Session No. 7, Paper No. 17

Modelling Aircraft Maintenance Scheduling Using Petri Nets

Darren Prescott

Nottingham Transportation Engineering Centre, University of Nottingham,

Nottingham, NG7 2RD, UK

[Darren.Prescott@nottingham.ac.uk](mailto:Darren.Prescott@nottingham.ac.uk)

# Abstract

Time-Limited Dispatch (TLD) allows aircraft dispatch for limited periods of time with faults present in engine control systems. This means maintenance can be scheduled conveniently and service disruption can be minimised. This paper reviews the concept of TLD and briefly describes the features of an existing software-coded Monte Carlo (MC) simulation model before introducing a modular Petri net (PN) model which was developed to model the application of TLD to an example system. The PN provides a modelling framework for MC simulation. The example system has features typical of systems to which TLD is applied and is analysed using the PN model. Results are presented in the form of probability distributions and these are analysed in the context of the application of TLD to the system. The distributions exhibit particular characteristics, which are explained in the context of the example system and serve to validate the model. This validation, along with the clarity of the PN, achieved through its modular structure, leads to a modelling approach that is more transparent than the software-coded MC model for TLD.

**Keywords** – Time-Limited Dispatch, Petri nets, Monte Carlo simulation

# 1 Background

In the 1980s commercial aircraft were controlled by Full-Authority Digital Electronic Control (FADEC) systems for the first time. Upon their introduction, the FADEC systems replaced mechanical and hydromechanical control (HMC) systems and assumed the role of governing engine thrust from the start of fuel metering to the point of fuel shutoff. This was the first time that there was no HMC system available to pilots in the event of electronic system failure [1]. This was acceptable since the FADEC systems comprised inherently reliable electronic components and redundancies could be introduced without incurring the weight penalties that would result from incorporating redundancies in HMC systems.

It was expected that the introduction of these FADEC systems, with reliable components and dual channels for all critical functions, would lead to an improvement in system performance. However, there was an increase in the number of flight delays and cancellations [2,3]. This was due to the application of the dispatch criteria that had previously been applied to HMC systems, which were too restrictive since they did not take advantage of the FADEC system component reliability and redundancy. In order to utilise these features Time-Limited Dispatch (TLD) was developed.

# 2 Time-Limited Dispatch (TLD)

Time-Limited Dispatch (TLD) allows aircraft to be dispatched with faults in their FADEC systems for limited periods of time, after which the faults must be cleared before the aircraft can be dispatched further. This dispatch in the presence of faults makes it possible to schedule maintenance so that flight delays and cancellations are minimised, benefitting airlines, operators and passengers. In order to apply TLD a number of rules must be followed. These are described in the following sections.

## 2.1 Dispatch Criteria, Categories and Intervals

In practice, TLD requires a set of dispatch criteria to be specified. These dispatch criteria list all possible faults and fault combinations and assign them to one of four possible dispatch categories:

* No dispatch (ND)
* Short-time dispatch (ST)
* Long-time dispatch (LT)
* Manufacturer/operator-defined dispatch (MD)

Each of these dispatch categories has associated with it a dispatch interval, which dictates the maximum permissible time for aircraft dispatch in the presence of a particular category of fault. The dispatch categories are assigned to faults and fault combinations according to the likelihood of further faults causing system failure. The greater the likelihood of system failure, the more restrictive the applied dispatch category. Therefore, once defined, the dispatch criteria specify, for each fault, the maximum possible dispatch interval when dispatching the aircraft with that fault.

