MAINTENANCE OPTIMISATION OF A DIGITAL ENGINE CONTROL SYSTEM WITH LIMIT FAILURE RATE CONSTRAIN

Michel Boussemart, Snecma Control Systems
Thierry Bickard, Snecma Control Systems
Nikolaos Limnios, Université de Technologie de Compiègne

Abstract

In this paper, we consider error tolerant systems that remain fail-operational when affected by some identified faults. The idea is to use this feature to enhance the maintenance procedures for safety-critical systems having a stochastic failure scheme (e.g. electric and electronic control components) when they are embedded in a larger system composed of life-limited parts requiring periodical overhaul (e.g. a jet engine).

The current certification objectives require the manufacturer to show that the system's asymptotic failure rate is bounded to a prescribed value. One major constrain when optimizing the maintenance cost is to fulfil this certification objective.

The paper starts with an unambiguous redefinition of often misused probabilistic terms such as failure rate and asymptotic failure rate. Then some theoretical results are given to compute the associated figure with continuous and discrete Markov models. These models are handled using studies about positive matrices, which calls for the Frobenius spectral analysis.

In a second part, some examples of electronic control system architecture are given with some proposed associated failure model. Distributed architectures are particularly detailed because they are suspected to be well adapted to provide extended time limited dispatch capabilities due to their multiple reconfiguration capability.

The optimization of economical criteria is then introduced. Controlled Markov models are shown to be well suited to solving maintenance problems. These systems can be described as a finite state machine. Each state transition is associated with a decision making : dispatch or repair. The cost of each alternative is evaluated considering the original state and the time since last maintenance action. Further decisions are oriented by all past actions.

The optimization consists of computing a matrix linking the decision probability with the state.

The optimization criterion is the mean operating cost considered over the up periods. The rationales of the choice for that economical criterion are given.

The optimization problem is then turned into a linear optimization scheme, which is easy to solve with a simplex algorithm. For our real problem, facing a too large number of unknowns, an other approach need to be developed.

Finally, a complete and easy to figure out example is given. Our method is applied on a triple modular redundant computer but also on a distributed architecture. The missions are supposed to be of constant duration. The state is observed at each mission end and the probability figures are computed, providing a help in taking the decision to repair or to dispatch by indicating what is the best action to minimize the operating cost on the long term.

1. Introduction

Modern jet engine are controlled by a computer that assists the pilot in setting the required thrust, prevents the engine from entering potentially dangerous functioning areas. On most modern jet fighter and airliner, this computer is a full authority digital engine control (FADEC). It has to operate under very harsh functional and environmental constraints :

- unless other avionics equipments, it is nacelle-mounted and thus, it has to cope with extreme temperature variations, high vibration level and potential chemical contamination by a fuel leak, engine cleaning materials, hydraulic fluid and corrosive atmosphere. That’s why the components selection and usage, the box design and fastening are of primary importance ;
- it is the only mean to control the engine since no redundant hydraulic nor mechanical control remains. So it has to remain operational under all foreseeable circumstances, including internal fault, electrical power loss, etc. The computer is usually organized with a built-in dual redundancy, designed to tolerate a single physical component failure.

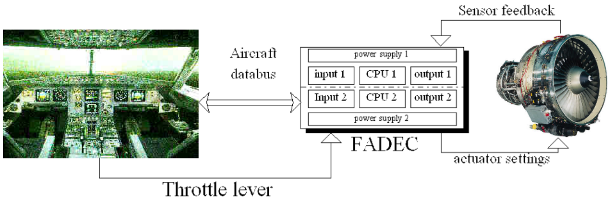

Figure 1

Both parts of the propulsion installation - the mechanical part and the electronic part – are subject to component failure. But the distribution of those failure are fundamentally different.

The failure process of mechanical parts is related to the fatigue phenomenon. It is quite easy to predict with an excellent level of confidence how long a component will last or how long it will take for him to fail after the first clue of wear has been detected. Thus, with a periodic inspection and overhaul scheme, it becomes possible to obtain the availability and reliability required by the airline companies.

