Operational Risk of Aircraft System Failure

A. AHMADI*, U. KUMAR and P. SÖDERHOLM

Division of Operation and Maintenance Engineering, Luleå University of Technology, SE-971 87 Luleå, Sweden

(Received on April 17, 2009, revised November 03, 2009)

Abstract: The purpose of this paper is to describe a methodology based on Event Tree Analysis (ETA) for identification of the possible operational consequences of aircraft system failures and their associated costs. The developed methodology uses scenarios to explain the adverse effects of failure on an aircraft’s operating capability, by an integration and correlation of key parameters and events that are driving factors in causing the ultimate state of aircraft operation. The methodology was developed through studies of consequence scenarios and risk estimations where empirical data were extracted through document studies and interviews. The paper also demonstrates the application of the methodology through a case study of a hypothetical commercial aircraft.

Keywords: Event tree analysis (ETA), Operational risk, Failure consequences, Aircraft maintenance, Maintenance programme, Operation interruption, MSG-3.

1. Introduction

Assessment of the operational consequences of known, or suspected, technical failures of aircraft systems and their associated costs is an essential input for identification of the potential failure modes and their impact on aircraft operation, to enhance the capability of taking correct decisions for maintenance task development. It is also essential to identify possible design modification requirements, and to perform an analysis of the maintenance tasks’ applicability and effectiveness.

However, during the development of an initial maintenance programme for a new aircraft, the identification and quantification of the operational risk of aircraft system failure is a great challenge. This is due to a long list of uncertainties related to the large number of contributory factors, the inadequacy of in-service information, and a lack of understanding of the influence of failures.

The purpose of this paper is to describe a methodology guided by the application of an Event Tree Analysis (ETA), for identification and quantification of the different operational risks caused by aircraft system failure. The paper suggests a definition of operational consequences of failures in aircraft operation and discusses different impacts of failure on the ground and in the air. The paper introduces key parameters that are driving factors in determining the ultimate state of the operational situation when a failure occurs, and deals with the actions required if the failure has an adverse effect on the aircraft’s operating capability.

*Communicating author’s email: Alireza.ahmadi@ltu.se
The paper presents an improved and extended version of Ahmadi and Söderholm [1] with focus on methodology for consequence scenario development and failure-cost calculations.

2. Operational risk of failures

Risk can generally be defined as “a potential of loss or injury resulting from exposure to a hazard or failure”. It is an expression of the probability and the consequences of an accidental event. [2]

\[
\text{Risk (Consequence per Unit of time or space)} = \text{Frequency (Event per Unit of time or space)} \times \text{Magnitude (Consequence per Event)}
\]

The most important part of risk analysis is risk identification. Only those risks that have been identified can be managed in a systematic and conscious way. However, identification is not enough. There is also a need for action, using risk evaluation to take the appropriate operational and maintenance decisions regarding risk reduction and control, thus ensuring that the system stays in a safe state, regarding both the technical and the organizational parts [3,4].

To this end, Reliability Centred Maintenance (RCM) can be seen as a reliability and risk management methodology which seeks to identify the Maintenance Significant Items (MSI) and the applicable and effective preventive maintenance (PM) tasks. The applicability of PM tasks refers to the ability of those tasks to prevent or eliminate a failure, or at least reduce the probability of failure occurrence to an acceptable level, or reduce or mitigate the consequences of failure (the impact of failures). The PM task’s effectiveness is a measure of how well it accomplishes its purpose and the extent to which it is worth performing; i.e., whether or not it costs more than the failure(s) which it is intended to prevent [5,6,7].

The term consequence in this paper is defined in a very broad sense, and is used to mean all the events causing any type of loss, such as injury or loss of life, a high repair cost, the loss of a system, and delay or flight cancellation. Within civil aviation maintenance, the term “operational risk of failure” could be defined as “the possibility of losses arising due to aircraft technical failure, interrupting planned flight operation and making the aircraft mission incomplete”.