## 2.2 Certification Requirements

The aircraft industry is strictly regulated and the safety of aircraft to which TLD is applied must be demonstrated. The dispatch criteria applied to all possible faults must be such that fault dispatch categories, and their associated dispatch intervals, do not lead to an unacceptable likelihood of system failure. Since FADEC systems govern engine thrust, the system failure mode that is considered during FADEC certification for TLD is the Loss of Thrust Control (LOTC) rate. There are two requirements. Firstly, the *average* system LOTC rate must not exceed 10 failures per 106 flight hours (fh). This limit was specified since it was the level required of HMC systems prior to the introduction of FADEC systems. Secondly, the *instantaneous* LOTC rate, i.e. the failure rate when dispatching with faults present, must not exceed 100 failures per 106fh. The dispatch category for a fault is determined using the instantaneous LOTC rate as follows (*λi*,*L* represents the instantaneous LOTC rate from fault state *i*):

* LT: *λi*,*L* < 75 failures per 106fh,
* ST: 75 ≤ *λi*,*L* < 100 failures per 106fh,
* ND: *λi*,*L* ≥ 100 failures per 106fh.

There are no requirements for MD faults since this category is reserved for faults which do not affect the system LOTC rate.

## 2.3 Maintenance

Two types of maintenance are employed when TLD is applied: minimum equipment list (MEL) maintenance and periodic inspection and repair (PIR) maintenance. Although not always the case, MEL maintenance is usually applied to ST faults and PIR maintenance to LT faults [2].

2.3.1 MEL Maintenance

When faults are revealed, this time-since-fault maintenance approach is applied. Figure 1 shows an example where a fault occurs at time *t*1 and a dispatch interval is initiated. If the fault is not cleared as the dispatch interval ends at *t*2 then the aircraft cannot be dispatched until the fault is addressed. As mentioned previously, the length of the dispatch interval depends on the category of the fault

2.3.2 PIR Maintenance

When faults are unrevealed, and inspections must be performed to discover them, PIR maintenance is applied. An example is shown in Figure 2, where an unrevealed fault occurs at time *tf*, between two consecutive inspections, *I*1 and *I*2. The fault is discovered at *I*2, when it is assumed to have occurred midway between the two inspections, at time *t*1. The dispatch interval is then assumed to have started at this time and hence the aircraft may be dispatched for a further time *T* (≥0) following *I*2 before the fault must be cleared in order for further dispatch to be allowed. The inspection interval can be adjusted according to the duration of the dispatch interval in order to give a value of *T* that will allow sufficient flexibility for convenient scheduling of maintenance.

*t*1

*t*2

*t*

dispatch interval

**Figure 1. MEL maintenance**

*t*1

*t*2

*t*

dispatch interval

*I*1

*I*2

*tf*

*T*

**Figure 2. PIR maintenance**

## 2.4 Multiple Faults

When a combination of faults is present in the system, there is the opportunity to employ different repair strategies. Figure 3 shows a simple example of this in the case of faults addressed using MEL maintenance, where two faults, *A* and *B*, are both assigned to the LT category. Occurring in isolation, they would lead to dispatch intervals ending at *t*1 and *t2* respectively. However, the simultaneous presence of both faults in the system as *B* occurs at *tB* leads to an increase in the instantaneous LOTC rate, which requires application of the ST category due to the fault combination *AB*. This leads to the initiation of an ST dispatch interval ending at *t*3. There are three options at *t*3: clear both faults (allowing indefinite dispatch); clear *A* alone (allowing dispatch until *t*2, since *B* is still present); clear *B* alone (allowing dispatch until *t*1, since *A* is still present). Whilst the scenario described is simple, care must be taken when applying TLD to ensure the correct timing of dispatch intervals, e.g. if *B* were to occur later it could be that *t*1 < *t*3, which would mean the LT dispatch interval associated with *A* would end before the ST interval associated with *AB*. The occurrence of further faults and the application of PIR maintenance can also have a bearing on the choice of repair strategy.

*tA*

*t*1

*t*

LT

*tB*

*t*2

LT

*t*3

ST

Figure 3. Two faults combining under MEL maintenance.

# 3 Existing TLD Models

In order to demonstrate that TLD can be safely applied to a system models must be constructed and analysed to show that the TLD application complies with certification requirements. Techniques such as Fault Tree Analysis are unsuitable because of the dependencies that are introduced during the application of TLD. A Markov Analysis model that covers all possible system states would also be unsuitable because of the state space explosion that would occur because of the system complexity.