On the other hand, the electronic parts are affected by random component errors. It is impossible to predict how long a solid state electronic component will last. The behavior over time reveals to be a constant failure rate, meaning that no life-time prediction can be made on an isolated item. If an electronic item powers-up correctly, it can continue to run properly for one century, or fail within the following minute. Methods to reduce that failure rate are well-known : supplier selection, components screening, stress limitation, etc. but none exists that enables a prediction of the remaining life-time. Such a behavior means that the only efficient maintenance scheme is to wait for a component failure to replace it.

The propulsion system is thus under the sway of a periodic inspection program aimed at getting rid of unavailability, and even though, the aircraft has to be grounded, each time the electronics fails, for an immediate overhaul. This phenomenon has no real implication as long as the remaining unattended mechanical outage rate is high compared to the intrinsic failure rate of the electronic items. But as mechanics improve their knowledge, techniques and materials, the residual unattended failure rate of the engine has fallen in such a way that an engine can now operate more than 30000 hr without unscheduled part replacement. This becomes better than the mean time between failure (MTBF) of a FADEC, and the aircraft grounding rate due to FADEC problems emerges among other no-go sources.

The time limited dispatch concept

Some simple analyses, based on a Markov reliability model and a fault categorization derived from the system safety assessment, show that the dual redundancy can enable to continue flying the aircraft, even with some faulty parts in the FADEC system, without an unacceptable impact on the probability of in-flight engine loss.

The engine manufacturers and the certification authorities agreed on the applicable rules for flying with faulty subitems in the control system. The corresponding paper is an SAE document [1]. It uses an approximate Markov model to determine the allowed dispatch times.

Our concern is to extend the time limited dispatch capabilities by providing the evidence that the safety is not impacted. This requires more powerful models that are developed hereafter.

2. Definition

2.1 Preliminaries

States. Our aeronautical electronic system can be in s+1 states :

- The state '1' is the Full-up state,
- The states '2,...,S' are up states affected by some identified faults. The system remains operational but may be degraded.
- The state 'S+1' is the down set, also called the LOTC (Loss Of Thrust Control) state.

Failure transitions. Every electronic component of our system have a constant failure rate.

Repair transitions. In many applications, in particular in the SAE document, the repair transitions are also given by constant rates. If the average time before the repair is T then the transition rate is 1/T.

Under the two above assumptions, it is possible to build a continuous model for the maintenance of our system. Section 2.2 shows how to define it and how to calculate the security criterion (Cf. Theorem 1) and the economic criterion (Cf. Theorem 2).

Unfortunately, for our real problem, the assumption about constant rate of the repair does not apply. Indeed, the duration of missions and the instants of planned maintenance must be considered. Section 2.3. gives us the material to define a new discrete model for the maintenance. Moreover, since the definition of the security criterion by the SAE document concerns a continuous model, it is important to extend the definition of the security criterion and the economic criterion.

2.2 Continuous model for the maintenance

This section presents the main ideas of the SAE document, including :

- the definition of the Markov process
- the calculation of the asymptotic failure rate.

Moreover, we define the economic criterion.

Let us define the stochastic process describing the failures and the maintenance of our system. Let $X=(X_t)$ denotes a Markov process with a state space E. At each continuous instant t, X_t represents the state of the system. Let us denote by α the initial distribution, i.e. for all state i in E: $\alpha(i) = \mathrm{P}(X_0 = i)$.

Let $A=(a_{ij})$ be the intensity matrix of X :

- all entries a_{ij} (i<j or j>i) correspond to a transition i⟶j.
- the a_{ii} are such that $\sum_{j\in E} a_{ij} = 0$.

Let us define the nature of the transitions (i⟶j) of our continuous Markov model :

- if j>i then it is a failure transition,
- if j<i then it is a repair transition. Generally we have j=1. If T_i is the average time before the repair then the transition rate is given by $1/T_i$.

Let us define a partition U,D of E, where U is the up state set and D is the down state set.

