The safe dispatch of aircraft with known faults

International Journal of Performability Engineering Vol. 4, No. 2, July, 2008, pp. 243-253.

Printed in India

The Safe Dispatch of Aircraft with Known Faults

D. R. PRESCOTT and J. D. ANDREWS*

Department of Aeronautical and Automotive Engineering, Loughborough University, LE11 3TU, UK

(Received on December 07, 2006)

Abstract: Time-limited dispatch (TLD) allows the dispatch of aircraft with faults present in their control systems for limited time periods. In order for TLD to be applied to an aircraft system it is first necessary to demonstrate that the relevant safety and certification requirements are being met by modelling the system in question. To do this existing modelling techniques use variations of fault tree analysis and Markov analysis with various simplifying assumptions, made to assist in the analytical process. Monte Carlo simulation is presented here as an alternative method of analysis, which can deal well with the potential difficulties that may present themselves when modelling TLD, such as the complex architectures of aircraft systems and dependencies that are introduced when applying TLD. In this paper a simple example system is introduced and the application of TLD to it is modelled using the existing variation of Markov analysis and a Monte Carlo simulation technique. The results obtained using the different techniques are seen to differ and a number of reasons are suggested for this difference.

Keywords: *Time-Limited Dispatch, TLD, Monte Carlo Simulation*

1. Introduction

Time-limited dispatch (TLD) was first used after the introduction of Full Authority Digital Electronic Control (FADEC) systems to commercial aircraft in the mid-1980s. Upon their introduction FADEC systems assumed the role that had previously been undertaken by hydromechanical control (HMC) systems, namely that of governing engine thrust from the beginning of fuel metering to the point of fuel shutoff. It was to be the first time that a HMC system would be unavailable to pilots in the event of electronic system failure [1].

FADEC systems are designed to incorporate redundancy. Critical loops and functions have either dual systems or redundant elements. With this in mind and also the high reliability of the electronic components that make up the FADEC systems one would expect that there would be an increase in control system integrity. This could also be assumed to lead to a reduction in the number of delays and cancellations of aircraft due to control system failures. However, because the dispatch criteria applied to the aircraft were essentially those that were applied to aircraft with HMC systems the frequency of flight delays and cancellations increased [2,3]. The dispatch guidelines were too conservative and did not take into account the high reliability of individual system components and the redundancies contained within the FADEC systems. Accounting for these qualities, dispatch would be allowed with faults present in the FADECs.

* Corresponding author's email: J.D.Andrews@lboro.ac.uk

The necessary airworthiness requirements would be met and also aircraft operators and passengers would benefit from the reduction in unscheduled maintenance operations. This new approach to aircraft dispatch, allowing aircraft dispatch with faults, is called time-limited dispatch (TLD).

TLD allows aircraft dispatch with known faults present within the engine control system for a limited period of time only. When it is implemented a certain level of system reliability must be met. This level was set to match that required of the HMC systems that were used before the advent of FADEC systems and specifies a maximum limit of 10 failures per 10^6 flight hours (flt. hrs.) for the *average* loss of thrust control (LOTC) rate of the system [2]. The regulations also specify that other restrictions must apply to the system LOTC rate. These relate to the *instantaneous* LOTC rates when operating with faults present within the system. For a fault to be dispatchable the instantaneous LOTC rate must be less than 100 failures per 10^6 flight hours whilst operating with that fault. The aircraft may be dispatched for differing periods of time according to the significance of faults present within the system. Depending on the value of the instantaneous LOTC rate for a fault the fault may be classified as falling into one of four dispatch categories (FAA Memo, 2001). These are:

- Do Not Dispatch - DND
- Short Time Dispatch - STD
- Long Time Dispatch - LTD
- Manufacturer/Operator Defined Dispatch - MDD

Each of these is dependent upon the likelihood of further faults causing system failure given the presence of the dispatchable fault. DND faults prohibit dispatch of the aircraft and must be addressed immediately (a LOTC rate of greater than 100 failures per 10^6 flt. hrs. would instigate this). The instantaneous LOTC rate for STD faults must lie between 75 and 100 failures per 10^6 flt. hrs. and the rate for LTD faults must be less than 75 events per 10^6 flt. hrs. The final dispatch category, MDD, is reserved for faults that don't fall into any of the other categories or do not affect the LOTC rate of the system.