Two models are recommended for the analysis of TLD [3], with examples of their application to simple systems given in [1]. They are simple, state space models with a reduced number of system states. The models ideally require the use of in-service data to provide transition rates between the different modelled states. They do not cover all complexities of TLD but, when in-service data is available, provide a suitable means of system analysis.

A Monte Carlo (MC) simulation model was proposed that is ideal in situations where in-service data is unavailable, such as during a system’s design phase or at any point prior to a system’s introduction to a fleet [4]. The MC model handles MEL and PIR maintenance [5], along with the possible repair strategies at maintenance [6] and the occurrence of multiple faults [7]. Further development included a novel, automated, iterative approach for setting the dispatch criteria for a system [8] and the MC model was validated on a small-scale system using a Markov model that included all possible system states [9]. The MC model was further expanded to produce a number of importance measures that can be used to identify system weak points for design improvements, to prioritise repairs when time is limited and to prioritise repairs that take place as part of preventive maintenance [10].

The MC model brings a number of features that make it very well-suited to the analysis of TLD. However, the main criticism of the model is its lack of transparency to the user, given that it is, in essence, a ‘black box’ software model. This makes it unlikely to be applied during certification. For this reason, a Petri net (PN) modelling approach was proposed in order to clarify the model construction through a modular PN model whose graphical layout brings transparency to the modelling process [11]. The modelling approach was applied to a small system in [12] and used to calculate the system’s LOTC rate. This paper contains an overview of the PN model applied to this system. A subset of the results are analysed and features of the examined distributions used to help to verify the correctness of the model.

# 4 Petri Nets (PN)

Petri nets (PN) are graphical and mathematical tools that can be used to model and analyse dynamic system behaviour [13,14]. They are directed, bipartite graphs that contain two types of nodes: *places* (circles) and *transitions* (bars), which are connected by *edges* or *arcs*. The places contain *tokens* and the PN *marking* is given by the distribution of tokens among the places. Different markings represent different system states and the PN moves between different markings as the transition process of *switching* or *firing* takes place. Figure 4 shows, for a simple PN, how the firing process works.

Figure 4. Transition enabling and switching.

3

2

2

3

2

2

***t***

***t***

time *t* later

The transition in the PN shown on the left of Figure 4 has three input places, each marked with a number of tokens greater than or equal to the number of arcs between the place and the transition. For this reason, the transition is *enabled*, meaning that once the time delay *t*, associated with the transition has elapsed, the transition will fire. When the transition fires, an arc number of tokens is removed from each of the input places and an arc number of tokens is added to each of the output places, resulting in the PN being marked as shown on the right of Figure 4. If the time delay associated with the transition is 0, it is termed *immediate* and the transition is depicted as a solid bar.

Figure 5 depicts another type of arc, an *inhibitor* arc, which connects a further input place to the transition depicted in Figure 4. The inhibitor arc works by preventing the firing of a transition to which it is an input regardless of whether or not the transition would be enabled by the other places that are inputs to it. Therefore, as can be seen in Figure 5, the transition does not fire after a time *t* because of the presence of the inhibitor arc.

Figure 5. Inhibitor arc preventing switching.

3

2

2

***t***

time *t* later

3

2

2

***t***

The structure of PN and their dynamic behaviour makes them an ideal framework for MC simulation [14,15]. PN form a pictorial representation of the simulation model to be implemented and the system moves from one state to another as transitions fire within the PN. The transition delays are obtained during the simulations by sampling from probability distributions that are associated with the process related to the transition, such as component failure or repair.

# 5 System for Analysis

In this section a proposed modular PN model for a simple system, previously presented in [12], is briefly outlined. Whilst small, the modelled system exhibits the basic characteristics of a FADEC system and allows the demonstration of the modular constructs that can be used to model the application of TLD to systems and find the average system LOTC rate for the system.

The system contains four components, A, B, C and D, whose failures combine to lead to a LOTC event as depicted in the fault tree in Figure 6. The fault combinations AB and CD cause system failure. The system is assumed to have an operational lifetime of 130 000fh.

Figure 6. Fault tree representing LOTC for the example system.

