



HAL
open science

Impact de l'évaluation de la fiabilité opérationnelle pendant la mission d'un avion

Kossi Tiassou, Karama Kanoun, Mohamed Kaâniche, Christel Seguin, Chris
Papadopoulos

► **To cite this version:**

Kossi Tiassou, Karama Kanoun, Mohamed Kaâniche, Christel Seguin, Chris Papadopoulos. Impact de l'évaluation de la fiabilité opérationnelle pendant la mission d'un avion. Congrès de Maîtrise des Risques et de sûreté de Fonctionnement (Lamda Mu 17), Oct 2012, Tours, France. 9 p. hal-00761050

HAL Id: hal-00761050

<https://hal.science/hal-00761050>

Submitted on 4 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

IMPACT DE L'ÉVALUATION DE LA FIABILITE OPERATIONNELLE PENDANT LA MISSION D'UN AVION

IMPACT OF OPERATIONAL RELIABILITY ASSESSMENT DURING AIRCRAFT MISSION

Tiassou Kossi^{1,2}, Kanoun Karama^{1,2} et
Kaâniche Mohamed^{1,2}

¹ CNRS, LAAS,
7 avenue du colonel Roche,
F-31400 Toulouse, France
² Univ de Toulouse, LAAS,
F-31400 Toulouse, France
{prénom.nom}@laas.fr

Seguin Christel

ONERA
2 Avenue Edouard Belin
31055 Toulouse,
Cedex 4, France

christel.seguin@onera.fr

Papadopoulos Chris

AIRBUS Operations Ltd.
New Filton House
Golf Course Lane,
Filton, Bristol, BS99 7AR,
United Kingdom

Chris.Papadopoulos@Airbus.com

Résumé

Lors de la conception des avions, il est courant que les constructeurs évaluent la sûreté de fonctionnement en utilisant des modèles stochastiques, mais l'évaluation de la fiabilité opérationnelle à l'aide de modèles, en ligne, reste rarement effectuée. Souvent, l'évaluation stochastique concerne la sécurité des avions ou des missions. Cet article aborde la fiabilité opérationnelle des missions d'avion, à la suite de défaillances de composants, de modifications dans l'environnement opérationnel, ou de changement concernant les possibilités de maintenance dans les diverses escales que comporte la mission. Nous décrivons comment l'évaluation de la fiabilité opérationnelle en ligne peut permettre d'ajuster une mission d'avion, en cas de changements majeurs durant sa réalisation. L'évaluation est rendue possible grâce à la construction et à la validation d'un modèle de sûreté de fonctionnement facile i) à utiliser pour la définition d'une mission initiale, et ii) à mettre à jour lors de la réalisation d'une mission, suite à l'occurrence de certains événements majeurs. Le modèle peut être construit dès la phase de conception, par des ingénieurs spécialistes en sûreté de fonctionnement, en utilisant les processus stochastiques. La mise à jour et le traitement du modèle, en phase opérationnelle, peuvent être effectués par les exploitants, qui ne sont pas nécessairement familiers avec les processus stochastiques. Nous présentons des exemples de résultats qui montrent le rôle important de la réévaluation de la fiabilité opérationnelle pendant une mission d'avion.

Summary

Dependability assessment, by system manufacturer, during aircraft design, based on stochastic modeling, is of common practice, but model based operational dependability assessment in real-time, in the way described in this paper, is seldom done. Usually, the stochastic assessment addresses aircraft or mission safety. This paper will address an aircraft mission operational reliability as resulting from component failures, environment changes, and maintenance facilities offered at the various stops involved in the mission. We will show how the on-line assessment of operational reliability will help adjust an aircraft mission, in case of major changes during the mission. The assessment is made possible thanks to the building and validation of a generic dependability model that is easily i) processed for the assignment of an initial mission, and ii) updated during mission accomplishment, following the occurrence of some specific major events. The generic model can be built as early as the design phase, by engineers who are specialist in dependability assessment, based on stochastic processes. Model update and processing, during aircraft operation, can be achieved by operators who are not necessarily familiar with stochastic processes. We will present examples of results that show the valuable role of operational dependability re-assessment during aircraft mission.

