Aircraft Safety Modeling For Time-Limited Dispatch

Darren R. Prescott, Loughborough University
John D. Andrews, Loughborough University

Key Words: Time-Limited Dispatch, FADEC system reliability, Monte Carlo simulation

SUMMARY & CONCLUSIONS

This paper offers an alternative method of modeling the Time-Limited Dispatch (TLD) of aircraft. Existing methods involve the use of fault tree analysis and Markov analysis with various simplifying assumptions. Monte Carlo simulation (MCS) is the suggested alternative, which overcomes the problems associated with the other techniques, such as dependencies between basic events (fault tree analysis) or huge number of system states (Markov analysis). The results obtained from the analysis of a simple example are compared for the existing modeling approaches and MCS. MCS is seen to have potential advantages, especially when modeling TLD for large, full scale systems.

1. *BACKGROUND*

Introduced to commercial transport aircraft about 20 years ago, Full Authority Digital Electronic Control (FADEC) systems govern engine thrust from the time fuel metering begins to the point of fuel shutoff. Until the introduction of these electronic engine control systems hydromechanical control (HMC) systems were used. In these applications of FADEC it was to be the first time that pilots would have no HMC systems available as backup in the event of an electronic system failure [1].

FADEC systems contain a certain level of redundancy, incorporating a dual channel control system. This involves having two essentially identical channels per engine. Each critical loop or function in the FADEC contains either redundant elements or dual systems. Despite this redundancy, the dispatch criteria imposed after the introduction of FADEC were overly restrictive, increasing the numbers of delays and cancellations of flights [2]. This was due to the occurrence of independent faults in more than one channel. Because levels of reliability are higher for FADEC systems than for HMC systems an opportunity existed to use available redundancy to allow dispatch with faults present. This would still allow airworthiness standards to be met and also reduce the numbers of delays and cancellations, along with the added benefit of allowing better planning of maintenance operations. This new approach, allowing degraded redundancy dispatch was named time-limited dispatch (TLD).

2. *INTRODUCTION TO TLD*

TLD allows the dispatch of aircraft in the presence of one or more known faults whilst assuring a certain level of system reliability. Depending on the significance of the faults aircraft may be dispatched for differing lengths of time. These dispatch intervals give the maximum length of time that the aircraft may be dispatched with faults present before those faults must be addressed. There are four categories of dispatch interval. These are:

- Do Not Dispatch (DND),
- Short Time Dispatch (STD),
- Long Time Dispatch (LTD),
- Manufacturer/Operator Defined Dispatch (MDD).

The implementation of the DND dispatch category means that the aircraft must not be dispatched because of the faults present and maintenance must be undertaken immediately. The STD dispatch category allows dispatch in the short-term and the LTD category for a relatively longer time before repairs are carried out. The final category of dispatch, MDD, is reserved for faults falling into none of the other three categories and not affecting the loss of thrust control (LOTC) rate [2]. An upper limit for the LOTC rate of 100 events per 10^6 flight hours (flt. hrs.) is given by the FAA for dispatchable system configurations. The maximum average LOTC rate of the system must not exceed 10 events per 10^6 flt. hrs. This level matches that which was achieved by the HMC systems superceded by FADEC.

2.1 *Maintenance Strategies*

Two strategies exist that may be used to maintain the FADEC systems of aircraft when TLD is applied. The first of these is minimum equipment list (MEL) maintenance [2], which would normally be used on STD category faults. The exact time of occurrence of any fault maintained using this approach must be known. As the fault occurs a 'countdown' of the dispatch time is initiated. The fault must be remedied, at the latest, by the time the countdown reaches zero. Figure 1 illustrates this process. The fault occurs at time t_1, after which the dispatch interval is initiated. At the end of the countdown, at t_2, the fault must be repaired, if the repair has not already been implemented.

The second maintenance strategy used is periodic inspection/repair (PIR), which involves checking the system for faults at regular intervals. This is most often used to maintain faults in the LTD category. Unlike MEL maintenance PIR does not require knowledge of the exact time of occurrence of the fault. Faults, discovered at inspections, are assumed to occur at the midpoint of consecutive inspections [2]. This is considered reasonable since the fault will, on average, occur at this time, assuming the failure rates for faults are constant with time and the periodic inspection interval is less than the mean time between failures (MTBF) of

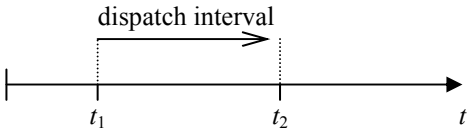

Figure 1. MEL Maintenance.