LOTC

The dispatch criteria for the system involve all single faults, A, B, C and D, being classified as LT dispatch faults and all dispatchable dual faults, AC, AD, BC and BD, being classified as ST dispatch faults. The LT faults for this system are maintained using PIR maintenance with a dispatch interval of 500fh. The inspection interval is set at 800fh and this leads to a delay before maintenance (corresponding to *T* in Figure 2) of 100fh. The ST faults are maintained using MEL maintenance, with the dispatch interval set at 250fh.

The failure probability distributions assumed for each of the components are not intended to be representative but their characteristics will assist in the verification of the PN model. A and D are assumed to fail according to a negative exponential distribution with failure rates of 2×10-5 failures per fh and 1×10-5 failures per fh respectively. The failures of components B and C are assumed to follow Weibull distributions, with shape parameters of 0.7 and 0.6 (indicating burn-in) and scale parameters of 5.0×10-4 and 7.5×10-4 respectively.

The repair strategy employed in routine maintenance is to clear only the fault or fault combination that caused a dispatch interval to be initiated as that dispatch interval comes to an end. When a LOTC event occurs all faults are cleared from the system but the system is not returned to an as-new state.

# 6 PN Model of System

This section contains a brief overview of the PN model for the application of TLD to the system described in the previous section. The PN modules are shown in Figures 7 and 8. More detail of the model can be found in [11]. In the PN modules shown, bidirectional arcs are depicted using dotted lines and places that occur in more than one module are depicted using two concentric circles.

## 6.1 Component failure and repair (Figure 7a)

Component A failure and repair is implemented in the PN by the ‘A fail’ and ‘A rep’ transitions, which mark the ‘A up’ and ‘A dn’ places as appropriate. The failure transition is timed with delay sampled from the relevant failure probability distribution and the repair transition is immediate, but can only be enabled when the ‘rep A now’ place is marked. This is marked according to the maintenance that must take place.

## 6.2 LOTC events (Figure 7b)

The PN that encodes the state of the system is obtained from the fault tree for LOTC and its dual. The ‘LOTC’ and ‘not LOTC’ places are marked according to the component states.

## 6.3 Setting dispatch intervals (Figure 7c)

When the TLD fault is revealed, the ‘set’ place is marked; when it is no longer present (after maintenance), the ‘not set’ place is marked. The fault is revealed either instantly, in the case of MEL faults, or after inspection, in the case of PIR faults.

## 6.4 Scheduling PIR inspections and maintenance (Figure 7d)

Between inspections (‘PIR wait’) any of the LT faults can occur unrevealed. After the inspection interval (the delay associated with transition ‘PIR insp int –LT’) has elapsed the inspection takes place, and doesn’t end until all LT unrevealed faults are revealed. Then after a ‘PIR delay’ (equivalent to *T* in Figure 2) elapses, PIR maintenance is performed, not ending until all revealed PIR faults have been repaired.