1 Introduction

Lors de la conception des avions, il est courant que les constructeurs évaluent la sûreté de fonctionnement en utilisant des modèles stochastiques. C'est très utile pour définir une architecture appropriée, satisfaisant les exigences de sûreté de fonctionnement définies pour un système donné. Cependant, actuellement, lors de l'utilisation des avions, les compagnies aériennes ne s'appuient pas sur une approche d'évaluation de fiabilité en ligne, basée sur des modèles, telle que celle décrite dans ce papier. Elles utilisent des règles déterministes prédéfinies pour prendre les décisions concernant les vols et la réaffectation des missions. Le but de notre travail est d'aider les compagnies aériennes à utiliser l'évaluation de la fiabilité avant et pendant la réalisation des missions, en plus des moyens actuels, pour assigner une mission ou pour optimiser les opérations de maintenance au cours de la réalisation des missions. Pour atteindre ce but, nous avons développé une approche de modélisation. Les principes préliminaires et les principales étapes de cette approche ont été présentés dans (Tiassou *et al.*, 2011a; Tiassou *et al.*, 2012). Dans ce papier, nous présentons différents exemples de résultats qui illustrent l'impact de la réévaluation de la fiabilité opérationnelle sur les missions.

A notre connaissance, la modélisation de la fiabilité opérationnelle des avions a été très peu abordée dans la littérature. Les travaux réalisés sont plutôt concentrés sur les aspects sécurité - voir (Kehren *et al.*, 2004; Prescott et Andrews, 2005; Ramesh *et al.*, 2008) par exemple, et la plupart des travaux publiés sur la fiabilité opérationnelle ont été réalisés à des fins d'amélioration de la conception des avions (Bineid et Fielding, 2003; Saintis *et al.*, 2009), à l'exception de (Tiassou *et al.*, 2011b; Tiassou *et al.*, 2011a). Dans (Sachon et Paté-Cornell, 2000), la problématique de l'estimation des retards et de la sécurité des vols en rapport avec les activités de maintenance a été abordée. Un modèle probabiliste d'analyse de risque a été développé afin de quantifier l'effet de la politique de maintenance sur l'opérabilité des avions. Une approche d'aide à la décision, concernant la planification des activités de maintenance, est présentée en (Papakostas *et al.*, 2010). Les auteurs proposent une méthode pour planifier la maintenance en tenant compte des critères d'optimisation comme le coût, la durée de vie résiduelle et les risques opérationnels. Le travail effectué ne concerne pas l'évaluation de fiabilité, mais utilise plutôt la mesure de fiabilité comme entrée. Dans (Ahmadi et Soderholm, 2008), les conséquences opérationnelles des défaillances système ont été analysées en utilisant les arbres d'événements. L'article analyse les éventuelles conséquences des défaillances en tenant compte de la

phase de vol durant laquelle elles ont eu lieu. Une approche de modélisation basée sur l'arbre de défaillance du système avion est présentée dans (Saintis *et al.*, 2009), en considérant seulement les événements liés à l'autorisation de vol, sans aborder les conséquences des défaillances en vol.

(Chew *et al.*, 2008; Mura *et al.*, 1999) abordent la modélisation de la fiabilité des systèmes en considérant des missions structurées de phases ayant des durées déterministes. (Mura *et al.*, 1999) montre que, sous certaines conditions, le modèle proposé peut être traité en utilisant une méthode analytique. (Chew *et al.*, 2008) aborde le problème dans le cadre de la mise en œuvre du concept de MFOP (Maintenance-Free Operating Periods), qui caractérise des périodes durant lesquelles le système est utilisé sans possibilité de maintenance. Le modèle développé est résolu par simulation.

De tous ces travaux, aucun ne vise directement la modélisation de la fiabilité des avions en phase opérationnelle. Les travaux les plus proches (Ahmadi et Soderholm, 2008; Saintis *et al.*, 2009) sont effectués pour une analyse globale de la fiabilité opérationnelle, portant sur toute la période de vie du système. Ces travaux se sont basés sur des arbres de fautes et des arbres d'événements. Par ailleurs, à notre connaissance, notre travail est le seul présentant des résultats permettant d'illustrer l'estimation et la mise à jour en ligne de l'évolution de la fiabilité opérationnelle des avions.

Cet article aborde la fiabilité opérationnelle des avions en utilisant des modèles stochastiques à espace d'état. Le modèle est essentiellement utilisé pour évaluer la probabilité d'accomplir la mission sans interruption jusqu'à une date donnée, en tenant compte des événements récents. La probabilité estimée permettra de déterminer si une action corrective doit être initiée ou non.