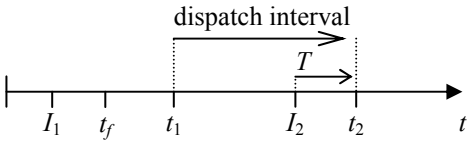

Figure 2. PIR Maintenance.

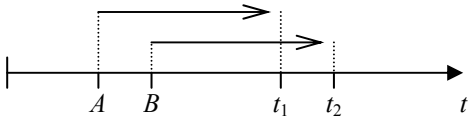

Figure 3. Multiple Faults

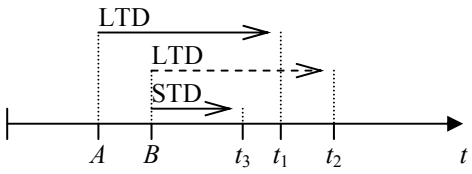

Figure 4. Faults Acting in Combination – MEL

the sum of failure rates in that category. The dispatch interval is then deemed to have begun at the midpoint of the inspections and the allowable period of dispatch after the inspection is calculated. This maintenance strategy is illustrated in Figure 2. I_1 and I_2 represent two consecutive inspections. A fault, occurring at time t_f, is discovered at I_2 and assumed to occur at t_1. If the dispatch interval is assumed to begin at this time the aircraft may be dispatched until time t_2, giving an allowable period of dispatch of time T at I_2. In practice the inspection interval for a fault category must not exceed twice the dispatch interval for faults of that category. This ensures that the average exposure to faults does not exceed the dispatch interval.

If PIR is used to maintain faults of more than one dispatch category a situation can occur where a fault is discovered at an inspection for faults of a different category. In this case the fault could be treated as if found for the first time at the next inspection for faults of its own dispatch category. In this way a STD fault discovered at a LTD inspection could be treated as if discovered at the next inspection for STD faults [2].

Due to the different approaches involved in the MEL and PIR maintenance strategies the maximum possible exposure time of the system to faults will differ. In MEL the maximum possible exposure time is equal to the dispatch interval, but in PIR the maximum possible exposure time is equal to twice the dispatch interval.

There is a possibility that more than one fault may exist within a FADEC system at any one time. In such cases these faults may be repaired in a number of different ways. Below are some examples of the situations that may arise, along with some of the maintenance possibilities.

Figure 3 depicts the occurrence of two faults, A and B. If these faults were to be maintained using MEL maintenance dispatch intervals for these faults would end at t_1 and t_2 respectively. Upon reaching the end of the first dispatch interval, at t_1, a number of strategies are possible. At this point fault A must be addressed to allow further dispatch. Fault B may also be repaired at this time, allowing dispatch until another TLD fault occurs. Alternatively, fault B may be left in the system and the aircraft may be dispatched until its associated dispatch interval ends at time t_2.

In the situation just described it may be that with the simultaneous occurrence of faults A and B a reduction in the dispatch interval is specified. This scenario is depicted in Figure 4, again for the case of MEL maintenance. In this case faults A and B, when occurring alone, bring about the initiation of LTD intervals, which would end at t_1 and t_2 as before. However, when both faults are present within the system the dispatch interval is reduced to STD. Thus, as fault B occurs the STD interval ending at t_3 is initiated, rather than the one ending at t_2. Upon reaching t_3 three maintenance strategies exist. These are:

- Repair both faults, A and B, allowing unlimited dispatch of the aircraft,
- Repair fault A only, allowing dispatch until t_2, at which point fault B must be repaired,
- Repair fault B only, allowing dispatch until t_1, at which point fault A must be repaired.

When faults combine in this manner to reduce the dispatch interval it is possible for the ordering of the faults to also play a part. It may be the case that the dispatch interval would be reduced when either A was followed by B or B was followed by A. However, another possibility is that the dispatch interval may only be reduced if A is followed by B but not if B is followed by A.

The situations occurring above may also arise when PIR maintenance is being used to maintain the FADEC system. However, the reduction or otherwise of the dispatch intervals can be more complex, since the exact time of occurrence of the faults is not known. As an example of this increased complexity consider Figure 5, which shows the occurrence of two faults A and B. Each of these faults has an associated LTD interval and LTD faults are to be maintained using PIR. In combination the faults A and B initiate a STD interval. In the figure I_1 and I_2 represent two consecutive PIR inspections. At inspection I_2 faults A and B are discovered and assumed to have occurred at the midpoint of the two inspections, t_1. A LTD interval initiated at this time allows dispatch of the aircraft for a time T after inspection I_2. However, if the simultaneous existence of faults A and B causes the initiation of a STD interval ending at t_3 the situation is complicated somewhat. Upon reaching the maintenance deadline at t_3 faults A and B, fault A alone or fault B alone could be repaired. If A and B are both repaired the aircraft may be dispatched indefinitely. If just fault A or fault B is repaired the aircraft may then be dispatched until t_2 when the remaining fault must be repaired.