On the other hand, the term “operational risk of failure” can also convey the possibility of the occurrence of a failure with an operational effect, and how likely (or probable) such a consequence is. Hence, the first step in formal risk assessment is identification of the set of failure modes that may affect normal flight operation. For determining the failure modes and their effect, a functional block diagram or, as an alternative, the Failure Mode and Effects Analysis (FMEA) methodology can be used [2]. Then the analysis follows the following two steps (for each failure mode):

1. Consequence scenario development,
2. Risk estimation, which includes:
   a. Calculation of the rate of occurrence of possible consequence scenarios,
   b. Calculation of the expected (financial) loss due to the failure consequences.

3. Operational consequences of failures

In this paper, failure modes with possible operational consequences are defined as: “failure modes that might reduce the operating capability of the aircraft to meet the
intended functionality and performance requirements in the application in which the aircraft is operated”.

In general, failures affecting the aircraft’s flight altitudes, landing and flight distances, maximum take-off weight, and high drag coefficients, or failures affecting the routine use of the aircraft are also considered to have an adverse effect on the operating capability.

The effects of these failure modes interrupt the planned flight operations and interfere with the completion of the aircraft’s mission, and these operational interruptions are events by which the rate and quality of flight production are seriously affected. In aviation, the operational consequences can usually be expressed in terms of the inability to deliver services (e.g., to passengers) in a timely fashion.

These types of failures are potentially harmful to the normal scheduled operation of the aircraft, and could lead to consequences such as flight delays or cancellations, the additional cost of operational irregularities, and the cost of unplanned maintenance. When the operating capability is affected seriously, the flight crew might also have to refer to the crew check lists for abnormal occurrences or emergencies.

Failures with operational consequences may also cause different operational impact depending on whether the aircraft is on the ground or in the air. The impact on the ground may include delays related to flight dispatch, a ground turn-back (back to the gate), an aborted take-off, an aircraft substitution, and a flight cancellation. The impact in the air may include an in-flight turn-back, a diversion, a go-around, a touch-and-go landing, and re-routing. Hence, when such failures occur, they affect the rate and quality of flight production to different degrees. However, in the event of such a failure occurring, the correlation of many contributory factors can be used to recognize the ultimate state of an operation, and the extent to which the rate and quality of flight production have deviated from the pre-defined ones. Therefore, it is necessary first to identify the key contributory factors, and then to use a systematic methodology to illustrate the possible combinations of events, i.e., consequence scenarios.

4. Consequence scenario development

The goal is to identify the key parameters and events that contribute to the cause and effect relationship between the failure modes and the subsequent event progression. In fact, the integration and correlation of those parameters and events are a driving factor in causing the ultimate state of the operational situation and a factor determining the extent to which the rate and quality of flight production deviate. Through extensive studies of documents and interviews with experts, as well as the authors’ experience, the following key parameter has been recognized:

1. the nature of the failure, in terms of the adverse effects on the operating capability,
2. the possibility of the operating crew detecting the failure, during normal aircraft operation,
3. the phase of flight when the failure may occur,
4. the possibility of dispatching an aircraft with an inoperative item,
5. the possibility of continuing a flight with an inoperative item, and ultimately,
6. the pilot’s decision.

In fact, the combination of these six parameters determines 1) the extent to which operational action(s) is (are) required to keep the aircraft in operation, 2) the extent to which it is possible to postpone the maintenance action, or 3) whether or not it is necessary to restore the aircraft to its normal operating state immediately (see Figure 1).
In summary, the adverse effects of a failure on the operating capability may require the following actions which are proposed by the ATA MSG-3 document [8]:

- the correction of the failure prior to further dispatch; i.e., the failure needs immediate maintenance action,
- the use of an immediate operational procedure in flight, such as the activation or deactivation of a system,
- the imposition of operating restrictions such as a reduced flight altitude, and
- the use of abnormal or emergency procedures by the flight crew when the aircraft is airborne, e.g., an aborted take-off, an in-flight turn-back, a diversion, or a touch-and-go landing.

5. Proposed methodology for consequence scenario development

In order to illustrate the integration and correlation of the above-mentioned parameters and to develop possible consequence scenarios, Event Tree Analysis (ETA) was chosen as an appropriate methodology in this study.

One major reason for this selection is that ETA can be used to determine the likelihood and severity of a range of consequence scenarios, given different sequences of events. Moreover, ETA can be used for qualitative as well as quantitative reliability and risk analyses [9]. Hence, if sufficient data and information regarding the failure frequency and the probability of occurrence of each event are available, the frequency of occurrence of each consequence scenario can be calculated.