Nous présenterons premièrement le contexte et les objectifs de l'évaluation. Ensuite, nous présenterons brièvement l'approche de modélisation, ainsi qu'une illustration du type de modèles qui peuvent être construits. Nous donnerons enfin des exemples de résultats d'évaluation et de leur utilisation en temps réel.

2 Contexte de l'évaluation et objectifs

Une mission d'avion consiste à effectuer une liste prédéfinie de vols sous certaines conditions opérationnelles et de maintenance. La réalisation de la mission est telle que chaque vol est suivi par une escale où l'avion est apprêté pour le prochain vol. A chaque escale, l'avion est inspecté et les anomalies observées lors du vol précédent sont examinées. Si une défaillance d'un équipement est détectée, une décision doit être prise quant à l'aptitude à effectuer le prochain vol. Le commandant de bord et les agents de maintenance se réfèrent à un document (appelé Minimum Equipment List) où les composants sont répertoriés avec le statut Go, Goif ou Nogo.

Le statut Go est le cas où l'avion peut voler avec le composant défaillant. Il est à noter que même dans ce cas, il faut faire attention au comportement futur de l'avion puisqu'une nouvelle défaillance pourrait conduire à l'interruption du vol.

Pour le statut Goif, le vol peut être effectué à condition qu'un certain nombre d'autres équipements soient opérationnels et que certaines procédures opérationnelles ou de maintenance soient possibles :

- Goif-o: Des procédures opérationnelles doivent être effectuées ou réalisables pour pouvoir effectuer le vol. Il s'agit essentiellement d'une limitation des fonctionnalités disponibles pendant le vol.
- Goif-m: Des dispositions concernant la maintenance doivent être prises dans un délai acceptable prédéfini pour régler le problème ; par exemple, la défaillance doit être réparée dans un délai de dix jours.

Le statut Nogo empêche l'avion de voler. Dans ce cas, la défaillance doit être réparée avant tout vol.

Le vol est autorisé s'il n'y a pas de Nogo et si toutes les conditions Goif sont réalisables. Lorsqu'il est autorisé, il peut être interrompu ou dérouter si la capacité de avion est considérablement dégradée. Des procédures décrites dans le manuel de vol servent de support pour déterminer si le vol doit être dérouter ou non.

Les situations indésirables pendant la réalisation d'une mission entraînent des interruptions de mission telles que les retards de vol, les annulations, les demi-tours et les déroutements (Ahmadi et Soderholm, 2008; Saintis *et al.*, 2009). Notre travail prend en compte principalement les interruptions causées par des défaillances système ou par l'incapacité d'effectuer la maintenance corrective dans un délai acceptable.

2.1 Rôle de l'évaluation de la fiabilité

L'objectif est de pouvoir évaluer, au cours des opérations d'un avion, son aptitude à satisfaire les exigences opérationnelles suite à un événement, et d'initier des actions correctives afin d'éviter les situations indésirables. L'évaluation est à utiliser pour la planification des missions et pendant leur réalisation.

Pour planifier une mission, la mesure de fiabilité est utilisée pour estimer la durée pendant laquelle l'avion peut voler sans qu'une situation indésirable ne se produise. Cela permettra de déterminer le type de profil de mission à assigner à l'avion.

Une fois qu'une mission est assignée à l'avion, l'évaluation est utilisée au cours de sa réalisation, à la fois au sol et en vol, pour évaluer la capacité à poursuivre avec succès le reste de la mission, ou le réadapter si nécessaire, en cas de changements majeurs. Pour ce faire, le modèle est mis à jour avec les informations sur le nouvel état de l'avion et sur son environnement, avant l'évaluation.

Pendant le vol (ou au sol, lors de l'inspection de l'avion), l'évaluation de la fiabilité opérationnelle est effectuée, après l'occurrence (ou la détection) d'événements majeurs qui peuvent affecter l'exploitabilité, pour fournir une indication sur la fiabilité durant la partie restante de la mission. Le résultat peut être utilisé par le centre de contrôle des opérations, pour aider dans la décision de continuer la mission ou de revoir la mission initialement planifiée.

En cas de décision de dérouter le vol, l'évaluation peut être utilisée pour aider à déterminer lequel des aéroports de déroutement candidats, a suffisamment de moyens pour remettre l'avion en état opérationnel.