Assumption 1. All states i, j of U communicate, i.e. there exists a path between each state i and j. A sufficient condition is that for all state i>1 of U there exists a repair transition (i.e. a path between i and 1).

Let us define T, the life time of our system, i.e. the time of the first passage in D by: T=inf($t \in \Re : X_t \in D$). The reliability a each instant t is defined by: R(t)=P(T>t).

The SAE document gives the definition of the failure rate and the asymptotic failure rate.

Definition 1 *(Failure rate) The failure rate is the instantaneous number of LOTC events per hour, i.e.,*

$$\lambda(t) = -\frac{R'(t)}{R(t)}.$$

The failure rate does not necessary converge to a value as t tends to infinity. Nevertheless, under assumption 1, a limit exists, thus the following definition.

Definition 2 *(Asymptotic failure rate) Under assumption 1, the asymptotic failure rate λ_c is the average number of LOTC events per hour when the system runs during a large amount of time :* $\lambda_c = \lim_{t\to\infty}\lambda(t)$.

Note: In fact in the SAE document, the security criterion is not really the asymptotic failure rate of the system but the average asymptotic failure rate of a fleet of many systems. Here and in the same manner as in the SAE document, we make the assumption that one system is representative of the entire fleet.

Theorem 1 *Under assumption 1, the asymptotic failure rate is* λ_d=-ν, *where* ν *is the real negative eigenvalue with the smallest modulus of* A_1, the restriction of A on U × U.

Numerically, it is easy to compute the asymptotic failure rate, since it is easy to calculate the eigenvalues of a matrix.

Let us define the economic criterion. The objective of new architectures is that the repairs coincide at most as possible with the planned maintenance. Therefore, the objective is to minimize the number of immediate repairs. Another formulation is to maximize the time between two immediate repairs. This time is called the MTBUR.

Definition 3 (Economic criterion for a continuous model) Let F be a subset of U, that do not induce immediate repairs. Then, the MTBUR is the average sojourn time of X in F.

The next theorem gives us the material to calculate the economical criterion.

Theorem 2 *Let F be a subset of U. Then the average sojourn time s_F in set F is given by :*

$$s_F = -\alpha_F A_{FF}^{-1} 1_F,$$

where α_F is the restriction of α on F, where A_{FF} is the restriction of A on F × F and where 1_F is the |F| elements column vector with all elements equals to 1.

The continuous model presented here becomes insufficient when we must consider real constraints such as the discrete time of observations, the planned maintenance, etc. In the next section, we build a new discrete model in order to integrate these constraints. Nevertheless, we can use the above continuous model for giving the order of the security and economical criterions.

2.3 Discrete model for the maintenance

Let X=(X_n) be a Markov chain with initial distribution α and with transition matrix P.

Let T be the life time of our system (i.e. the time of the first passage in the set D). Let θ be the discrete step time (i.e. the duration of each mission).

Since in a discrete model the failure rate does not converge to a value, but to many asymptotic values, the idea is to define the asymptotic failure rate by the average of these limit values, thus the following definition.

Definition 4 *(Average asymptotic failure rate) Under assumption 1, the average asymptotic failure rate λ_d is defined by*

$$\lambda_d = \frac{1}{\theta}\lim_{n\to\infty}\frac{1}{n+1}\sum_{k=0}^{n}\mathrm{P}(T = k | T \geq k).$$

Note : for the new definition of the asymptotic failure rate, we keep the idea of the SAE document. Moreover, we can use the model of section 2.2 as an approximation to verify if the maintenance strategy is such that the security constraint is satisfied.

Approximation. In practice, we have : $\lambda_d \approx \theta^{-1}.(1-r)$, where r is spectral radius (also called the Perron-Frobinus eigenvalue) of Q, restriction of P on U × U.