These examples of situations that may arise when

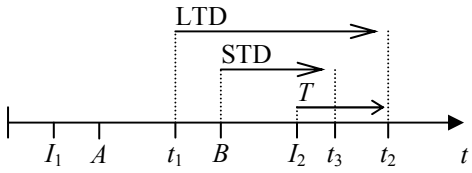

Figure 5. Faults Acting in Combination – PIR

implementing TLD to FADEC systems by no means cover all possibilities. They merely highlight some of the many cases that must be considered when attempting to model TLD.

3. *MODELING TLD*

Before applying TLD to aircraft it is important to be sure that the aircraft will still conform to the levels of safety desired of it. The first step in demonstrating this conformity is to construct a mathematical model of the system in order to predict its behavior when TLD is used. In [1] and [3] two of the commonly-used methods of TLD analysis are presented – a fault tree-based approach and a Markov modeling approach. These approaches are demonstrated here for the simple system shown in Figure 6. Monte Carlo simulation is then applied to the same system. The system is that given as an example in [1] and consists of two units, *U*1 and *U*2. These have failure rates per hour of $\lambda_{U1} = 0.0002$ and $\lambda_{U2} = 0.0001$ respectively.

3.1 *Time-Weighted Average (TWA) Fault Tree Approach*

In this method the overall average failure rate of the system is obtained by adding the failure rates of the HMC faults, λ_{HMC}, and the uncovered faults, λ_{UC}, to a time-weighted average (TWA) of the failure rates of the system from each of its dispatchable configurations, i.e.

$$\lambda_{\mathrm{TWA}} = \lambda_{\mathrm{HMC}} + \lambda_{\mathrm{UC}} + t_{\mathrm{FU}}\lambda_{\mathrm{FU,L}} + t_{\mathrm{STD}}\lambda_{\mathrm{STD,L}} + t_{\mathrm{LTD}}\lambda_{\mathrm{LTD,L}}, \quad (1)$$

where λ_{TWA} is the TWA failure rate of the system. t_{FU}, t_{STD} and t_{LTD} are respectively the fractions of time spent in the full-up, STD and LTD dispatchable system configurations. $\lambda_{\mathrm{FU,L}}$ is the LOTC rate of the system from the FU state to LOTC. $\lambda_{\mathrm{STD,L}}$ and $\lambda_{\mathrm{LTD,L}}$ are the average LOTC rates with STD and LTD faults. If the system has n dispatchable configurations, let state $i = 1$ represent the full-up configuration (i.e. the state with no failed components). States $i = 2,\ldots m$ and $i = m + 1,\ldots,n$ will represent the STD and LTD dispatchable system configurations respectively. If $\lambda_{i,\mathrm{L}}$ is the failure rate to LOTC for the i^{th} configuration it may be calculated as follows. The failure probability (of LOTC) for each state is divided by a suitable time period, such as the average flight time, to obtain a probability per flight hour. This is then equated to the average failure rate to LOTC over the time interval [2]. Thus

$$\lambda_{i,\mathrm{L}} = \frac{Q_{i,\mathrm{L}}}{t_{\mathrm{flt}}}, \quad (2)$$

where $Q_{i,\mathrm{L}}$ is the failure probability (of LOTC) for state i and t_{flt} is the average flight time. Define T_{STD} and T_{LTD} as the lengths of time spent in the STD and LTD dispatchable system states before repair, i.e. the STD and LTD dispatch intervals. If λ_i is the failure rate *into* a failed dispatchable system state then the fractions of time spent in the STD and LTD dispatchable system configurations may be approximated as follows (see[3]):

$$t_{\mathrm{STD}} = \sum_{i=1}^{m} \lambda_i T_{\mathrm{STD}} \text{ and } t_{\mathrm{LTD}} = \sum_{i=m+1}^{n} \lambda_i T_{\mathrm{LTD}}. \quad (3)$$