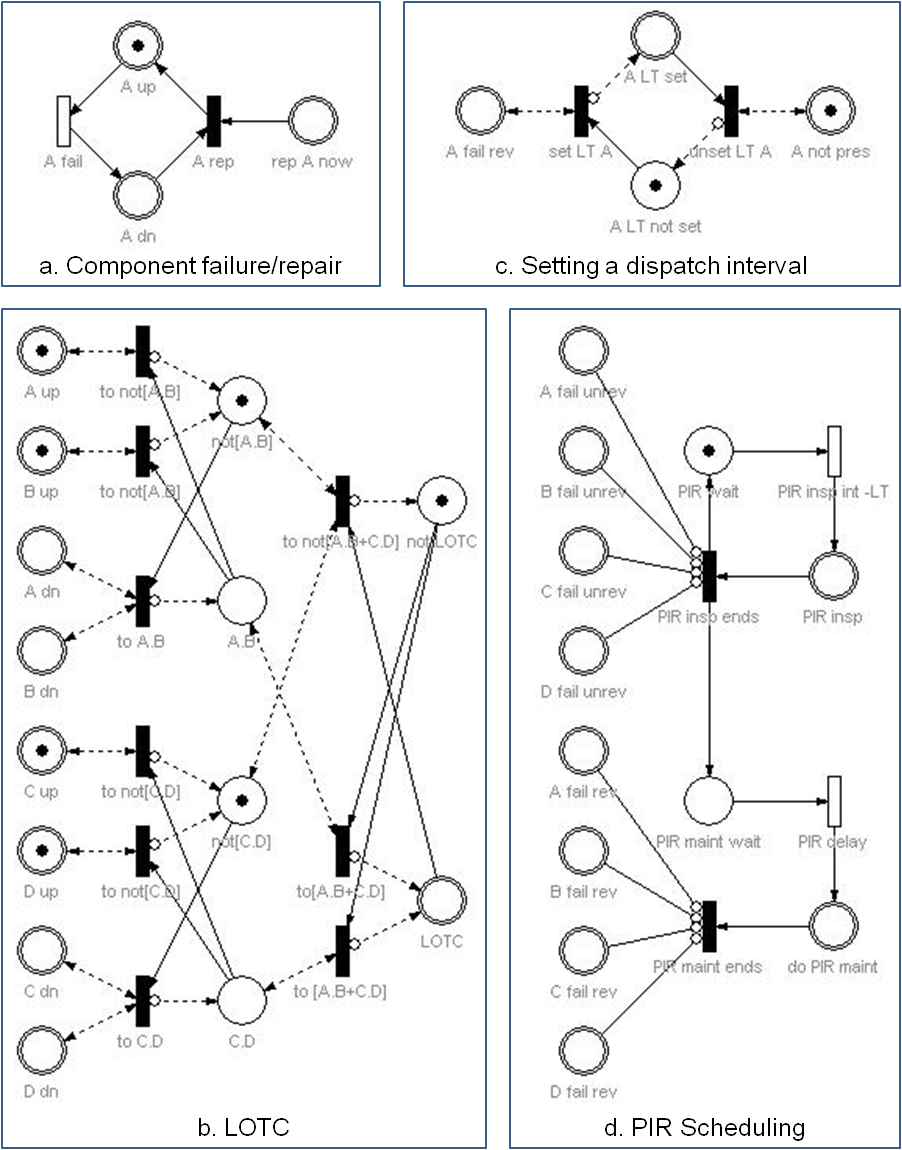


Figure 7. PN modules for component failure repair, LOTC, setting TLD

intervals and scheduling PIR maintenance.

## 6.5 MEL deadlines and maintenance (Figure 8a)

For ST faults, which are covered here by MEL maintenance, the fault is revealed as soon as it occurs (‘AC pres rev’ is marked). This enables the transition ‘ST MEL int’, which has a delay the length of the dispatch interval. Once this transition fires, the place ‘do AC ST rep’ ensures the relevant places are marked to initiate component repair, as shown in Figure 7a. There are two transitions (labelled ‘clearing AC’) which ensure the PN is returned to the shown initial state if the fault is cleared before MEL maintenance takes place, e.g. due to PIR maintenance of the constituent faults, or maintenance following a LOTC event.

## 6.6 PIR maintenance (Figure 8b)

The PN module for PIR maintenance is similar to that for MEL maintenance, with the exception of additional places and transitions representing faults being revealed.

## 6.7 Maintenance following LOTC (Figures 8c,8d)

When a LOTC event occurs the transition ‘start rep at LOTC’ fires, marking place ‘rep after LOTC’. This maintenance will only end after each component fault has been cleared.