The ETA presented in this study starts with the identification of the initiating events (the first triggering event of the sequence), i.e., the failures of interest for further analysis. The consequences of the candidate failures are developed by considering the failure and success of two predefined main criteria and their included alternative states. The two main criteria displayed in the proposed event tree analysis are (see Figure 2):
1. The phase of flight operation when the failure occurs or is detectable. In this
criterion five different states have been included, i.e., prior to take-off, take-off,
climb, cruise, and approach and landing. In the real world, two different events
may occur in each state; i.e., the failure either occurs or does not occur.

2. The adverse effect of the failure on the operating capability of the aircraft. In this
second criterion, three different states have been included which indicate the
extent to which the failure affects the operating capability of the aircraft, i.e., the
deferability of the failure, the imposition of any operational restriction, or the use
of abnormal or emergency procedures.

   The first state of the second criterion, “the deferability of the failure”, indicates
whether the failure is deferrable or if it requires an immediate action, e.g., performing
corrective maintenance or following some specified operational procedures. Failures that
are related to deferrable items are those that are non-critical with regard to aircraft safety;
i.e., the aircraft can continue its normal flight with the failure present [10]. This can be
identified through consultation of the Minimum Equipment List (MEL), the Flight Manual
(FM), the Flight Crew Operation Manual (FCOM), or the Quick Reference Handbook
(QRH). MEL advice is a Time-since-Fault repair strategy which involves a countdown
being started towards the appropriate dispatch time. Once this countdown has reached
zero, the fault must be repaired before further dispatch of the aircraft is allowed [11].

   The second state of the second criterion, “the imposition of any operational
restriction”, concerns the need to impose any operational restrictions, such as an altitude
restriction, which are mandated by procedures or by a pilot decision. Finally, the third
state of the second criterion, “the use of abnormal or emergency procedures”, refers to the
application of some emergency or abnormal operation which is mandated by procedures
or by a pilot decision. The analysis proceeds through all the alternative paths, by
considering each consequence as a new initiating event (see Figure 2).

5.1 Results of the proposed ETA development

In Figure 3 it is shown how the combination of the occurrences of different events (Yes or
No) within the states of the two criteria (the operational phase and the effect on the
operating capability) will create different scenarios, which in turn will determine the
ultimate operational consequences.

   Based on the possible combination of events, 25 primary scenarios were identified
which ultimately will lead to one or a combination of the following classes of
consequences:

   1. No operational consequence,
   2. Ground delays (at departure and on arrival),
   3. Airborne delays,
   4. Emergency or abnormal operation, which may include:
      a. aborted take-off,
      b. in-flight turn-back, or
      c. diversion, go-around, and touch-and-go landing.
Out of the 25 different scenarios that were identified, there are six scenarios with no operational consequences. One of these scenarios is when a failure never occurs, i.e., scenario 25. The other five scenarios where no operational consequences occur are when the failure’s associated maintenance is deferrable and there are no necessary operational restrictions or abnormal procedures applied (see Figure 3 for scenarios 2, 6, 11, 16 and 21). There are also 14 event scenarios where the consequences are some sort of delay (i.e., scenarios 1, 3, 4, 5, 8, 9, 10, 13, 14, 15, 18, 19, 20, 23 and 24). Out of these scenarios, there are five where the operational consequences are manifested only as airborne delay (i.e., scenarios 1, 5, 10, 15, 20 and 23). These scenarios are connected to the occurrence of a failure which is related to deferrable maintenance, but which requires some operational restrictions. It has to be noted that this study has not taken into account the effect of failure which ultimately leads to higher fuel consumption or a loss of the ability to use the normal capacity of the aircraft as planned. Hence, these consequences are not included among the ultimate consequences. However, in future implementation of the proposed methodology, one could include them without any major changes in the proposed methodology. Abnormal procedures contributing to operational consequences have also been found in four scenarios (i.e., scenarios 7, 12, 17 and 22). All these scenarios are related to failures which need non-deferrable maintenance, which entail some sort of significant operational restriction, and which require emergency and abnormal procedures to be initiated by the flight crew. All of these events result in direct financial losses, such as additional costs related to the flight crew, the ramp and airport, the aircraft itself, and the passengers, and might lead to a loss of revenue if the failure effect leads to flight cancellation.