1.1 Maintenance Strategies

Two different maintenance strategies may be adopted when applying TLD to a system. These strategies are minimum equipment list (MEL) maintenance and periodic inspection and repair (PIR) maintenance. It does not matter to which of the fault categories these are applied to but it is common for STD faults to be addressed using MEL maintenance and LTD faults to be addressed using PIR maintenance.

MEL maintenance is a time-since-fault repair strategy and, if applied, the exact time of occurrence of the fault must be known. At this time a 'countdown' of the appropriate dispatch time is started and once this countdown reaches zero the fault must have been repaired before further dispatch of the aircraft is allowed. This process is illustrated in Figure 1, where a fault occurs at time t_1. As the fault occurs a dispatch interval is initiated. This dispatch interval ends at time t_2 and once time t_2 is reached the fault must be cleared from the system in order to allow further dispatch of the aircraft.

PIR maintenance differs from MEL maintenance in that the exact time of the fault need not be known. The system is checked for faults at regular intervals and when a fault is discovered it is assumed to have occurred at the midpoint of consecutive inspections. This is considered reasonable since the fault will, on average, occur at this time if one assumes that the failure rates for faults are constant with time and that the periodic inspection interval is less than the mean time between failures (MTBF) of the sum of the failure rates in that

category. Once the fault is assumed to have occurred at the midpoint of inspections the dispatch interval is assumed begins at this point and the allowable period of dispatch after the current inspection is calculated. This means that the inspection interval for a fault category cannot exceed twice the dispatch interval for that category. The PIR maintenance process is illustrated in Figure 2. On this diagram two periodic inspections are shown, I_1 and I_2. Here a fault occurs at time t_f but in this case the exact time of the fault is not known so it is only discovered at I_2. It is then assumed to have occurred at the midpoint of the two consecutive inspections, t_1, and a dispatch interval is assumed to have started at this point. This then allows dispatch for a time T after I_2 until time t_2 when the fault must be cleared from the system in order for further dispatch to be allowed.

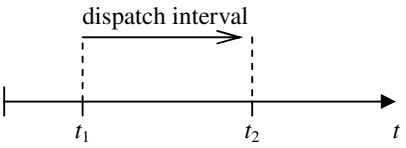

Fig. 1: MEL Maintenance

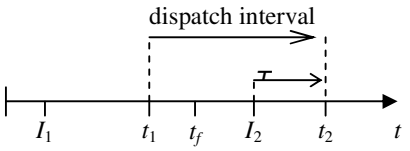

Fig. 2: PIR Maintenance

If PIR maintenance were used to maintain both STD and LTD faults, situations could arise where a fault of one category were discovered at inspections for faults of another category. In situations such as these it is possible to treat the fault as though it was discovered at the next inspection for its own category. To illustrate this, consider a LTD fault discovered at an inspection for STD faults. In this case the LTD fault could be treated as though found at the next inspection for LTD faults.

1.2 Multiple Faults

Despite the relatively high reliability of FADEC systems it is still possible that more than one fault can be present within the system at any one time. In such situations the faults may be cleared from the system in a number of ways, each of which would affect the exposure of the system to the faults. A number of examples are outlined below. These are by no means exhaustive but serve to provide an indication of the complexities that are potentially involved when one attempts to model the application of TLD to a system. The examples shown are for the MEL maintenance process. When one attempts to model PIR maintenance, a combination of MEL and PIR maintenance, or even the presence of more faults, the maintenance options may become more complex.