Note : The definition of λ_d coincides with the definition of λ_c. Indeed if $X=(X_n)$ is the digitization of the previous Markov Process with time step θ then:

$$\lambda_d \approx \theta^{-1}.(1-e^{\theta\upsilon}) \approx -\upsilon = \lambda_c \, .$$

In the same manner as in section 2.1, let us define the MTBUR. Here, we can be more precise : the MTBUR is the average time between two repairs not coinciding with the planned maintenance. Thus the following definition.

Definition 5 (Economic criterion for a discrete model).
Let F be a subset of U, that does not induce repairs not coinciding with the planned maintenance. Then, the MTBUR is the average sojourn time of X in F.

Theorem 3 *Let F be a subset of U. Then the average sojourn time s_F in set F is given by :*

$$s_f = \theta.\alpha_F (I - P_{FF})^{-1} 1_F \, ,$$

where α_F the the restriction of α on F, where P_{FF} is the restriction of P and where I is the identity matrix.

Approximation. In practice (if all states i, j of F communicate), we have: $s_F \approx \theta.(1-r_F)^{-1}$, where r_F is the spectral radius of P_{FF}.

3. Examples of electronic control system architecture

3.1 Dual redundancy

This is the well known architecture of most engine control in service today. Both control channel are identical and perform the same computations at the same time. A fault is detected by output comparison. The faulty channel is identified by a built-in self test (BIST). The state set is E={1, 2, 3}:

- state 1 : both channel are up,
- state 2 : one of the two channel is down,
- state 3 : both channel are down, or one channel is down and the BIST has failed to discriminate the faulty one. This is the LOTC state.

We have U={1,2} and D={3}.

The failure model (without any maintenance consideration) is represented by the figure 2, where λ is the elementary channel failure rate and where τ is the fault detection probability.

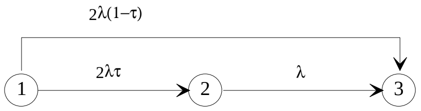

Figure 2 - Failure model of a dual system

3.2 Triple redundancy

This system behaves first like a '2 out of 3' system. After the first fault, it behaves like the dual system. The state set is E={1, 2, 3, 4}:

- state 1 : the three channels are up,
- state 2 : one of the three channel is down,
- state 3 : two channels are down
- state 4 : all three channels are down, or two are down and the BIST failed. This is the LOTC state.

We have U={1, 2, 3} and D={4}. The failure model is represented by the figure 3.

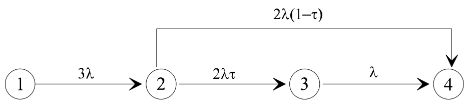

Figure 3 - Failure model of a triple redundancy system

3.3 Distributed architecture

The distributed architecture we consider here is a modular computer composed of four processing units interconnected by point to point hi-speed links (see figure 4). At least two processing units are necessary to perform the full control functions.

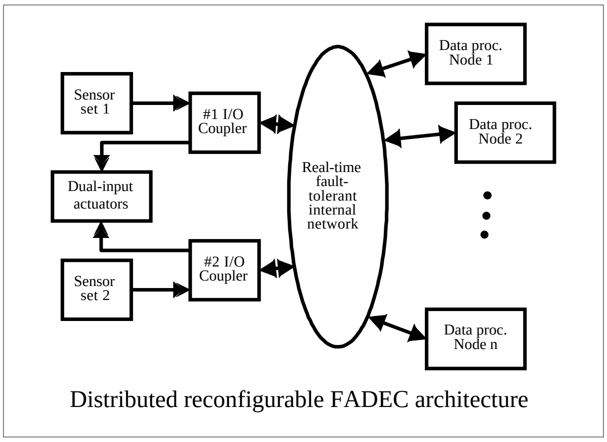

Figure 4

Let us define the failure model. Each state of the graph is a pair (n, m), where n is the number of links and where m is the number of working processing units. A state corresponds to a set of equivalent configurations (Cf. figure 5).

Each transition of the graph represents a failure, either a processing unit (which failure rate is λ_S) or a link (which failure rate is λ_L). Using the symmetry of the problem and forbidding some configurations (see the note below), we obtain our failure model (Cf. figure 6).