6. Risk estimation

The total operational risk is the sum of all the risks associated with the possible consequence scenarios in all the operational phases that have arisen from the proposed ETA. Hence, for a single component with a failure of type \( i \) and with \( n \) as the number of consequence scenarios, the total associated financial risk, \( R_{\text{Total}} \), can be calculated as:

\[
R_{\text{Total}} = \lambda \times \left[ \sum_{k=1}^{n} (P_i \times C_{s_k}) \right]
\]

where, \( R_{\text{Total}} \) = the expected financial risk of failure per flight hour (FH), \( \lambda \) = the rate of occurrence of failure per FH (a constant value), \( C_{s_k} \) = the cost of consequence scenario \( i \) (USD/consequence), and \( P_i \) = the probability of scenario \( i \). For a multi-consequence scenario, \( R_{\text{Total}} \) can be expressed as:

---

**Figure 2:** The main criteria and states for aircraft operational consequences.
Operational Risk of Aircraft System Failures

\[
\text{Amount of loss(Cost)} \downarrow
\]

\[
\begin{bmatrix}
\text{Probability of scenario 1} \\
\vdots \\
\text{Probability of scenario n} \\
\end{bmatrix}
\times
\begin{bmatrix}
\text{Consequences of scenario 1} \\
\vdots \\
\text{Consequences of scenario n} \\
\end{bmatrix}
\]

Consequently, the annual expected loss, i.e., the financial risk due to failure type \(i\), for the whole aircraft can be estimated as:

\[
R_{\text{Annual}} = R_{\text{total}} \times U \cdot N
\]

where \(U\) is the average annual utilization of the aircraft (FH/year), and \(N\) is the quantity per aircraft (QPA). This calculation can in turn easily be expanded for an aircraft fleet.

7. Verification of the proposed methodology

In order to verify the application of the proposed event tree, the example of a failure mode of an engine driven hydraulic pump (EDHP) of an aircraft hydraulic system has been selected. The example involves a hypothetical EDHP and aircraft, but it is still representative. The EDHP is used to provide a hydraulic pressure of 3500 ± 300 PSI for different systems, mainly the flight control, landing gears, and doors. The system has a highly redundant design with two EDHPs and two back-up electrically driven hydraulic pumps. One of the functional failures of the EDHP system can be defined as the “inability to provide the required hydraulic pressure” due to the failure mode “pump jammed”, with a failure rate of \(1.02 \times 10^{-4}\). If this failure occurs, a “low pressure” warning light turns on or a message appears on the cockpit display, so that the crew will be aware of the fault in any phase of flight. Hence, the failure is classified as an evident functional failure. Due to the high redundancy of the system, the failure does not have any direct adverse effect on safety. However, the failure will have a direct adverse effect on the operating capability. Therefore, according to the manufacturer’s advice and related regulations, the aircraft must be restored to its normal operating state by the maintenance crew immediately. Depending on the phase of flight during which the failure occurs, the failure situation may require the pilot to perform one of the following actions: a return to gate, an aborted take-off, an in-flight turn-back, or a diversion to another airport than the planned one. The outcome of the ETA for the hypothetical EDHP, the applicable values for each probability, and the average consequence cost, which has been gathered from expert opinions, are shown in Table 1, where \(P_1\) and \(P_2\) denote the probability of the first and second criteria in ETA, respectively. Using Equation 1 and Table 1, for a single EDHP, \(R_{\text{Total}}\) can be estimated as:

\[
R_{\text{Total}} = \left(1.02 \times 10^{-4}\right) \times \begin{bmatrix} 0.10; 0.35; 0.1; 0.2; 0.25 \end{bmatrix} x = (0.05825 \text{USD/FH})
\]

Assuming 3,000 FH of utilization per year, the annual total consequence cost for the whole aircraft (two EDHPs, \(N = 2\)) can be estimated in accordance with Equation 2:

\[
R_{\text{Annual}} = R_{\text{Total}} \times U \cdot N = 1.05825 \times 3000 \times 2 = 6349.5 \text{ per Aircraft/Year}
\]
### Figure 3: Proposed event tree for assessing the possible operational consequence scenarios caused by aircraft system failure
8. Conclusions

The available standards regarding aircraft maintenance programme development (e.g., RCM) describe the steps required for their implementation on a general level. However, some steps, such as determining the risk of operational consequences of failures, which play a vital role in selecting an applicable and effective decision, have not been defined in detail. This paper aims at bridging this gap by outlining a proposed methodology for identification of the different operational consequences and associated costs of aircraft system failure due to technical interruption.