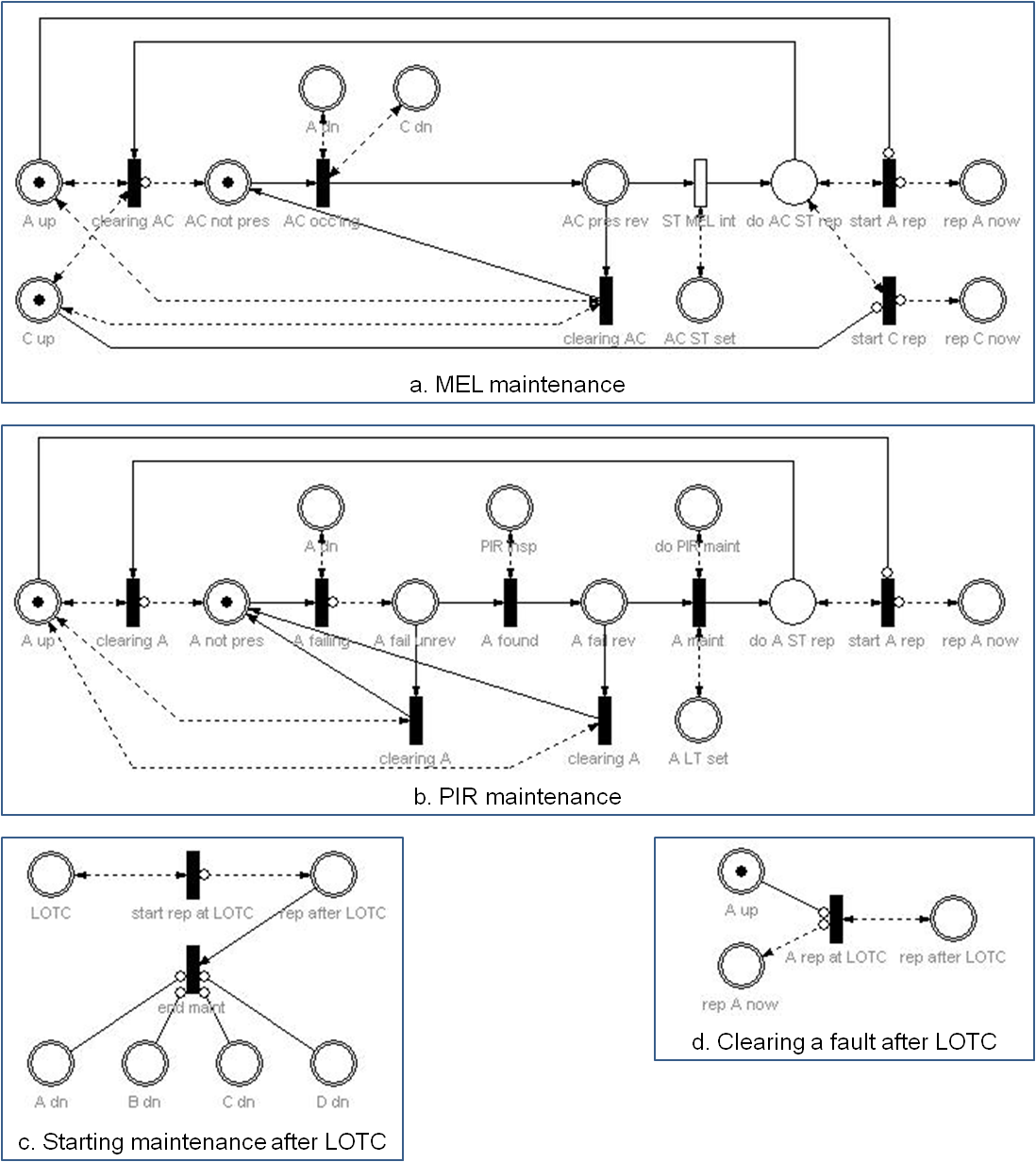


Figure 8. PN modules for MEL and PIR maintenance, and starting and performing maintenance after a LOTC event.

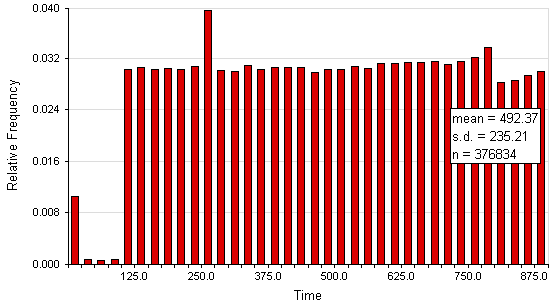
# 7 Results

By carrying out a MC simulation using the developed PN as a framework, the average system LOTC rate was calculated to be 5.16×10‑7, which was in agreement with results obtained using a previously-existing MC model [12]. Further validation of the PN model can be achieved through analysis of the distributions of the lengths of time that certain places are marked.