Figure 3 shows the occurrence of two faults, *A* and *B*, addressed using MEL maintenance, which have dispatch intervals ending at t_1 and t_2 respectively. At t_1 a number of options are possible. Fault *A* must be cleared from the system in order to allow further dispatch. Also at this time fault *B* could be allowed to remain in the system, thus allowing dispatch until time t_2 when it must be repaired. A second option is available. This would be to opportunistically repair fault *B* also, allowing unlimited dispatch of the aircraft from time t_1.

Figure 4 also shows the occurrence of two faults, *A* and *B*, addressed using MEL maintenance. If either were to occur in isolation the dispatch category applied would be LTD. However, the simultaneous presence of *A* and *B* in the system causes a reduction in the dispatch category to STD. As t_3 is reached repairs are required in order to allow further

dispatch of the aircraft. In this situation more options are possible. Clearly, both *A* and *B* could be cleared from the system allowing unlimited dispatch from t_3 or *A* alone could be repaired, allowing dispatch until t_2 when *B* must be repaired or *B* alone could be repaired, allowing dispatch until t_1 when *A* must be repaired for further dispatch to be possible. This

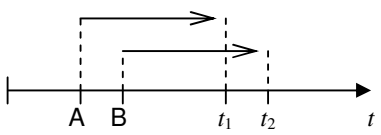

Fig. 3: Multiple Faults (MEL Maintenance)

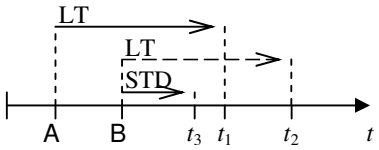

Fig. 4: The Combination of Multiple Faults (MEL Maintenance)

scenario could be complicated further still if the ordering of the faults *A* and *B* dictated whether or not the dispatch interval was reduced from LTD to STD. For example, *A* followed by *B* could lead to the scenario shown in Figure 4, but *B* followed by *A* might not lead to a reduction in the dispatch interval.

These examples serve to show some of the complexities involved when applying TLD to a system and maintaining that system. When modelling the application of TLD it is important that the model used can deal with such complexities, should they arise, in order to have reasonable confidence in the results gained.

2. Example System – Modelling TLD

Figure 5 shows a block diagram of a simple example system, which consists of two essentially identical channels, *X* and *Y*. Each channel performs two functions, F_1 and F_2, which, if either fails, will cause that channel to fail. For example, considering channel *X*, the function F_1 is performed by the components *A* and *B* in parallel and the function F_2 is performed by the components *C*, *D* and *E* according to the configuration shown. Note that there are dependencies between the channels, since components *B* and *E* appear in each of the channels. The corresponding fault tree for this system is given in Figure 6. Each of the components of the system is assumed to have an exponential failure time distribution and Table 1 shows the failure rates of each of these components.

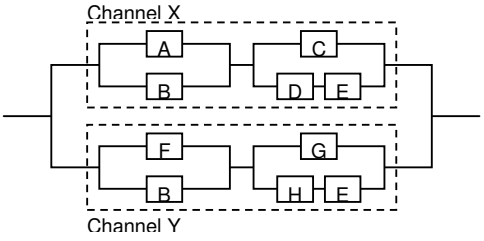

Fig. 5: Example System Block Diagram

Table 1: Component Failure Rates

Component/s	Failure rate (per hr)
A, *F*	5.0×10^{-5}
B	3.5×10^{-5}
C, *G*	7.5×10^{-5}
D, *H*	6.0×10^{-5}
E	4.0×10^{-5}

Before modelling the system the faults that will be considered dispatchable faults must be identified. In the examples studied in [4] and [5] the dispatchable faults all correspond to basic events in the fault tree representation of the LOTC top event. In this example intermediate events will be included in the dispatch criteria, along with some basic events. The reason for this choice is to try to include typical characteristics in the example that occur

in real systems. For real systems the fault tree would most likely be drawn down to component level for the FADEC system and its constituent functions. However, for the majority of these components it seems unlikely that they will be included explicitly in the dispatch criteria. It would seem more likely that combinations of basic events, represented by intermediate events in a fault tree, would correspond to faults that would be included in the dispatch criteria for a system. Thus, for this example, the basic events *A*, *B* and *F*, and the intermediate events F_2X (F_2X Fails) and F_2Y (F_2Y Fails) were chosen as the faults included in the dispatch criteria.