Enfin, le résultat peut aider à choisir le programme de maintenance ou le programme d'opération le plus approprié afin d'améliorer l'aptitude à réaliser toute la mission. Pour ce faire, différentes stratégies de maintenance peuvent être comparées en considérant différentes alternatives pour effectuer la maintenance des composants. La meilleure stratégie est alors choisie en fonction de la probabilité estimée, d'accomplir la mission sans interruption.

2.2 Principaux changements devant être pris en compte

Comme le système sera surveillé en permanence, des informations de diagnostic et de pronostic notifieront les changements majeurs concernant les composants du système, leur état fonctionnel, leur défaillance, les taux d'occurrence et les distributions de probabilités associés aux événements de défaillance et de réparation. Par exemple, la défaillance d'un calculateur peut initialement suivre la loi exponentielle et le pronostic peut indiquer lors de la réalisation d'une mission, une augmentation du risque de défaillance, suggérant une distribution suivant une loi de Weibull. Comme ces changements peuvent affecter la

fiabilité de mission, initialement estimée, le modèle doit être mis à jour avec la nouvelle distribution, afin de réévaluer la fiabilité. Nous avons identifié trois types de changements majeurs qui pourraient avoir lieu lors de la réalisation d'une mission, résumés ci-après.

C1: Les changements concernant l'état des composants du système : Ceux ci correspondent aux cas où par exemple un composant système a défailli lors de la réalisation de la mission (nous supposons que cette défaillance n'impacte pas la sécurité, sinon la mission est interrompue). Même si un tel événement a été pris en compte dans le modèle stochastique, entreprendre de nouveaux vols peut avoir un impact sur l'opérabilité.

C2: Changements concernant les taux de défaillance des composants : Ceux ci concernent principalement les cas où de nouveaux taux de défaillance ou de nouvelles distributions ont été pronostiqués pour les composants du système, pendant la réalisation de la mission.

C3: Les changements dans le profil de mission : Une mission est caractérisée par le nombre de vols par jour, le nombre de jours, et la durée de chaque vol. Suite à des événements extérieurs comme les conditions météorologiques ou la défaillance d'autres avions, le nombre de vols et les destinations de vol peuvent changer. Cela peut influencer sur le nombre et la durée des vols. Changer le profil de mission implique également des changements dans les possibilités de maintenance disponibles aux différentes escales (ou destinations), ainsi que dans le temps moyen de réparation des composants défectueux ou la distribution du temps de réparation elle-même.

Les changements de types C1 et C2 sont fournis par le diagnostic et le pronostic, tandis que les changements de type C3 sont régis par les agents d'exploitation de la compagnie aérienne.

3 Approche de modélisation

Pour résumer, notre objectif est de rendre possible l'évaluation de la fiabilité opérationnelle des avions lors de la réalisation de leurs missions. Le modèle aidera à assigner une mission qui est en conformité avec les états des composants de l'avion et les conditions pouvant l'impacter. Durant la réalisation de la mission, à l'occurrence de l'un des changements listés au paragraphe précédent, la fiabilité opérationnelle est réévaluée pour mesurer l'impact du nouvel état sur la réussite de la mission. En pratique, un changement conduit à la mise à jour du modèle de fiabilité. Le modèle global de fiabilité doit être conçu de façon à effectuer de façon aisée et efficace son ajustement, sa mise à jour, et son traitement. Par ailleurs, comme le modèle doit être utilisé au moment de l'exploitation de l'avion, l'ajustement et la mise à jour ne devraient pas nécessiter la présence de spécialistes de modélisation. Il devrait être possible d'ajuster ou de mettre à jour le modèle de l'extérieur, sans nécessiter une connaissance profonde du modèle.

En conséquence, notre approche consiste à construire et valider un modèle de fiabilité initial dont les informations opérationnelles essentielles peuvent être saisies et validées via une interface dédiée. Par ailleurs, l'ajustement et la mise à jour du modèle ne devraient pas nécessiter la connaissance de la technique de modélisation sous-jacente, ni le formalisme utilisé. En effet, le modèle global initial, incluant les détails sur les composants du système et les fonctions, leurs interactions, et leur comportement stochastique, ne peut être construit que par le constructeur de l'avion et les spécialistes de la maintenance, qui ne seront pas nécessairement impliqués dans l'ajustement et la mise à jour du modèle en opération.