Note : for example, a configuration that consists in a chain of 4 processing units is forbidden.

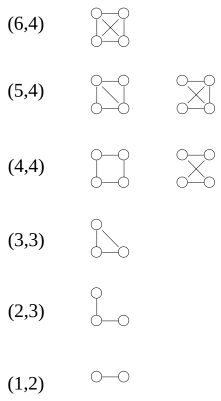

Figure 5 - States (equivalent configurations) of the failure model

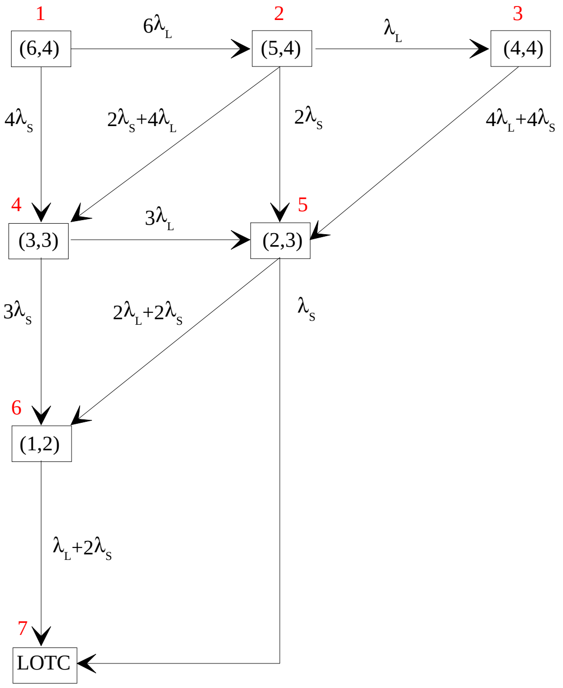

Figure 6 - Failure model of a distributed architecture

4. Discrete Model for the maintenance

Our aeronautical system accomplishes constant duration missions. Before each mission, an inspection or a power-on test gives the observed state of the FADEC : i=1,...,s+1. If i=1 (Full Up state) or i=s+1 (the absorbing down state) then no decision has to be taken. Else we must decide whether to repair or not.

Every N missions, a maintenance of the aeronautical system is planned. Under the constraint on the asymptotic failure rate, the objective is to maximize the time between each repair not coinciding with the planned maintenance. This time is called the MTBUR (mean time between unscheduled repair).

To keep the idea of the SAE document [1], the aim is to determine for each new failure transition and for each instant a new dispatch time before the repair. Unfortunately, for the maintenance, we cannot use classical Markov models : we cannot keep the homogeneous assumption and the independence of the past on the future (Markov property).

Instead of using a one dimensional Markov Chain, a solution is to use multidimensional Markov chain. One dimension gives the state of the system, another gives the time and all others the information about past decisions.

In the next section, our model is built to consider specific kind of maintenance strategies. The optimization problem does not appear. The aim is to propose a model when the maintenance strategy is known. In the second section we compute the security criterion and in the third section, the economic criterion.

4.1 Markov Model for any maintenance policies

Let us denote by $X=(X_n)$ the Markov chain for the maintenance (failure + repairs) with state space E, up states U and down state D.

For each n, X_n is a vector $X_n=(E_n, T_n, S_n, D_n)$:

- E_n : the observed state at the end of a mission,
- T_n : the number of the mission after the maintenance inspection,
- S_n : the number of missions since the first failure,
- D_n : the delay for the repair.

The state set of X is E={1,...,S+1} × {1,...,N} × {1,...,R} × {1,...,R}, where R is the maximal cumulated delay allowed in the failure state.

At each end of mission, a new vector X_n is observed and a decision (or new repair delay) is taken. Thus, the transition matrix P depends on the maintenance strategy.

When the currently observed state is $E_n=1$ (resp. S+1), since it is the Full Up state (resp. the absorbing down state), $S_n=D_n=1$ (we do not need this information).