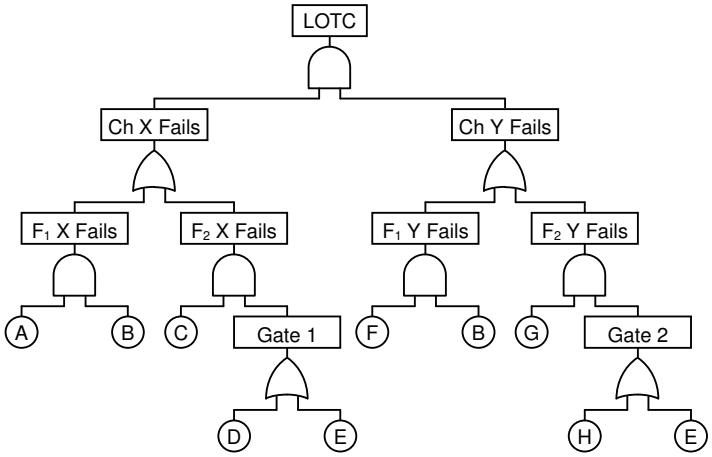

Fig. 6: Fault Tree of System Shown in Figure 5

There are two approaches recommended for the modelling of systems to which TLD is applied [3]. These are based on fault tree analysis (time-weighted average or TWA) and Markov analysis (reduced fault state Markov model). A third approach is proposed in this paper as being very well-suited to modelling the application of TLD to systems. This approach is Monte Carlo simulation (MCS). The following sections outline the application of two of these modelling techniques (reduced fault state Markov, in fact dual fault state Markov, and MCS) to the example system given above. The TWA approach is not used here since in previous work by the authors on small examples [4,5] results obtained proved to be in poor agreement with results obtained using the reduced fault state Markov and MCS approaches.

2.1 Dispatch Criteria

For both models, before modelling the application of TLD to the example system, a set of dispatch criteria must be decided. These dispatch criteria are a list of faults and fault combinations and the dispatch categories that will be associated with them. As described in the introduction, the dispatch categories are set according to the values of the instantaneous failure rates to LOTC. Although the code developed by the authors can be used to calculate the instantaneous failure rates to LOTC, and hence set the dispatch criteria, the work presented here uses the dispatch criteria obtained for the dual fault state Markov model. This was done in order to compare the dual fault state Markov and MCS approaches with as little variation between the ways the system was modelled as possible. Calculating the instantaneous failure rates to LOTC from the single and dual fault states is not a simple task, even for such a simple system. The decision was taken to use the method given in [1],

wherein the failure rates to LOTC from the fault states are approximated by the probability of LOTC for those fault states divided by the flight time. That is, the failure rates are approximated by a 'probability per flight hour.' However, finding the probability of failure from the different system fault states is not necessarily simple for a real, larger, more complex system. In the case of this example the relevant fault or combination of faults was assumed to be present in the system, the probability of that fault would be set to true and the system unavailability calculated. For example, if one wants to find the probability of system failure with fault *A* present then fault *A* is set to true in the fault tree shown in Figure 6. This gives the following Boolean representation of the system top event LOTC (where + represents Boolean OR and . represents Boolean AND):

$$\begin{aligned} LOTC_A &= [B + C.(D + E)][F.B + G.(H + E)] \\ &= B.F + B.G.H + B.E.G + C.D.G.H + C.E.G \end{aligned} \tag{1}$$

where $LOTC_A$ represents the LOTC of the system given that *A* is failed. If we use the rare event approximation the system unavailability given that *A* is failed, $Q_{SYS|A}$, is given by:

$$Q_{SYS|A} = q_B q_F + q_B q_G q_H + q_B q_E q_G + q_C q_D q_G q_H + q_C q_E q_G , \tag{2}$$

where q_i represents the probability of failure of component *i*. This is considered appropriate since this will be an upper bound for the system unavailability and as such will be conservative. Approximating these q_i's using the exponential distribution

$$q_i = 1 - \exp(-\lambda_i t), \tag{3}$$

where λ_i represents the failure rates given in Table 1, we can calculate failure rates to LOTC for each of the single and dual system faults. Therefore, in order to approximate the instantaneous failure rate to LOTC with *A* failed one would then substitute Eqn. 3 into Eqn. 2 and divide the resultant probability by the length of an average flight.

Note that a problem occurs when considering the faults F_2X and F_2Y since a number of different scenarios can cause these faults to occur and also that they have a common component in *E*. Thus, when calculating the failure probability with F_2X or F_2Y failed assume the worst-case scenario that *E* is failed. In this way if one, for example, considers the dual fault system state where *A* and F_2X are present in the system the Boolean representation of the system top event LOTC is:

$$LOTC_{A,F_2X} = B.F + G , \tag{4}$$

which leads to the rare event, upper bound, approximation:

$$Q_{SYS|A,F_2X} = q_B q_F + q_G . \tag{5}$$

Using the above technique gives the approximations for the instantaneous failure rates to LOTC from each of the single and dual system fault states, given to 3 significant figures in Table 2. A time of 10 hours was assumed for the average flight time. Also shown in Table 2 is the corresponding TLD category.

Table 2: Instantaneous LOTC Rates and Associated TLD Categories (Cat) for A Dual Fault State Markov Model. Note that LOTC Rates Shown are in Failures Per 106 Flt Hrs

	A	*B*	*F*	F_2X	F_2Y	*AB*	*AF*	AF_2X	AF_2Y	*BF*	BF_2X	BF_2Y	FF_2X	FF_2Y
LOTC	0.018	0.025	0.018	75	75	50	35	75	110	50	125	125	110	75
Cat	LTD	LTD	LTD	STD	STD	LTD	LTD	STD	DND	LTD	DND	DND	DND	STD

Note that there are four fault states whose instantaneous failure rates to LOTC are equal to 75 failures per 10^6 flight hours. This is exactly on the boundary between the STD and LTD categorisation. The conservative approach was taken to put these faults into the STD category. There are also four dual fault system states that have failure rates above 100 failures per 10^6 flight hours, leading to them being categorised as DND faults.

2.2 Dual Fault State Markov Model

The LOTC rates given in Table 2 mean that a dual fault state Markov model can be constructed that will have the form given in Figure 7. Note the feedback repair transition, with corresponding rate μ_{fbk}, which is included in the model to aid the calculation of a steady-state solution to the model [3]. Because of the way the LOTC rate is calculated the solution does not depend on this feedback transition rate. Note that the Markov model shown depicts only the failure transitions into single and dual fault states and the LOTC state. The failure rate to LOTC from the full-up state, $\lambda_{FU,L}$, is shown on the model, along with the artificial feedback rate, μ_{fbk}. Not shown on the model in order to retain the diagram's clarity are repair transitions from each of the single and dual fault states back to the full-up system state. The transitions from the full-up state to each of the single fault states are labelled on the model with the appropriate failure rate. Not labelled are the transitions from the single fault states to the dual fault states which will correspond to the occurrence of a further single fault within the system. For example, the transitions to dual