Notre travail a donc deux facettes complémentaires, non indépendantes, liées respectivement à i) la construction du modèle initial de fiabilité par les constructeurs ou spécialistes de la maintenance des équipements, et à ii) son ajustement et sa mise à jour pour l'adapter aux conditions courantes d'exploitation. La première facette est dédiée à la définition d'une approche de modélisation, basée sur les processus stochastiques, dans laquelle certains paramètres devraient être configurables de l'extérieur; cette approche est détaillée dans (Tiassou *et al.*, 2012). La deuxième facette est plus orientée vers la façon d'utiliser ce modèle en phase d'exploitation et comment obtenir des résultats utiles.

Dans cet article, nous mettons l'accent sur la seconde facette et montrons comment utiliser les résultats de l'évaluation lors d'une mission, pour la gérer ainsi que les activités de maintenance associées.

L'approche de mise à jour du modèle consiste à utiliser des fichiers de configuration pouvant être mis à jour avec l'état courant de l'avion et de la mission. Un gestionnaire d'évaluation, composé d'un opérateur humain aidé par un algorithme automatique pour vérifier la cohérence, met à jour les fichiers de configuration et lance le traitement du modèle. Le modèle initial, qui n'intégrait pas les paramètres de quantification, ni une mission complète, est transformé en un modèle complet de sûreté de fonctionnement, après l'intégration de l'information fournie dans les fichiers de configuration. Le traitement du modèle obtenu fournit la mesure de fiabilité de mission. La figure 1 montre le scénario de mise à jour.

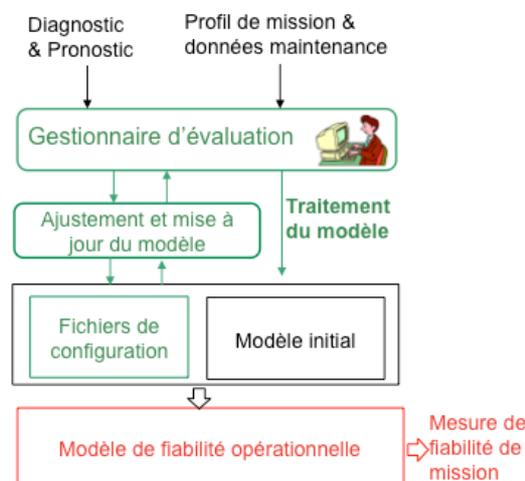


Figure 1. Mise à jour du modèle

Pour mettre à jour les fichiers de configuration, le gestionnaire d'évaluation se base sur : i) des modules de diagnostic et de pronostic, qui sont exécutés en temps réel, soit automatiquement grâce à des mécanismes intégrés dans les systèmes de contrôle de l'avion ou soit par l'équipage, et sur ii) les plans de vol.

Il convient de mentionner que la mise à jour et le traitement du modèle peuvent être effectués quand l'avion est encore en vol, sans attendre son atterrissage, afin d'obtenir dès que possible les nouveaux résultats d'évaluation.

Enfin, l'interface de paramétrage et de mise à jour du modèle doit être conviviale et ne devrait pas dépendre du formalisme de modélisation sous-jacent.

Il est à noter que la fréquence de mise à jour du modèle dépendra étroitement du contexte opérationnel et de la fréquence à laquelle une variation significative des paramètres du modèle est observée. La décision peut être prise automatiquement, par exemple, quand un seuil prédéfini de variation de certains paramètres est observé, ou sur une base régulière (par exemple, à la fin de chaque journée).

3.1 Le formalisme de modélisation

Le modèle peut être construit en utilisant les formalismes de modélisation de fiabilité classiques tels que les réseaux de Petri et leurs extensions, les réseaux d'activités stochastiques (SANs) ou AltaRica. La seule exigence est qu'une fois le modèle construit, il puisse être facilement ajusté de l'extérieur et traité efficacement. Pour l'utilisation finale, les modèles initiaux seront développés à l'aide du langage AltaRica (Arnold *et al.*, 1999; Boiteau *et al.*, 2006; Kehren *et al.*, 2004), et le module de traitement optimisé du modèle, qui est en cours de développement, est propriétaire. L'algorithme pour le gestionnaire d'évaluation et l'interface du modèle sont aussi propriétaires et sont encore en développement.

