The top event situation is conditioned via an OR gate by the impossibility of the crew to control the flight controls or engines. Impossibility to move the flight controls is caused by the failure of the hydraulic systems, which, in turn is caused by the uncontained failure of the engine. The impossibility of the flight crew to control the aircraft using the engines is given by the failure of the engines, in our case only number 2 engine has failed.

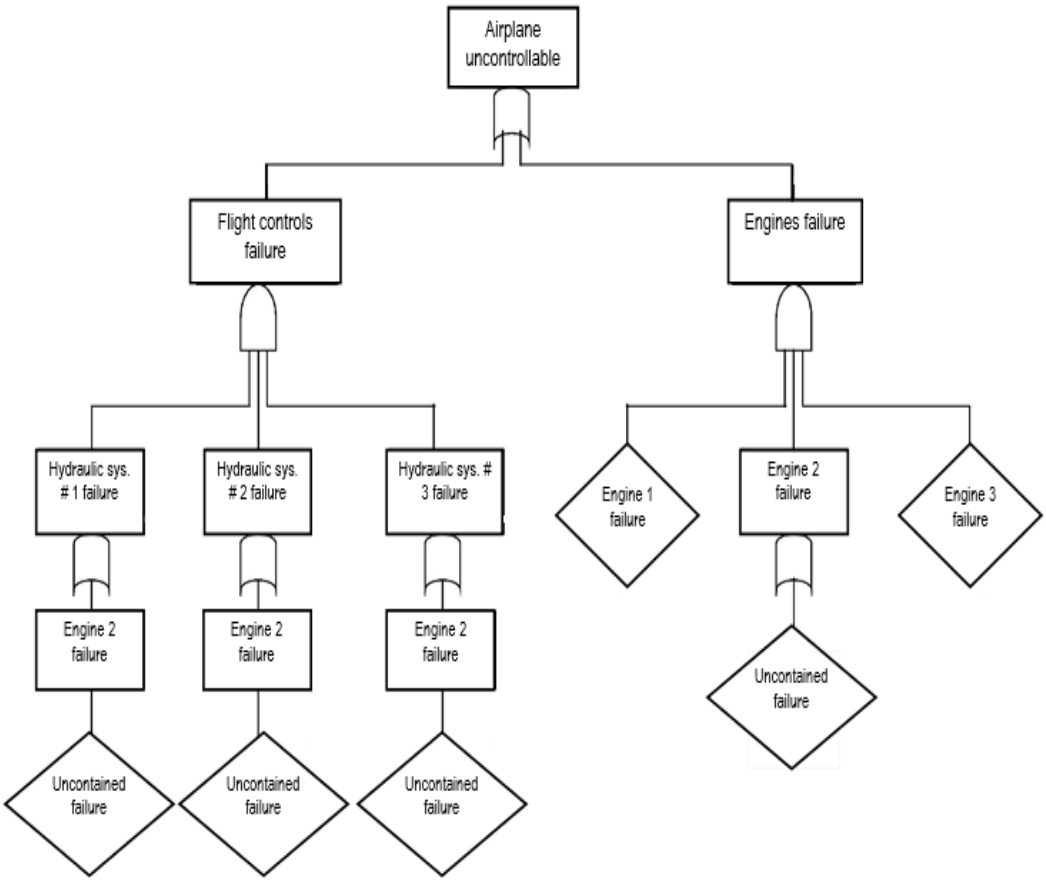

Fig. 6. Example of FTA

4. Conclusions

Reliability of aircraft, systems, components, and Risk analysis are very important tools in analysing and quantifying aircraft and aviation safety. The different methods discussed in this paper have different applicability within the aviation industry, even if some of them are borrowed from other industries (e.g. nuclear industry). They can be applied to aircraft design and certification, aircraft operation and aircraft maintenance. Improvement in technology continuously draws improvement of methods used in safety assessment, or sometimes a fully new method in order to be able to fit the idea of the new design. Nevertheless, a lot of these methods are used for years, some of them even from the beginning of the commercial aviation and they are still applicable and effective methods.

With present growing tendency of number of aircraft in service and, together with this, the number of aviation operations, the probability of the unpleasant events is increasing in direct proportion. Aviation operations include not

only the people in the air like flight crew and cabin crew, but also the people on the ground e.g. ground handlers, air traffic controllers and maintenance engineers. This is why in such a complex system with such a wide range of activities, risks appear almost everywhere. The only way safety can be improved is to understand this risks, analyse them and take the mitigation actions in order to protect the system against them.

The above presented methods are not applicable in full to these activities in operations environment, but they still represent a powerful apparatus we can use to model on different situations and to quantify, or when not possible, to make a qualitative risk assessment which can give us an idea about where we are positioned related to our safety margins.

R E F E R E N C E S

[1]. *European Aviation Safety Agency (EASA)*, Certification Specifications for Large Aeroplane, CS-25, Amendment 10, 2010.
[2]. Oxford Dictionary, 2014.
[3]. *D. P. O'Connor, A. Kleyner*, Practical Reliability Engineering, Fifth Edition, Wiley, UK, 2012.
[4]. *Isograph*, Markov Analysis (WWW document). http://www.isograph.com/software/reliability-workbench/markov-analysis/ (accessed Jan 2014).
[5]. *P. J. Wilkinson, T. P. Kelly*, Functional hazard analysis for highly integrated aerospace systems, 1998.
[6]. R. A. *Stephans*, System Safety for the 21st Century, The updated and Revised Edition of System Safety 2000, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.
[7]. *A. C. Ericson*, Hazard Analysis Techniques for System Safety, John Wiley & Sons, Hoboken, New Jersey, 2005.
[8]. *E. Lloyd, W. Tye*, Systematic Safety, Safety Assessment of Aircraft Systems, England, 1982.