The fraction of time spent in the full-up state, t_{FU}, is determined using the fact that the fraction of time spent in the failed states added to the fraction of time in full-up state will be unity. Therefore once the fractions of time spent in all the failed states is known, t_{FU} may be calculated as follows:

$$t_{\mathrm{FU}} = 1 - t_{\mathrm{STD}} - t_{\mathrm{LTD}}. \quad (4)$$

The average LOTC rates with STD and LTD faults are defined in [3] as:

$$\lambda_{\mathrm{STD,L}} = \frac{\sum_{i=1}^{m} \lambda_i \lambda_{i,\mathrm{L}}}{\sum_{i=1}^{m} \lambda_i} \text{ and } \lambda_{\mathrm{LTD,L}} = \frac{\sum_{i=m+1}^{n} \lambda_i \lambda_{i,\mathrm{L}}}{\sum_{i=m+1}^{n} \lambda_i} \quad (5)$$

The dual unit system shown in Figure 6 has three dispatchable configurations, numbered states 1 to 3 as follows:

1. *U*1 and *U*2 work (Full-up),
2. *U*1 is failed, *U*2 works (STD),
3. *U*1 works, *U*2 is failed (LTD).

If q_{U1} and q_{U2} represent the probabilities of failure of *U*1 and *U*2 then, substituting these into equation (2), we get:

$$\lambda_{1,\mathrm{L}} = \frac{q_{U1}q_{U2}}{t_{\mathrm{flt}}}, \lambda_{2,\mathrm{L}} = \frac{q_{U2}}{t_{\mathrm{flt}}}, \lambda_{3,\mathrm{L}} = \frac{q_{U1}}{t_{\mathrm{flt}}}. \quad (6)$$

Substituting these into equation (3) we obtain the fractions of time spent in the STD and LTD dispatchable system configurations:

$$t_{\mathrm{STD}} = \frac{q_{U2}}{t_{\mathrm{flt}}} T_{\mathrm{STD}}, t_{\mathrm{LTD}} = \frac{q_{U1}}{t_{\mathrm{flt}}} T_{\mathrm{LTD}}, \quad (7)$$

which may then be substituted into (4) to give the fraction of time spent in the full-up state:

$$t_{\mathrm{FU}} = 1 - \frac{q_{U2}}{t_{\mathrm{flt}}} T_{\mathrm{STD}} - \frac{q_{U1}}{t_{\mathrm{flt}}} T_{\mathrm{LTD}}. \quad (8)$$

Substituting (6), (7) and (8) into (1) gives λ_{TWA} for this dual unit system. If the failure probabilities q_{Ui} are given by:

$$q_{Ui} = 1 - e^{-\lambda_{Ui} t_{\mathrm{flt}}}, \quad (9)$$

then λ_{TWA} can be calculated for different values of T_{STD} and T_{LTD}, which are the dispatch intervals for *U*1 and *U*2 respectively. The flight time, t_{flt}, was assumed to be 5 hours.

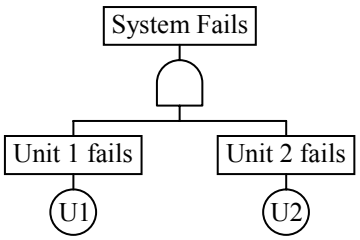

Figure 6. A Dual Unit System

3.2 *Single Fault State Markov Approach*

Like the fault tree approach, this technique has several

attractive features [1]. For instance, Markov modeling makes direct use of failure and repair rates, negating the need to equate the failure rates to probability/flight hour, as is the case with the fault tree approach. The main drawback with Markov analysis is the potentially huge number of system states that may be present within the model [4]. For this reason [3] considers failures that lead to one final failed state representing LOTC. This failed state is absorbing, since once the system is in this state no transition may occur to any other state. However, in [3] an artificial feedback loop, a "simulated repair", is introduced that takes the system from the final failed state back to the full-up state with no components failed. It is argued that a steady-state solution for the average failure rate of the system is required but that without a feedback loop the steady-state probability of the system being failed will always approach a value of 1. In [3] this simulated repair rate is set to unity, for simplicity. This choice is arbitrary, made since, if a LOTC event occurs for an engine, the control must be repaired before the next flight takes place. A repair interval of one hour is deemed suitable. This method also differs from a conventional Markov technique in that it involves only lower order fault states, commonly only single-fault states, although dual fault states are included if important for the analysis. The Markov model obtained using this technique is like that in Figure 7. The transition rates from the full-up state to the STD and LTD fault states are λ_{STD} and λ_{LTD} and the corresponding repair rates are ν_{STD} and ν_{LTD}. In [3] λ_{STD} and λ_{LTD} are approximated by the sums of the failure rates of all of the STD and LTD type faults respectively. ν_{STD} and ν_{LTD} are given by the reciprocal of the dispatch intervals, T_{STD} and T_{LTD}. The failure rates from the STD and LTD fault states are given by $\lambda_{STD,L}$ and $\lambda_{LTD,L}$ and the simulated repair is given by ν_{FB}. The Markov model leads to a system of 4 linear differential equations, given by:

$$\dot{\underline{Q}} = \underline{Q}A, \tag{10}$$

where A is the transition rate matrix,

$$A = \begin{bmatrix} -(\lambda_{STD}+\lambda_{LTD}) & \lambda_{STD} & \lambda_{LTD} & 0 \\ \nu_{STD} & -(\nu_{STD}+\lambda_{STD,L}) & 0 & \lambda_{STD,L} \\ \nu_{LTD} & 0 & -(\nu_{LTD}+\lambda_{LTD,L}) & \lambda_{LTD,L} \\ \nu_{FB} & 0 & 0 & -\nu_{FB} \end{bmatrix} \tag{11}$$

and

$$\underline{Q} = [Q_{FU}, Q_{STD}, Q_{LTD}, Q_{LOTC}], \tag{12}$$

where Q_{FU}, Q_{STD}, Q_{LTD} and Q_{LOTC} are the probabilities of the system being in the full-up, STD, LTD and LOTC states respectively. At steady state the derivatives of these probabilities will be zero, i.e.

$$\underline{Q}A = \underline{0}, \tag{13}$$

and thus a system of 4 linear equations is obtained. This system of equations is dependent. In order to obtain a system of independent equations one of the equations is replaced by the condition that the sum of the probabilities of being in each state is unity, i.e.

$$Q_{FU} + Q_{STD} + Q_{LTD} + Q_{LOTC} = 1. \tag{14}$$

Column 1 of A is arbitrarily chosen to be replaced by (14), giving a system of equations that is solved to find $\underline{Q}$ at steady state. In order to find the LOTC rate for the system the

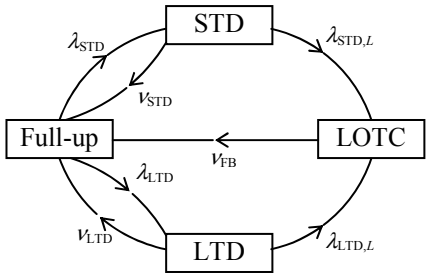

Figure 7. Single Fault State Markov Diagram.

average transition rate *into* the LOTC state is considered [3]. This LOTC rate, obtained from the single fault state Markov model is:

$$\lambda_{Mkv} = \frac{\text{Probability flow into LOTC state}}{1 - \text{Probability of being in LOTC state}}, \tag{15}$$

At this point faults that are required to be modeled as leading directly to the LOTC state, i.e. HMC faults or uncovered electronic faults, are added. Since these faults could lead to LOTC from any non-LOTC state the sum of their failure rates is multiplied by the sum of the probabilities of being in all the states except the LOTC state [3]. Thus (15) becomes:

$$\lambda_{Mkv} = \frac{(Q_{FU}+Q_{STD}+Q_{LTD})(\lambda_{HMC}+\lambda_{UC}) + Q_{STD}\lambda_{STD,L} + Q_{LTD}\lambda_{LTD,L}}{1-Q_{LOTC}}. \tag{16}$$

When modeling the dual unit system shown in Figure 6 the failure rates for the single fault state Markov model may be calculated as they were for the TWA model.

Markov models of TLD all inherently model the MEL maintenance strategy. This is because as soon as a component of the system fails the system will make a transition to a different state and thus the failure time of the component will be known. If PIR is to be used as a maintenance approach the maximum allowed dispatch time calculated using a Markov approach is doubled in order to calculate the maximum periodic inspection interval.

3.3 *Conventional Markov Approach to Single Fault State Model*

Note that the LOTC rate obtained from the single fault state Markov model, λ_{Mkv}, is dependent on the value of the feedback rate, ν_{FB}, and independent of the initial conditions of the system. Andrews and Moss [4] detail a method of finding the asymptotic failure rate of a system with absorbing final failed states. This may be applied to the Markov model described in the previous section. In this case there is no need to include a simulated repair from the final fully-failed state, i.e. the feedback rate, ν_{FB}. Thus the transition rate matrix is:

$$A = \begin{bmatrix} -(\lambda_{STD}+\lambda_{LTD}) & \lambda_{STD} & \lambda_{LTD} & 0 \\ \nu_{STD} & -(\nu_{STD}+\lambda_{STD,L}) & 0 & \lambda_{STD,L} \\ \nu_{LTD} & 0 & -(\nu_{LTD}+\lambda_{LTD,L}) & \lambda_{LTD,L} \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{17}$$

