

# Average Probability Calculation Methods for System Safety Analysis

Anapathur V. Ramesh  
Boeing Commercial Airplanes

## ABSTRACT

Fault-tolerance in commercial aircraft applications is typically achieved by redundancy. In such redundant systems the primary component is checked before the start of a flight to see if it operates correctly. The aircraft will not take off unless the primary is functioning. Airplane manufacturers must certify the airplane systems to be safe for flight. One means of safety certification is by safety analysis which shows that the probability of failure in a typical flight is bounded. The probability bound requirement for a system is based on the criticality of system failure.

Usually backup components are checked at intervals that span multiple flights. The first backup may be checked more frequently than the second or higher levels. This leads to flights where the system may have latent faults in the backup components. The probability of failure in such cases varies from flight to flight due to the different exposure times for components in the system. So we are led into the concept of "Average Probability of Failure per Flight".

AC/AMC 25.1309 and SAE ARP 4761 document simple formulas for average probability failure calculation which are applicable under restricted conditions such as small failure rates etc. In this paper we will discuss new methodologies and equations which relax these restrictions. The intent of this paper is to provide a single source for Average Probability of Failure per Flight calculations, describe the role of advanced Markov and Petri Net tools in these calculations, and provide best practice recommendations.

**CITATION:** Ramesh, A., "Average Probability Calculation Methods for System Safety Analysis," *SAE Int. J. Aerosp.* 8(2):2015, doi:10.4271/2015-01-2436.

## INTRODUCTION

Safety analysis is an important and acceptable means of compliance in the airplane system safety certification process [7,8,9]. Fault Tree Analysis (FTA) is a well-known and most used technique for system safety analysis. Adequate guidance for the safety analysis process is available in industry recommended best practices such as SAE ARP4761 [9]. Although highly useful, FTA methodology has some limitations in modeling specific scenarios such as in calculating average probability of failure when multiple latent faults are present, especially so if present in the same minimal cutset. The limitations arise due to FTA not being capable of representing repairs, sequence dependence and time-dependence very well. FTA can handle very large system safety models essentially because it focuses on the system failure structure (combinations) very well but not as well on the failure dynamics. Stochastic process modeling methods such as Markov Models and Petri nets are needed if one wants to model the time and sequence dependence on failures and repairs well in addition to the structure. In some scenarios the system dynamics become important such as deferred repair scenarios (MMEL or TLD), conditional repair, time-dependent failure rates or repair, accurate average probability evaluation of multiple latent scenarios etc. The

soon to be released update of ARP4761 intends to provide best practice guidance on Markov models for modeling such scenarios. In what follows we first define the concept of "Average Probability of Failure" for a system and the equation for it. Later we describe the different methods to calculate the average probability from simple equations (approximate and exact) to more complex modeling methods which will require custom analysis solvers and tools. We also show the application of these methods via examples and provide guidance on using them in practical applications.

## AVERAGE PROBABILITY DEFINITIONS

Assume that an airplane is operated for a total of  $N$  flights in its life time with each flight being of a constant duration of  $t$  flight hours. This is an idealization of reality (see Figure 1) and  $t$  represents the average flight length of a typical airplane of a specific type. An example could be 3000 flights per year of average duration of 1.5 hours and an airplane life of 20 years. This results in  $N = 60000$  with  $t = 1.5$  hours. Airplane life can also be expressed in flight hours as  $T$ , which in this example would be 90000 hours.

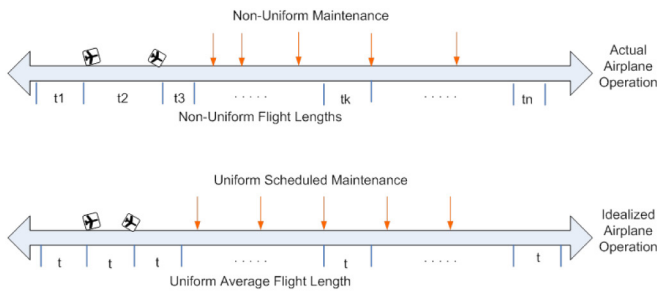


Figure 1. Motivation for Average Probability Analysis - Operation Idealization for Safety Analysis

Assume that the system under analysis comprising one or more redundant components operates and provides a function for the full flight of duration  $t$ . If the system operates for only a portion of the flight, the analysis methods can be applied by adjusting the flight length to system operation time.