When a first failure is observed, i.e. when a transition '$E_n=1$'→ '$E_{n+1}=i$' (or for short a transition '1→i') is observed then a delay $D_{n+1}=d_{n+1}$ before the repair is imposed. The delay must be inferior than R (the maximal allowed delay).

When a second (third, fourth, etc.) failure is observed, i.e. when a transition 'i→j' is observed then a new delay $D_{n+1}=d_{n+1}$ before the repair is imposed. It can depend on S_n, the total sojourn time in degradable states. d_{n+1} must be strictly less than $D_n=d_n$. Moreover the sojourn time S_{n+1} equals to S_n+1 (because the sojourn time in degradable states must be cumulative).
for the transition '$T_n=t_n$'-'$T_{n+1}=t_{n+1}$', t_n and t_{n+1} are such that : $\begin{cases} t_{n+1} = t_n + 1 & if \quad t_n < N \\ t_{n+1} = 1 & if \quad t_n = N \end{cases}$.
if $D_n=0$, then a repair takes place before the next mission. Since the next observation X_{n+1} arises after the latter mission, we must consider a transition '1→i'.

Example. Let us consider the triple redundancy architecture. Every 2 missions, a maintenance is planned (at time $t_n=1$). We impose the following maintenance policy :

- for a first failure to the state 2 (i.e. for a transition '1→2'), the delay is such that the repair takes place during the planned maintenance (at time $t_n=1$).
- for a first failure to the state 3 (i.e for a transition '1→3'), the allowed delay before the repair is zero except for the case of one mission before the planned maintenance. Then the allowed delay is 1 (therefore the repair coincides with the planned maintenance).
- For all second failure (i.e. transition '2→3'), then the new delay is zero.

Cf. figure 7 for the Markov chain X. The transitions p_{11}, p_{12}, ... are obtained by the continuous failure model of figure 3, after digitization with step time θ=4h.

Note that the states (2,1,1,0), (2,1,2,0), (2,1,3,0) are aggregated in one state, and the same case for the states (3,1,1,0), (3,1,2,0), (3,1,3,0). Moreover the absorbing down state (4,.,.,.) is not represented (but there exists a transition between each state and the absorbing one).

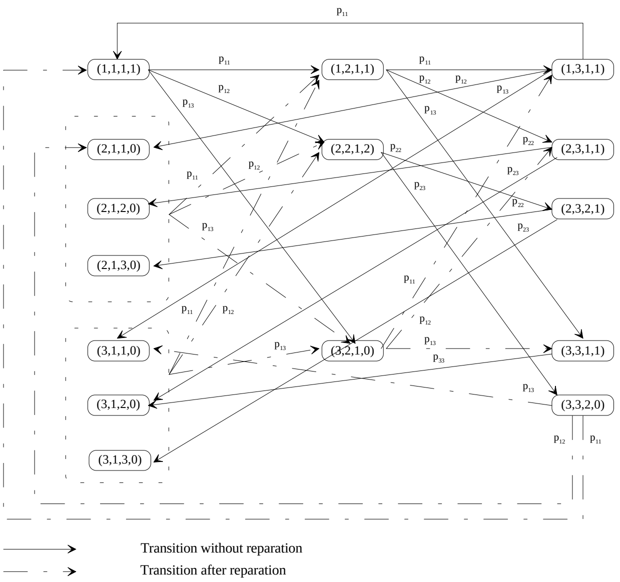

Figure 7 - Markov chain for the triple redundancy architecture

Obviously, the greater N is, the more our model becomes complicated. Therefore, a simple algorithm is needed to build automatically the graph.

4.2 Security criterion

We have to compute the asymptotic failure rate.

Example 1 (triple redundancy architecture, figure 7). The set U contains all the states of the figure. For the following data λ=1.10^{-5} h^{-1}, τ=1-1.10^{-3} h^{-1} and θ=4h, we obtain: λ_d=3,68.10^{-12} h^{-1}.