The reduced transition rate matrix, A_m, is obtained by truncating A by deleting entries for the absorbing states. Thus the final row and column of (17) is deleted to get A_m. The asymptotic failure rate, λ_{ASY}, is then given by:

$$\lambda_{ASY} = \frac{\left|A_m\right|}{\begin{vmatrix} 0 & Q_{FU}(0) & Q_{STD}(0) & Q_{LTD}(0) \\ 1 & a_{1,1} & a_{1,2} & a_{1,3} \\ 1 & a_{2,1} & a_{2,2} & a_{2,3} \\ 1 & a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}} \quad (18)$$

where the element of the reduced transition rate matrix in the i^{th} row and j^{th} column is defined as $a_{i,j}$ and $Q_{FU}(0)$, $Q_{STD}(0)$ and $Q_{LTD}(0)$ are the initial probabilities of being in the FU, STD and LTD system states. Therefore, note that in this case the solution is dependent on the initial conditions of the system.

3.4 *Monte Carlo Simulation Method*

Performing a Monte Carlo simulation (MCS) involves constructing and using a computer model of the system under investigation. This model is based on a structured, logical system representation and contains a set of rules that describe the response of the system to events that occur to it during its lifetime [4]. These events may be component repairs, failures or sequences of failures or, in this case, events that will lead to the implementation of TLD and its subsequent maintenance deadlines. In fact, any event may be added to the model subject to the complexity of the software used. MCS requires the generation of a uniform set of random numbers. These random numbers are then used to generate times of component failures by using the relevant failure distribution associated with each component. In the simulation code constructed during the course of this work the numbers generated are, in fact, pseudo-random. The system simulation may then be run many times, making a note after each simulation of any parameters of interest, and continuing the simulations until the required tolerance is reached for these parameters. In the work presented here the parameter of interest that had to be obtained from the system was its failure rate. Each simulation is carried out until a suitable point in time, whether this be the lifetime of the system or the time at which the system fails. The algorithm for the main module of the simulation program used in this work is given in Figure 8.

When modeling a system on which TLD will be applied the correct scheduling of all occurring events is of great importance. In the MCS code used here the component failure times are initially generated and added to an array that holds a reference to the component, along with the time that its failure will occur. A reference is also kept of the order of all the events in the schedule and this is updated as events are removed from, or added to, the schedule.

As component failures occur in the simulation a list of TLD criteria is checked to see if the failure of this component will initiate, either on its own or in combination with other component failures, the implementation of a TLD deadline. If this is the case the deadline itself is then added to the schedule along with its time of occurrence, which varies according to the dispatch category for that particular failure or combination of failures.

In each simulation loop the first event chronologically is removed from the schedule and the simulation time is advanced to time of this event. If this time exceeds the maximum lifetime of the system the simulation ends immediately. Otherwise, if the event is a component failure, the status of the system is updated and if the system fails the simulation ends. If the event is a maintenance deadline the appropriate repairs are carried out to components according to the maintenance strategies being applied to the system. In the case of the system being modeled here this simply means repairing the unit that failed to cause the maintenance deadline. Finally, if the event is a periodic inspection, a maintenance deadline will be added to the schedule at the appropriate point in time.

```
read system logic, component failure and repair
     distributions and TLD combinations from file
input TLD options
set max_sim_time
total_sim_time = 0, total_fail = 0, failure_rate = 0
while (failure rate has converged)
{
     marker for simulation failure initialized: flag = 0
     initial component failures added to empty schedule
     while (current_sim_ time ≤ max_sim_ time)
     {
          current_sim_time = time of 1st event in schedule
          remove 1st event from schedule
          if (1st event is a component failure)
          {
               update the status of the system
               if (system fails due to this component failure)
               {
                    simulation failed: flag = 1
                    end this simulation
               }
               if (TLD interval initiated due to this failure)
               {
                    add maintenance deadlines to schedule
               }
          else if (1st event is a maintenance deadline)
          {
               implement repairs according to maintenance
                    strategy
          }
          else if (1st event is a periodic inspection)
          {
               add maintenance deadline to schedule
          }
     }
     total_sim_time = total_sim_time + current_sim_time
     total_fail = total_fail + flag
     failure_rate = total_fail / total_sim_time
     check for convergence of failure rate
}
```

Figure 8. The Algorithm for the Main Module of the MCS.