Figure 9 shows the distributions of times spent in the ‘B dn’ place, which corresponds to the time taken to repair component B. The distribution has a number of features. It can be seen that the minimum time to repair B is 0fh and the maximum is 900fh. This relates to the PIR inspection interval of 800fh plus the maintenance delay of 100fh after an inspection (*T* in Figure 2). The mean time to repair B is less than the 500fh dispatch interval, which is expected due to the fact that, on occasion, B is repaired after the occurrence of a ST fault (either BC or BD) or after a LOTC event occurs. There are a number of other features:

1. The peak at 0fh relates to LOTC events which occur as B fails, where B is repaired immediately.
2. Other than at 0fh, there is a low probability of B being repaired before 100fh, the duration of the maintenance delay. This is because, unless A fails to cause a LOTC event within 100fh of B failing, B cannot be discovered within 100fh of failing and hence repaired (assuming that LT PIR maintenance only takes place if B is discovered at an inspection).
3. It can be seen that it is most likely that B will be failed for between 100fh and 900fh; this is mostly due to the fact that, if B alone is failed it will be failed for at least the 100fh maintenance delay.
4. There is a peak at 250fh, due to the occurrence of the ST dual faults where B is the fault which occurs second and causes the ST MEL deadline to be initiated.
5. Ignoring the step at 800fh, there is a general increase in the likelihood of B to be failed for longer periods of time, seen by the upward trend in the slope. This is due to the fact that B fails according to a Weibull distribution with shape parameter <1, indicating a burn-in phase for the component.
6. The step reduction at 800fh is caused by specific instances of B being repaired at an ST deadline. To illustrate such an instance, consider Figure 10. B fails after A was discovered at inspection *I*2, but before A is repaired at *t*2. Therefore ST maintenance is scheduled for *t*3. At *t*2 A is repaired, but B remains in the system, it’s failure was not revealed at *I*2 and it would ordinarily be repaired after discovery at the next inspection, somewhere between 800fh and 900fh from its failure. However, since the ST fault was not fully cleared, B is repaired at *t*3 as the ST MEL deadline is reached. This occurs frequently enough, with faults AB and AC, to cause the step seen in the distribution.

Figure 9. Distribution of times to repair for component B.



*t*1

*t*

LT

*I*1

*I*2

*T*

ST

*t*2

*B*

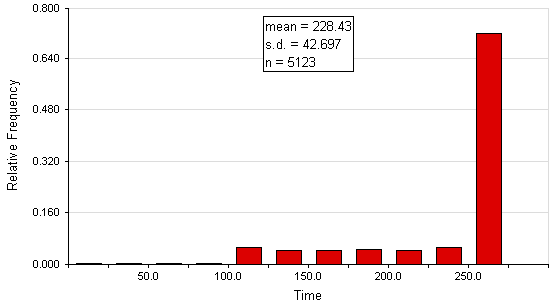
*A*

*t*3

Figure 10. Specific case of B repair after an ST fault

Figure 11 shows the distribution of the lengths of time for which place ‘AC ST set’ is marked. For the majority of times that A and C fail and cause an ST dispatch interval to be initiated, the ST fault is present for the entire ST dispatch interval, 250fh. The fault AC is cleared between 100fh and 250fh after occurring when the two LT faults, A and C, occur in the 150fh immediately before an inspection, are discovered at that inspection and repaired at the LT maintenance event that follows. Since both A and C are cleared at this time, so is the dual fault AC. It is rare for AC to be cleared within 100fh of occurring, as seen in the figure. This would only happen if either B or D occurred and caused a LOTC event to occur, after which all faults would be cleared.

Figure 11. Distribution of times for which the ST MEL interval for AC is set.