If  $P_i$  is the probability of system failure in the  $i$ -th flight then we define the Average Probability of Failure per Flight as

$$P_{avg} = \frac{\sum_{i=1}^M P_i}{N} \quad (1)$$

Note that  $P_i$  is the probability the system fails anywhere in the typical flight of duration  $t$  given that it was working at the start of a flight. If the system fails there is a loss of function that is noticeable or indicated and results in the full repair or complete replacement of the system on the ground before the next flight. The implication is that a system can fail only once in a given flight and hence the definition of average probability of failure as in Eq. (1) makes sense. Note that this definition is identical to the one in the Appendix 3, Eq. (c) if “system failure” is substituted for “Failure Condition” in AC 25.1309 (Arsenal Version), AMC 25.1309 [7,8].

Another way of describing the metric in (1) is

$$P_{avg} = \frac{E[M(T)]}{N} \quad (2)$$

where  $E[M(T)]$  is the expected number of system failures (full repairs/replacements) in the life  $T$  of the airplane. Based on the assumption of system repairs/replacements only on ground, at most one replacement can happen for every flight and thus  $M(T)$  is less than or equal to  $N$ , the measure in (2) above makes sense and is equivalent to Eq. (1). In ultra-high reliable systems or critical failure conditions  $E[M(T)]$  will be a small fraction of the order of  $1E-01$  to  $1E-05$ .

A near equivalent continuous-repair analogue of the metric in (1), (2) can be defined for ultra-high reliable systems with not much loss in accuracy if we remove the restriction of replacement/repair only on ground. Considering that for safety critical systems the probability of

system failure or failure condition is very small in a flight (of the order of  $1E-06$  to  $1E-09$  per flight) and that the flight length  $t$  is much smaller than life of airplane  $T$  the following definition is nearly equivalent to those in Eqs. (1) and (2).

$$P_{avg} = \frac{t}{T} \int_0^T m(x) dx = t * \frac{E[M(T)]}{T} \quad (3)$$

The integrand  $m(x)$  is also called the *Instantaneous System Renewal Rate*.  $P_{avg}/t$  is the “Average Probability of Failure per Flight Hour”. It is equivalent to the *average system renewal rate*. Stochastic Renewal theory and Modeling methods [1,4, 6] can be used to obtain the renewal rate as we will show in the following sections.

For highly reliable systems where the chance of multiple instance of system failures in life of an airplane is very small (as is common in airplane safety analysis) the instantaneous renewal rate  $m(t)$  may be replaced in Eq. (3) without much loss of accuracy by the failure density function  $f(t)$  and thus an approximate expression for failure probability is obtained as in Eq. (4) where  $F(T)$  is the system cumulative failure probability function evaluated at time  $T$ .

$$P_{avg} = \frac{t}{T} \int_0^T m(x) dx \approx \frac{t}{T} \int_0^T f(x) dx = t * \frac{F(T)}{T} \quad (4)$$

## ANALYSIS METHODS

Analysis methods can be classified multiple ways depending on how they attempt to calculate  $P_{avg}$ . The primary means is to compute  $P_i$  for each flight and then use Eq. (1) to compute the average. For small systems or a cutset with a small number of latent failures exact or approximate closed-form formulas can be derived using Eq. (1) or Eq. (3). For larger systems the methods available are to use numerical solution of Markov models and applying Eq. (1) and/or a hybrid approach where a closed-form solution or a numerical solution using a Markov model is combined with Fault Tree Analysis.

### Closed-Form Methods for Small Systems or FT Cutsets

For small systems or simple cutsets, Eq. (1) can be applied to generate closed-form formulas for average failure probability to varying degrees of approximation.

An approximation method for deriving closed-form formulas or computing system failure probability was detailed in [5] as follows.

1. Enumerate the possible states the system could be in at the start of a generic flight. This should take into account possible system and component maintenance just prior to the generic flight.
2. Evaluate the conditional probability of system failure in the generic flight given the system starts in each of the states enumerated in step 1. For a dual or triple redundant system with stochastically independent component failures the conditional

probability of failure can be quite easily expressed in terms of the conditional survival probabilities of the components.

3. Approximate the probability of being in the enumerated system states of step 1 using the latencies of the components. The latencies are calculated in terms of the number of flights since the last maintenance check for the component.
4. The probability of failure  $P_i$  is obtained by summing on all the enumerated system states in step 1 the product of the conditional probabilities of system failure evaluated in step 2 and the probability of being in the enumerated system state estimated in step 3.