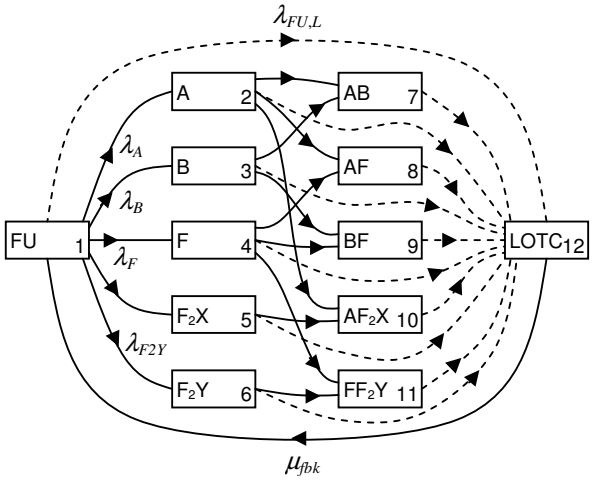

Fig. 7: Dual Fault State Markov Model Showing Only Failure Transitions

fault states from state 2 (single fault *A*) lead to states 7, 8 and 10 (dual faults *AB*, *AF* and AF_2X respectively). These transitions have corresponding rates λ_B, λ_F and λ_{F2X}. The final rates on the diagram lead from each of the single and dual fault states to the LOTC state and these correspond to the instantaneous failure rates to LOTC given in Table 2.

The current state of the Markov model thus requires three more failure rates to be calculated, these being $\lambda_{FU,L}$, λ_{F2X} and λ_{F2Y}. The first of these, $\lambda_{FU,L}$, can be calculated in a similar way to that used to calculate the instantaneous failure rates to LOTC for each of the dispatchable system states, that is to calculate the system unavailability and divide it by the average flight time to give a probability per flight hour. Again, the rare event approximation

is used in order to provide a conservative approximation and the value obtained is 3.13×10^{-10} failures per flight hour.

The final two failure rates into the single fault states with F_2X and F_2Y failed, λ_{F2X} and λ_{F2Y}, can be modelled using the same probability over flight time approximation. In each case we shall take the conservative approximation for calculating the failure probability of the fault by simply assuming that the failure of C (in the case of F_2X) or G (in the case of F_2Y) will cause the fault to occur. This yields identical rates for F_2X and F_2Y of 7.5×10^{-5} failures per hour. The Markov model produces state equation

$$\dot{\mathbf{Q}}(t) = \mathbf{Q}(t)\mathbf{A}\,, \tag{6}$$

where

$$\mathbf{A} = \begin{bmatrix}
-\Sigma_1 & \lambda_A & \lambda_B & \lambda_F & \lambda_{F_2X} & \lambda_{F_2Y} & 0 & 0 & 0 & 0 & 0 & \lambda_{FU,L} \\
\mu_A & -\Sigma_2 & 0 & 0 & 0 & 0 & \lambda_B & \lambda_F & 0 & \lambda_{F_2X} & 0 & \lambda_{2,L} \\
\mu_B & 0 & -\Sigma_3 & 0 & 0 & 0 & \lambda_A & 0 & \lambda_F & 0 & 0 & \lambda_{3,L} \\
\mu_F & 0 & 0 & -\Sigma_4 & 0 & 0 & 0 & \lambda_A & \lambda_B & 0 & \lambda_{F_2Y} & \lambda_{4,L} \\
\mu_{F_2X} & 0 & 0 & 0 & -\Sigma_5 & 0 & 0 & 0 & 0 & \lambda_A & 0 & \lambda_{5,L} \\
\mu_{F_2Y} & 0 & 0 & 0 & 0 & -\Sigma_6 & 0 & 0 & 0 & 0 & \lambda_F & \lambda_{6,L} \\
\mu_{AB} & 0 & 0 & 0 & 0 & 0 & -\Sigma_7 & 0 & 0 & 0 & 0 & \lambda_{7,L} \\
\mu_{AF} & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_8 & 0 & 0 & 0 & \lambda_{8,L} \\
\mu_{BF} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_9 & 0 & 0 & \lambda_{9,L} \\
\mu_{AF_2X} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_{10} & 0 & \lambda_{10,L} \\
\mu_{FF_2Y} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_{11} & \lambda_{11,L} \\
\mu_{fbk} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\mu_{fbk}
\end{bmatrix}, \tag{7}$$