# Summary & Conclusion

A PN model for the application of TLD to a simple system has been briefly presented (further detail can be found in [12]). Its modular format gives it a clarity lacking in previous MC simulation models.

Following on from initial model validation in [12], further place sojourn time distributions were considered in order to offer additional evidence of the validity of the developed PN model. The properties of the considered distributions are fully consistent with the features of TLD as applied to the example system and serve to increase confidence in the TLD PN model.

The proposed TLD PN model offers advantages over previously-developed MC simulation models of TLD in its clarity and the ease with which validation can be performed, using both the graphical layout of the model and statistics that can be easily obtained from the PN while it is used as a framework for simulation. This clear validation means that a generalised TLD PN model of this type could be more easily accepted for certification purposes than the coded MC simulation approach presented in the past.

# Acknowledgement

Darren Prescott is The Lloyd’s Register Educational Trust Lecturer in Risk and Reliability Engineering at the University of Nottingham and gratefully acknowledges the support of The Lloyd’s Register Educational Trust (The LRET). The LRET is an independent charity working to achieve advances in transportation, science, engineering and technology education, training and research worldwide for the benefit of all.

# 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] 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., “Monte Carlo Simulation Modelling of Aircraft Dispatch With Known Faults,” Proceedings of ICRMS 2009 (International Conference on Reliability, Maintainability and Safety), Chengdu, China, 21-25 July 2009, pp 532-535, ISBN 978-1-4244-4903-3.

[5] Prescott, D.R. and Andrews, J.D., “Aircraft Safety Modelling for Time Limited Dispatch”, Proceedings of the Annual Reliability and Maintainability Symposium, Virginia, USA, January 2005, pp 139-145.

[6] Prescott D.R. and Andrews, J.D., “A Comparison of Modelling Approaches for the Time Limited Dispatch of Aircraft”, IMechE Part O Journal of Risk and Reliability, Vol. 220, No. O1, June 2006, pp 9-20, ISSN: 1748-006X.

[7] Prescott, D.R. and Andrews, J.D., “The Safe Dispatch of Aircraft With Known Faults”, International Journal of Performability Engineering, Condition Monitoring and Condition Based Maintenance Special Issue, Kumar, U., (ed), Vol. 4 No. 3, July 2008, pp 243-253, ISSN: 0973-1318.

[8] Prescott, D.R. and Andrews, J.D., “Modelling and Specification of Time-Limited Dispatch Categories for Commercial Aircraft”, ASME Journal of Dynamic Systems, Measurement and Control, Vol. 130 Issue 2, March 2008, ISSN: 0022- 0434.

[9] Prescott, D.R. and Andrews, J.D., “Modelling the Time-Limited Dispatch of Aircraft,” Proceedings of the 26th ISSC (International System Safety Conference), Vancouver, Canada, 25-29 August 2008, [CD-ROM].

[10] Prescott, D.R. and Andrews, J.D., “Component importance measures to identify contributions to system failure for aircraft which dispatch with known faults,” Proceedings of ESREL (European Safety and Reliability Conference) 2009, Prague, Czech Republic, 7-10 September 2009.

[11] Prescott, D.R., “Using Petri Nets to Model Time-Limited Dispatch,” Proceedings 19th AR2TS, Advances in Risk and Reliability Technology Symposium, Stratford-upon-Avon, UK, April 2011, pp 297-309.

[12] Prescott, D.R., “A Petri Net Model of Aircraft Maintenance Scheduling”, To appear in Proceedings of ESREL (European Safety and Reliability Conference) 2011, Troyes, France, September 2011.

[13] Murata, T., “Petri Nets: Properties, Analysis and Applications,” Proceedings of the IEEE, Vol.77 No. 4, pp. 541-580, April 1989.

[14] Schneeweiss, W.G. 1999. Petri Nets for Reliability Modeling, Hagen: LiLoLe.

Dutuit, Y., Chatelet, E., Signoret, J.P. & Thomas, P. 1997.

[15] Dependability Modelling and Evaluation by Using Stochastic Petri Nets. Reliability Engineering and System Safety, 55: 117-124.