## Dual Redundant System or Dual-Term Cutset

### Single Latent Failure Scenario

Consider a dual redundant system with two components A and B. Component A is the active component providing the necessary function. Component B is the backup component and is switched in when A fails during a flight. We make the following assumptions about the system:

- The active component A is always checked and restored (or replaced) if failed before any flight.
- The backup component B is never checked for airplane life and therefore can fail latent.
- The switching system that switches in a backup cannot fail.

Let  $\lambda_A$  and  $\lambda_B$  represent the constant failure rates of the components A and B respectively. At the beginning of the  $i$ -th mission ( $i \geq 1$ ) component A is guaranteed to work. Only B may or may not be working. Using the approximation method outline, the probability of system failure in the  $i$ -th flight is shown in Table 1 based on the conditions

Table 1. Dual Redundant System with a Single Latent Component

| Condition at the start of $i$ -th flight | P(system failing in $i$ -th flight   condition) | P(condition)               |
|------------------------------------------|-------------------------------------------------|----------------------------|
| A working, B working                     | $(1-e^{-\lambda_A t})(1-e^{-\lambda_B t})$      | $e^{-\lambda_B(i-1)t}$     |
| A working, B failed                      | $(1-e^{-\lambda_A t})$                          | $(1-e^{-\lambda_B(i-1)t})$ |

The conditional probabilities of system failure in column 2 of the table are exact and the approximation is only in column 3, where the probability of the condition is approximated by the latency of B alone. The true failure process is a complex renewal process and the Markov method internally calculates these probabilities accurately. Nevertheless for highly reliable systems the approximation is reasonable as will be seen later. We can now obtain  $P_i$  using step 4 of the approximation method detailed before.

$$P_i = e^{-\lambda_B(i-1)t} (1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t}) + (1 - e^{-\lambda_B(i-1)t}) (1 - e^{-\lambda_A t}) = (1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t})$$

(5)

Using Eq. (1) and using some algebra on the resulting series summation we can obtain  $P_{avg}$  as

$$P_{avg} = (1 - e^{-\lambda_A t}) \left( 1 - \frac{e^{-\lambda_B t} (1 - e^{-\lambda_B Nt})}{N(1 - e^{-\lambda_B t})} \right) \quad (6)$$

If the product of failure rates and latent component exposure time ( $Nt$ ) is small then a linear upper bound for the probability of failure (i.e. replace  $(1 - e^{-\lambda_B t})$  with  $\lambda_B t$ ) can be made resulting in

$$P_{avg} = (1 - e^{-\lambda_A t}) \frac{\sum_{i=1}^N (1 - e^{-\lambda_B it})}{N} \leq \lambda_A t \frac{\sum_{i=1}^N \lambda_B ti}{N} = \lambda_A t \lambda_B \frac{Nt}{2} \left( 1 + \frac{1}{N} \right) \quad (7)$$

The above equation shows that for average probability calculation we can multiply the exposure time ( $Nt$ ) of the latent component with a factor of 0.5. Industry guidelines such as in [9] recommend using  $(T/2)$  for the exposure time of the latent component in an active-latent two event AND gate in a FTA but it is recognized in the document that this is valid when the product of the failure rates of both active and latent event with the exposure time of the latent is small (which is typically less than 0.01).

Let  $t = 3$  hours and  $N = 1000$  flights. Table 2 shows the average per flight system failure probability as computed using Eq. (6) and the Markov solver and the relative error.

Table 2. Approximation accuracy for dual redundant system with single latent component for equal component failure rates

| $\lambda_A = \lambda_B$ (per hour) | $P_{avg}$ (per flight) |               | Error (%) |
|------------------------------------|------------------------|---------------|-----------|
|                                    | Eq. (6)                | Markov Solver |           |
| 1.0E-07                            | 4.5040E-11             | 4.5036E-11    | 0.009     |
| 1.0E-06                            | 4.5000E-09             | 4.4955E-09    | 0.100     |
| 1.0E-05                            | 4.4597E-07             | 4.4157E-07    | 0.996     |
| 1.0E-04                            | 4.0851E-05             | 3.7237E-05    | 9.70      |
| 1.0E-03                            | 2.0481E-03             | 1.2514E-03    | 63.6      |

From Table 2 we see that the approximation works well only when the system failure probability is low. From Table 3 we note also that the active component failure rate needs to also be small for good accuracy.