and

$$\mathbf{Q}(t) = [Q_1(t), Q_2(t), \ldots, Q_{12}(t)], \tag{8}$$

where Σ_i is the sum of the other elements in the i^{th} row of the matrix, μ_j is the repair rate of fault j and $\lambda_{i,L}$ is the instantaneous failure rate to LOTC from state i. $Q_i(t)$ is the probability of the system being in state i at time t. At steady state these equations satisfy:

$$\mathbf{Q}(t)\mathbf{A} = \mathbf{0}\,. \tag{9}$$

Now, the dual fault state Markov LOTC rate [3] of the system is given by:

$$\lambda_{dual,LOTC} = \frac{\text{Probability flow into the LOTC state}}{1-\text{Probability of being in the LOTC state}} = \frac{\sum_{i=1}^{11} Q_i \lambda_{i,L}}{1-Q_{12}}\,. \tag{10}$$

In order to make the system of equations given in Eqn. 9 linearly independent we must use the constraint equation,

$$\sum_{i=1}^{12} Q_i = 1. \tag{11}$$

Substituting in Eqn. 10 yields, with some rearrangement:

$$\lambda_{dual,LOTC} = \frac{\lambda_{1,L} + \sum_{i=2}^{11} \frac{Q_i}{Q_1}\lambda_{i,L}}{1+\sum_{i=2}^{11} \frac{Q_i}{Q_1}}\,, \tag{12}$$

The equations represented by columns 2 to 11 of the transition rate matrix **A** are then used to obtain algebraic expressions for the ratios Q_i/Q_1, which are then substituted into Eqn. 12, along with all of the appropriate failure rates to give an expression for the dual fault state LOTC rate of the system. Setting the repair rates, μ_i, to be the reciprocal of the appropriate STD or LTD intervals allows the LOTC rate to be calculated for different STD and LTD intervals.

2.3 Monte Carlo Simulation Model

It is proposed in this paper that Monte Carlo simulation (MCS) is an approach that is very well-suited to modelling the application of TLD to systems. Intricacies introduced by different maintenance strategies or the occurrence and ordering of multiple faults are easily dealt with in a MCS approach. What follows is a summary of the MCS approach proposed. The computer code developed is described in more detail in two previous papers [4,5]. The code requires three basic inputs, these being;

1. A fault tree representation of the system to be modelled,
2. The failure time probability distributions and associated parameters for the basic events in the fault tree,
3. The dispatch criteria to be applied to the system.

Along with these it is possible to specify how maintenance will take place. The failure probability distributions are used to generate failure times for the basic events. These are added to a schedule, used to retain the ordering of faults. The code works by moving chronologically through the schedule, changing the status of the relevant basic events and using the fault tree structure to see how the system is affected. As faults occur the system dispatch criteria must be checked to see if a TLD deadline must be added to the system schedule. At TLD deadlines the relevant maintenance must be carried out according to the fault that initiated the deadline. The main challenges in constructing the computer code were in ensuring the correct ordering of fault occurrences and maintenance deadlines within the schedule, then clearing the correct faults from the system at maintenance deadlines. Many simulations are executed in order to achieve convergence of results. In order to calculate the average LOTC rate of the system the total number of system failures and the total modelled system operational lifetime must be stored.

For the example system considered here a MEL maintenance approach was applied to both STD and LTD faults, since this is the approach most closely represented in the dual fault state Markov model. A total operating lifetime for the system of 130000 flight hours was used along with a flight time of 10 hours (the same flight time as that used in the dual fault state Markov model). The repair strategy used at maintenance deadlines was to repair just the fault/fault combination that caused the deadline to be initiated in the first place. For example, if one considers Figure 4 and the STD maintenance deadline at t_3, both faults, A and B, would be repaired at this time and the option would not be taken to repair A or B individually. This is in line with the repair transitions included in the dual fault state Markov model, which lead from each of the single and dual fault states back to the full-up system state.