In the MCS code a number of other assumptions are made. These are:

- The maximum lifetime of the system is set to be

200000 flight hours. This corresponds to a lifetime of about 37 years for a system used for 15 hours of flight per day, or 55 years for a system used for 10 hours per day.

o The length of a flight is 5 hours. This was chosen since this was used in the example in [1] when a flight length is needed for the TWA modeling approach.

o Maintenance operations and inspections cannot occur mid-flight. Thus, for any events of this type whose occurrence time is calculated to occur in flight, the time of the event is moved to the beginning of that flight. This is a conservative approach to this problem.

It should be noted that, despite the fact that they have been used in order to model this particular system, these assumptions may be easily changed within the MCS code, if necessary. The code may also be easily applied to other systems. This is because the system upon which the simulation is to be implemented is supplied to the code in a representation of the form of its fault tree. Other system-specific information supplied to the code is the failure distribution of each component, along with its associated parameters.

The failure rate of the system was actually calculated after every 1000 simulations. Results were obtained to an accuracy of 2 decimal places (for a failure rate given in units of number of failures per 10^6 flt. hrs.). If the failure rate matched over 10 consecutive calculations convergence was assumed.

4. *RESULTS*

Results were obtained using each of the above modeling approaches for differing intervals of dispatch for each unit in the dual unit example. The dispatch interval for U1 (STD) is represented as D1 and the dispatch interval for U2 (LTD) as D2. The MCS code was used to model all possible maintenance strategies for the dual unit system, with U1 and U2 being maintained using MEL and/or PIR. The PIR maintenance strategy was simulated with differing inspection intervals, incrementally from 0.25 to 2 times the length of the dispatch interval.

Results are shown in Figure 9 for a value of D1=100 flt. hrs. as was chosen in [1]. Presented in this way it can be seen that the results obtained from all of the methods are similar. The results obtained using the TWA approach give an overestimation of the failure rate in comparison to the other approaches, and each of the MCS models gives similar results to the Markov model, which is acknowledged to be the more accurate of the two approaches presented in [1] and [3]. Figure 10 shows the same results presented as a percentage difference from the results of the single fault state Markov approach. The TWA results grow from 7.1% above those of the single fault state Markov to 16.4% as D2 increases from 100 to 500 flt. hrs. All of the simulation results lie within 4% of the single fault state Markov results for D1 = 100 flt. hrs. As D1 increases from 100 to 500 flt. hrs. the simulation results remain close to the single fault state Markov results. However, as D1 rises the simulation results become progressively larger in comparison to the single fault state Markov results. Indeed, when D1 = 500 flt. hrs. the results from all of the simulations are greater than the results single

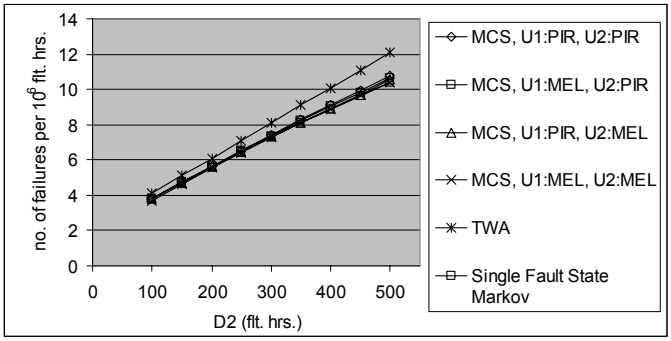

Figure 9. Comparison of Methods – D1=100 flt. hrs.

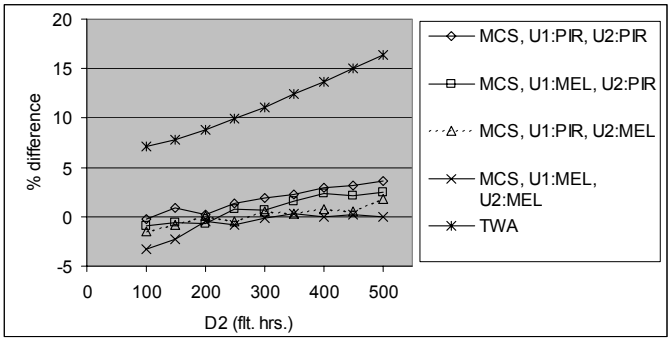

Figure 10. Percentage Difference from Single Fault State Markov – D1=100 flt. hrs.

faults state model, by as much as 5.95%. A trend that is also observed from the simulation results is that, for the most part, the system failure rate is observed to be higher for the case where both units are maintained using PIR than when one is repaired using PIR and one using MEL. The system failure rates when both units are maintained using MEL is the lowest obtained from all of the maintenance strategies and tend to lie closest to the single fault state Markov results. These results are as would be expected for this simple system. It should be noted that, for this simple dual unit system, all of the modeling approaches bar TWA give a similar allowable dispatch time for the remaining unit, given a dispatch time for one of the units, assuming that a failure rate of 10 failures per 10^6 flt. hrs. must not be exceeded.