Table 3. Approximation accuracy for dual redundant system with single latent component for diverse component failure rates

| $(\lambda_A, \lambda_B)$ (per hour) | $P_{avg}$ (per flight) |               | Error (%) |
|-------------------------------------|------------------------|---------------|-----------|
|                                     | Eq. (6)                | Markov Solver |           |
| (1.0E-08,1.0E-02)                   | 2.9015E-08             | 2.9015E-08    | 0         |
| (1.0E-07,1.0E-03)                   | 2.0512E-07             | 2.0511E-07    | 0.005     |
| (1.0E-06,1.0E-04)                   | 4.0857E-07             | 4.0818E-07    | 0.096     |
| (1.0E-04,1.0E-06)                   | 4.4993E-07             | 4.0818E-07    | 10.2      |
| (1.0E-03,1.0E-07)                   | 4.4973E-07             | 2.0511E-07    | 119.3     |
| (1.0E-02,1.0E-08)                   | 4.4375E-07             | 2.9015E-08    | 1429      |

We can relax the small failure rate assumption for both active and latent component further but retain the assumption that the failure probability of the system is small enough that more than one system failure in life of airplane is remote and perform a more careful analysis of the sequence of failures leading to a condition in the approximation method as shown in Table 4.

Table 4. Dual Redundant System with a Single Latent Component conditioning on component failure sequence

| Condition at the beginning of i-th flight          | P(Condition) | P(system failure in flight i   Condition) | Order of failure in flight i | Comments                                              |
|----------------------------------------------------|--------------|-------------------------------------------|------------------------------|-------------------------------------------------------|
| System failed                                      | $P(i-1)$     | 0.0                                       | N/A                          | System cannot fail twice (assumed)                    |
| System not failed AND B working $\equiv$ B working | P(C1)        | P(11)                                     | A fails first then B         | A is known to work at the beginning of flight         |
| System not failed AND B working $\equiv$ B working | P(C1)        | P(12)                                     | B fails first then A         | A is known to work at the beginning of flight         |
| System not failed AND B failed                     | P(C2)        | P(2)                                      | A fails                      | B is already failed; A is the only one which can fail |

Where

$$P(C1) = e^{-\lambda_B(i-1)t}$$

$$P(11) = (1 - e^{-\lambda_B t}) - \frac{\lambda_B}{\lambda_A + \lambda_B} (1 - e^{-(\lambda_A + \lambda_B)t})$$

$$P(12) = (1 - e^{-\lambda_A t}) - \frac{\lambda_A}{\lambda_A + \lambda_B} (1 - e^{-(\lambda_A + \lambda_B)t})$$

$$P(C2) = (1 - e^{-\lambda_B t}) \sum_{k=1}^{i-1} e^{-\lambda_B(i-1-k)t} e^{-\lambda_A k t}$$

$$= \frac{(1 - e^{-\lambda_B t}) e^{-(\lambda_A - \lambda_B)t}}{1 - e^{-(\lambda_A - \lambda_B)t}} (e^{-\lambda_B(i-1)t} - e^{-\lambda_A(i-1)t})$$

$$P(2) = (1 - e^{-\lambda_A t})$$

Note that P(C2) considers the case where B is already failed in a previous flight k and thus A has to not fail the entire period from when B failed to the i-th flight. Using these equations we have:

$$P(\text{system failure in mission } i \text{ with A failing first then B}) = P(C1) * P(11)$$

$$P(\text{system failure in mission } i \text{ with B failing first then A}) = P(C1) * P(12) + P(C2) * P(2)$$

$$P(\text{system failure in } N \text{ flights with A failing first then B})$$

$$= \text{TERM1}$$

$$= P(11) * \sum_{i=1}^N P(C1)$$

$$= \left[ (1 - e^{-\lambda_B t}) - \frac{\lambda_B}{\lambda_A + \lambda_B} (1 - e^{-(\lambda_A + \lambda_B)t}) \right] \frac{(1 - e^{-\lambda_B N t})}{(1 - e^{-\lambda_B t})}$$

$$P(\text{system failure in } N \text{ flights with B failing first then A})$$

$$= \text{TERM2} + \text{TERM3}$$

$$= P(12) * \sum_{i=1}^N P(C1) + P(2) * \sum_{i=1}^N P(C2)$$

where

$$\text{TERM2} = \left[ (1 - e^{-\lambda_A t}) - \frac{\lambda_A}{\lambda_A + \lambda_B} (1 - e^{-(\lambda_A + \lambda_B)t}) \right] \frac{(1 - e^{-\lambda_B N t})}{(1 - e^{-\lambda_B t})}$$

and