3. Results

The STD interval for the system was set at 200 flight hours and the system was modelled using both the dual fault state Markov model and the MCS code for LTD intervals varying from 500 to 2500 flight hours. LOTC rates from the MCS code were obtained after

convergence to at least 3 significant figures had been reached, with 1000000 simulations being performed before the results were checked. After this the LOTC rate was checked for convergence after every 50000 simulations and it was necessary for the obtained rate to be identical to 3 significant figures a total of three consecutive times for convergence to be assumed. The results obtained from these models are shown in Figure 8. Note that the system LOTC rate calculated using the MCS is generally higher than that calculated using

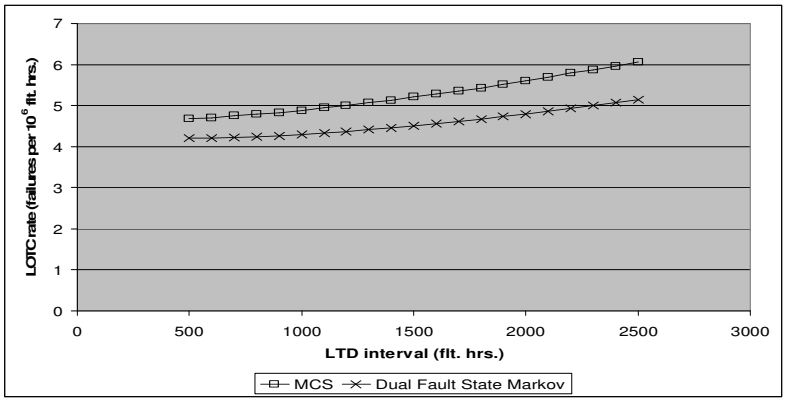

Fig. 8: A Comparison of the Results Obtained When Modelling the Example System Using the Dual Fault State Markov Model and the MCS Code

the dual fault state Markov model. The same trend was also observed for other lengths of STD interval. Note that if one wanted to set the dispatch intervals for this example, whilst ensuring that the system LOTC rate was to be below the maximum allowed of 10 failures per 10^6 flight hours, the MCS code could be expected to give the more conservative dispatch intervals since it would yield the maximum allowed LOTC rate for a lower LTD interval than that obtained for the reduced fault state Markov model.

4. Discussion/Conclusions

The motivation behind the choice of system used to demonstrate the method was to gain some insight into where problems could arise when modelling the application of TLD to real systems. Even for this small system, a problem that arises is the calculation of failure rates to be used in the dual fault state Markov model. The recommended method of approximating the failure rates by a failure probability divided by a flight time was simple to apply for this small example, upper bounds being used for the probabilities where appropriate. This should lead to some conservatism being incorporated into the dual fault state Markov model. However, in comparison to the MCS results the dual fault state Markov model seems to have produced low values for the system LOTC rate for this small example. Since there are no restrictions in the assumptions used in the MCS model and it does not use approximations this will produce the more accurate results.

References

[1]. Larsen, H. and Horan, G., *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 Control Systems*, Policy No. ANE-1993-

33.28TLD-R1., 2001.
[3]. SAE ARP5107 Rev A, *Guidelines for Time-Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems*, SAE International, 2005.
[4]. Prescott, D. R. and Andrews, J. D., *Aircraft Safety Modelling for Time-Limited Dispatch*, Annual Reliability and Maintainability Symposium 2005 Proceedings, 2005
[5]. Prescott D. R. and Andrews, J.D., *A Comparison of Modelling Approaches for the Time-Limited Dispatch of Aircraf*', Advances in Reliability Technology Symposium, 2005.

Darren Prescott is currently working as a Research Associate at Loughborough University and is in the process of completing his PhD studies, having previously graduated with a first class honours degree in Mathematics and gaining a masters degree with distinction in Industrial Mathematical Modelling. His current research is undertaken as part of the Risk and Reliability research group in the Aeronautical and Automotive Engineering department of Loughborough University.

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.