Note that the results obtained for the single fault state Markov model with an artificial feedback loop are, for this system, very close to those achieved by using the conventional Markov approach to modeling the single fault state model with initial condition that the system starts in the full-up state, i.e. both units work initially.

5. *CONCLUSIONS*

Each of the methods applied to the dual unit system brings with it both advantages and disadvantages, some of the main examples of which are shown in Table 1. The MCS method proves to be a match for existing techniques for the simple dual unit system considered. However, the slight differences in system failure rate observed between the MCS and the single fault state Markov could grow larger as the

Method	*Advantages*	*Disadvantages*
TWA fault tree	Clear auditable representation of system failure logic.	TLD introduces dependencies between the basic events, which are inappropriate for a conventional fault tree approach. Failure rates approximated from failure probabilities.
single fault state Markov/ conventional Markov	Overcome problems associated with dependencies in the system. Failure and repair rates are easily incorporated into the model.	Only the MEL maintenance strategy is modeled. Constant failure rates are required. Model grows exponentially and becomes increasingly difficult to audit as the number of system states increases (*conventional model*). Involves an approximation of the system, reducing the number of system states and ignoring many combinations of faults (*single fault state only*).
MCS	Dependencies, non-constant failure rates and (ordered) combinations of faults are easily dealt with. PIR and MEL maintenance are easily modeled, including different strategies for different dispatch categories, e.g. STD-MEL, LTD-PIR. Uses fault tree representation of the system, which brings the associated advantage of clarity of system failure logic representation. More information may be obtained from the model than with other methods – e.g. could identify faults with inappropriate dispatch intervals.	Initial generation of code may be time-consuming – however, the code can be used for many systems. Extra CPU time required to run many simulations – however, in comparison to the time taken designing a new aircraft and gaining certification this will be negligible.

Table 1. Advantages and Disadvantages of the Different Modeling Techniques.

system being modeled becomes more complex. Preliminary work to investigate this theory, in which a slightly more complex system is modeled, suggests the difference between the techniques is greater than for the dual unit system.

REFERENCES

1. H. Larsen, G. Horan, "Time-Limited Dispatch: An Interactive Training and Self-Study Course.", *Keybridge Technologies*, *Inc*., 2002.
2. "FAA Memorandum: Policy for Time-Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems", June 29 2001, Policy No. ANE-1993-33.28TLD-R1.
3. "Guidelines for Time-Limited-Dispatch (TLD) Analysis for Electronic Engine Control Systems", *SAE ARP 5107*, SAE International, 1997.
4. J. D. Andrews, T. R. Moss, *Reliability and Risk Assessment*, 2nd Edition, London, Professional Engineering Publishing, 2002.

BIOGRAPHIES

Darren R. Prescott
Department of Aeronautical and Automotive Engineering,
Loughborough University,
Loughborough,
Leicestershire, LE11 3TU, UK

e-mail: D.R.Prescott@lboro.ac.uk

Darren Prescott is currently studying for a doctorate at Loughborough University, having previously graduated with a first class honors degree in Mathematics and gaining a masters degree with distinction in Industrial Mathematical Modeling. His current research studies are undertaken as part of the Risk and Reliability group in the Aeronautical and Automotive Engineering department of Loughborough University.

John D. Andrews
Department of Aeronautical and Automotive Engineering,
Loughborough University,
Loughborough,
Leicestershire, LE11 3TU, UK

e-mail: J.D.Andrews@lboro.ac.uk

John Andrews is Professor of Systems Reliability in the Department of Aeronautical and Automotive Engineering. He joined Loughborough University in 1989 having previously gained nine years industrial research experience with British Gas. His current research interests concern the assessment of the safety and risk of potentially hazardous industrial activities. This research has been heavily supported by industrial funding. Over recent years grants have been secured from BAE Systems, MOD, Rolls-Royce, ExxonMobil and Bechtel. Professor Andrews has numerous journal/conference publications along with a jointly authored book 'Reliability and Risk Assessment' which is now in its second edition.

ACKNOWLEDGEMENT

The authors would like to acknowledge Phil Wilkinson for his involvement and support during the course of this work.