Example 2 (triple redundancy architecture, figure 7, with a modified delay). When the transition 1→3 is observed one mission before the planned maintenance, we impose a delay equals to zeros (instead of 1). With the same above data, we obtain: λ_d=3,66.10^{-12} h^{-1}.

4.3 Economic criterion

We have to calculate the MTBUR. It is given by the mean sojourn time of the Markov Chain X in a set F included in U. The set F must contain all states that do not generate a repair or states that coincides with a planned maintenance.

Example 1 (triple redundancy architecture, figure 7). We have F=U \ {(3,2,1,0),(3,3,2,0)}. We obtain: MTBUR=8,32.10^{8} h.

Example 2 (triple redundancy architecture, figure 7, with a modified delay). We obtain : MTBUR=6,24.10^{8} h.

5. Optimization of the maintenance

5.1 Theoretical methods

For our maintenance problem, a class of model widely found in the literature can be used : the Markov Decision Processes (MDP). A MDP is a classical Markov Process with two additional elements:

- a control (for us the maintenance strategy),
- an economic criterion (for us the MTBUR).

But an immediate solution does not exist in the literature :

- Generally the systems are repairable. But for us, there exists an absorbing set of states.
- Generally the constraint are about the state-action frequencies (Cf. [2]). The constraint on the asymptotic failure rate is new.

Therefore, the first step is to extend the known results. A method using the linear programming scheme to find an exact optimal solution is developed in two articles (Cf. [3] and [4]).

Unfortunately, we face a too large number of unknowns when the method is used in real problem. Nevertheless, these results can be used for small systems.

Another method must be developed. In fact, the principle is to test many different maintenance policies and also different architectures in order to keep the one offering the best result.

5.2 Approximated method

The objective is not really to find the optimal maintenance strategy. The aim is to introduce new architecture with a similar (or better) asymptotic failure rate and with a objective MTBUR. Thus, we do not need to find an absolute optimal maintenance policy. Our objective is only to find a suitable maintenance policy that considers the real constraints (mission duration, planned maintenance).

Since the dual redundancy architecture is already in use in a real systems, we take it as a reference. With the associated maintenance strategy, we first calculate the asymptotic failure rate and the MTBUR. Then, for the new architectures the objective is to find strategies with a similar asymptotic failure rate and a better (or fixed) MTBUR.

Note : The airworthiness rules require a value of the asymptotic failure rate less than 1.10^{-5} h^{-1}. In fact, when considering our model for the dual architecture and with the maintenance strategy, we find an asymptotic failure rate less than this value. This is due to the fact that our model is based on predictive components reliability figure, rather than actual data coming from the field. Nevertheless, we assume that the ratio is a constant and we keep this value as a baseline.

6. A real application

We first apply our model to the dual redundancy architecture with the currently applied maintenance in order to compute the asymptotic failure rate and the MTBUR. Then, we study the two other architectures.

6.1 The dual redundancy architecture

Numerical data. $\lambda=1.10^{-5}$ h^{-1}, $\tau=1\text{-}1.10^{-2}$, $\theta=4h$.

Maintenance strategy. When the transition '1→2' is observed, the allowed delay is zero (immediate repair).

Subset defining the MTBUR. F is the subset of U without the states introducing an immediate repair, i.e.

$$F = U - \{(e,t,s,d) \in U : d = 0 \text{ and } t > 1\}.$$

Results. We obtain $\lambda_c=2.10^{-7}$ h^{-1}, MTBUR=50500h.

The values we obtain here are considered as the baseline. Indeed, for the new architectures, we must have :

- $\lambda_c \leq 2.10^{-7}$ h^{-1} (1)
- MTBUR>50500h. (2)

6.2 The triple redundancy architecture

Numerical data. (the same as above).

Maintenance strategy.

- When the transition '1→2' is observed, we decide to repair at the pth encountered planned maintenance, where p is a fixed parameter.
- When the transition '1→3' is observed, the allowed delay is zero.

Subset for the MTBUR. (The same as above).

Results. For "p=infinity", we obtain: $\lambda_c=1.2.10^{-7}$ h^{-1}, MTBUR=83333h. Consequently, there is no need to repair when the transition '1→2' is observed.