The paper describes the key parameters and events that contribute to the cause and effect relationship between a failure mode and the subsequent event progression. The description demonstrates how the integration and correlation of the key parameters and events determine the ultimate state of the operational situation.

In order to enhance the implementation of the proposed methodology, uncertainty analysis should be performed regarding the rate of occurrence of failure and all the ETA headings. Furthermore, the quality and adequacy of the required information should be considered. This information is mainly related to the failure rate, and the probability of occurrence of each event. Moreover, enough knowledge about the reliability and the maintainability performance of the analysed system is essential. Other information that is needed is related to the aircraft operation and associated procedures which are given in formal documents. Therefore, both the available data and the knowledge of the analyst who is performing the ETA play important roles in achieving accurate results.

References


---

Table 1: Probability and Cost Figures of Operational Consequences

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Phase of Flight</th>
<th>Probability of Scenario</th>
<th>Candidate Failure Consequence(s)</th>
<th>Cost of event</th>
<th>Magnitude (Minutes)</th>
<th>Total cost of scenario (USD/event)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No4</td>
<td>Prior to take-off</td>
<td>0.10 0.10 0.10</td>
<td>Ground delay at departure</td>
<td>70 $/min.</td>
<td>120 min</td>
<td>8400</td>
</tr>
<tr>
<td>No7</td>
<td>Take-off</td>
<td>0.10 0.20 0.10</td>
<td>Aborted take-off</td>
<td>1900 $/event</td>
<td>NA</td>
<td>10300</td>
</tr>
<tr>
<td>No12</td>
<td>Climb</td>
<td>0.10 0.10 0.10</td>
<td>In-flight turn-back</td>
<td>2900 $/event</td>
<td>NA</td>
<td>11300</td>
</tr>
<tr>
<td>No17</td>
<td>Cruise</td>
<td>0.10 0.10 0.10</td>
<td>Ground delay on arrival</td>
<td>70 $/min.</td>
<td>120 min</td>
<td>10800</td>
</tr>
<tr>
<td>No22</td>
<td>Approach &amp; landing</td>
<td>0.25 0.25 0.25</td>
<td>Ground delay at departure</td>
<td>70 $/min.</td>
<td>120 min</td>
<td>13500</td>
</tr>
</tbody>
</table>

---

Additional text not included in the table:


Alireza Ahmadi is a Ph.D. candidate at the Division of Operation and Maintenance Engineering, Luleå University of Technology (LTU), Sweden. He has received his Licentiate degree in Operation and Maintenance Engineering in 2007. Alireza has more than 10 years of experience in civil aviation maintenance as licensed engineer, and production planning manager. His research topic is related to the application of RAMS to improve aircraft maintenance program development.

Uday Kumar is a Professor of Operation and Maintenance Engineering at Luleå University of Technology, Luleå, Sweden. His research and consulting efforts are mainly focused on enhancing the effectiveness and efficiency of maintenance process at both operational and strategic levels and visualizing the contribution of maintenance in an industrial organization. He has published more than 125 papers in peer reviewed international journals and chapters in books. He is reviewer and member of the Editorial Advisory Board of several international journals. His research interests are Maintenance Management and Engineering, Reliability and Maintainability Analysis, LCC, etc.

Peter Söderholm is an Assistant Professor at the Division of Operation and Maintenance Engineering, Luleå University of Technology (LTU). His research topics are risk, dependability, and application of Information & Communication Technology (ICT) within maintenance, mainly within aviation. He received his M.Sc. degree in 2001 in Mechanical Engineering and PhD in Operation and Maintenance Engineering in 2005, from LTU.