Since it is an architecture that offers interesting results, we can afford a worse value than 1.10^{-5} for λ (e.g. by allowing an increased complexity for each channel). Lets try $\lambda=2.10^{-5}$ h^{-1}. We obtain :

- "p=infinity" : $\lambda_c=2.4.10^{-7}$ h^{-1}, MTBUR=41667h. It is not an allowed maintenance strategy because condition (1) is not satisfied.
- P=1 : $\lambda_c=4.7.10^{-9}$ h^{-1}, MTBUR=2153200h
- P=20 : $\lambda_c=1.19.10^{-7}$ h^{-1}, MTBUR=82700h
- P=50 : $\lambda_c=1.83.10^{-7}$ h^{-1}, MTBUR=50600h.

It is therefore possible to increase by 60% the MTBUR by changing the dual architecture to a triple redundant one.

6.3 The distributed architecture

Numerical data. $\lambda_s=1.10^{-5}\ h^{-1}$, $\lambda_L=1.10^{-6}\ h^{-1}$.

Maintenance strategy. When the transition '1→2, 1→3 or 1→4' is observed, we decide to repair at the pth encountered planned maintenance, where p is a fixed parameter. When a transition, 'i→3' or 'i→4' is observed, the allowed delay is not modified. When a transition 'i→5' or 'i→6' is observed, the allowed delay is zero.

Results.

- P=1 : $\lambda_c=2.63^{-10}\ h^{-1}$, MTBUR=455500h.
- P=2 : $\lambda_c=7.4.10^{-10}\ h^{-1}$, MTBUR=161200h.
- P=40 : $\lambda_c=5.6.10^{-9}\ h^{-1}$, MTBUR=18300h.

6.4 Discussion

For the two new architectures, we have determined some maintenance strategies with associated asymptotic failure rate and MTBUR. Our objective is achieved because we can first specify an MTBUR in an allowed range (i.e. for which asymptotic failure rate is less or equal to $2.10^{-7}\ h^{-1}$) and then determine the maintenance policy.

Note : it is easy to consider other economic criteria than the MTBUR. Indeed, since for each specified maintenance strategy the entire model is built, all probabilistic values can be calculated.

7. Conclusion

In this paper, our main objective is to propose a method showing that the new architectures we want to introduce satisfy the security constraints and offer specified economical results (i.e. an objective MTBUR).

The SAE document [1] proposes a continuous model for the maintenance of dual architectures. Since we consider a discrete model (because there are only observations at discrete instants), the first step was to extend the definitions of the SAE document concerning the economic and the security criterion.

The new discrete model is such that it is possible to calculate the security criterion and the economic criterion for all maintenance strategies we have to consider. Thus by testing some maintenance strategies, we determine a policy that gives the objective MTBUR.

We could improve our method by considering new real constraints. First at each end of the missions, the inspection gives the state of the system with an uncertainty. Then, there is an uncertainty about the real application of the maintenance strategy. Moreover, the system should be integrated in a real environment, with power supplies, etc.

There exists many methods and models in the literature for these extensions. Nevertheless, in the same manner as the Markov Decision Processes when we try to adapt and apply them, we have two recurrent problems: first the numerical instability. And then the problem about the exponential complexity of the Markov Graph. The new models should use different method (such that the exact or the approximate aggregation of states) to implement the data.

8. References

[1] SAE ARP5107 (Aerospace Recommended Practice). "Guidelines for time-limited-dispatch (TLD) analysis for electronic engine control systems",1996.

[2] M.L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, Wiley New-York, 1994.

[3] M. Boussemart. T. Bickard, N. Limnios. *Markov Decision Process with a Constraint on Asymptotic Failure Rate* (to be submitted).

[4] M. Boussemart. T. Bickard, N. Limnios. *Non Ergodic Markov Chain and Decision Process with a Constraint on Asymptotic Failure rate*, MMR'2000, Bordeaux.