Pour obtenir des résultats nous permettant de vérifier la validité de la démarche, avant la fin de la mise en œuvre de tous les modules propriétaires, nous avons utilisé les outils existants pour construire et traiter les modèles. La mesure calculée est la fiabilité de mission. Nous avons utilisé d'une part AltaRica et d'autre part les SANs (J. F. Meyer *et al.*, 1985; W. Sanders et J. Meyer, 2001) pour construire et valider les modèles. Il convient de mentionner que les deux formalismes sont équivalents en terme d'expressivité. Le modèle présenté dans ce papier est basé sur les SANs. Il a été traité en utilisant l'outil Möbius (Daly *et al.*, 2000).

3.2 Fiabilité de mission

L'avion doit satisfaire des exigences pour être autorisé à voler ainsi que des exigences spécifiques en vol.

On distingue :

- les exigences minimales (Min_Sys_Req), indépendantes des profils de mission, qui doivent être satisfaites quelque soit le vol à effectuer.
- les exigences (Mission_Req) qui sont spécifiques au profil de mission.

L'évaluation est basée sur la satisfaction de ces exigences. Dans ce papier, nous nous concentrons sur la mesure de la fiabilité de mission, MR, définie comme la probabilité de réaliser la mission sans interruption. Elle est évaluée par rapport à Min_Sys_Req et Mission_Req pour déterminer si une action préventive doit être initiée ou non.

Il convient de mentionner que l'ajustement et la mise à jour du modèle concernent uniquement Mission_Req. Les Min_Sys_Req sont prises en compte dans le modèle initial.

3.3 Le modèle initial

Afin de faciliter la mise à jour du modèle, le modèle initial est structuré en deux couches principales, correspondant respectivement à i) la couche système (composé des modèles de sous-systèmes et les Min_Sys_Req), et ii) la couche de la mission (intégrant la description d'une mission, avec les possibilités de maintenance à chaque escale, et les Mission_Req).

4 Exemples de sous-système et de modèle

Afin d'illustrer les résultats, nous avons choisi un sous-système avion, le système de contrôle de la gouverne de direction. Il est composé (voir Figure 2) de trois calculateurs primaires (P1, P2, P3), un calculateur secondaire S1, trois servocommandes (ServoCtrl_G, ServoCtrl_B et ServoCtrl_Y), un module de contrôle secours (BCM) et deux composants (BPS_B et BPS_Y) permettant d'alimenter le module de secours en énergie.

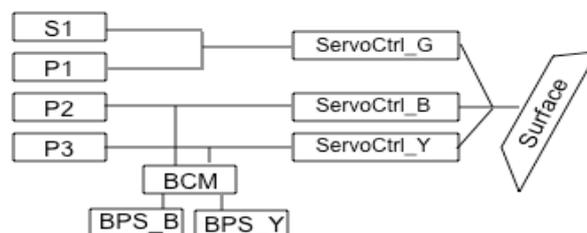


Figure 2. La structure du sous-système

Les calculateurs sont connectés aux servocommandes, qui font mouvoir la surface. S1 et P1 sont connectés à ServoCtrl_G, P2 à ServoCtrl_B, et P3 à ServoCtrl_Y. La connexion entre un calculateur et une servocommande forme une ligne de commande qui peut agir sur la surface. On a :

- PL1 : formée par P1 et ServoCtrl_G,
- PL2 : formée par P2 et ServoCtrl_B,
- PL3 : formée par P3 et ServoCtrl_Y,
- SL : formée par S1 et ServoCtrl_G.

Il y a également une ligne de commande secours (BCL), basée sur BCM, BPS_B, BPS_Y, ServoCtrl_Y et ServoCtrl_B.

Initialement S1, le module de commande secours BCM, BPS_B et BPS_Y sont inhibés, et la surface est contrôlée par les trois lignes de commande primaire (PL1, PL2, PL3). Lorsque les trois lignes de commande primaire sont défaillantes, S1 est activé et le système passe en SL. Si cette dernière devient également défaillante, les composants BCM, BPS_B et BPS_Y sont activés et BCL assure la commande.

Exigences opérationnelles (Min_Sys_Req) : Selon (MMEL, 2008), la perte de P2, ServoCtrl_G, ServoCtrl_Y, ServoCtrl_B, BCM, BPS_B ou BPS_Y conduit à un état Nogo. P1, P3 et S1 sont Goif avec comme conditions Goif énoncées respectivement aux sections MMEL 27-93-01-1, MMEL 27-93-01-3 et MMEL 27-94-01-1 du document. Les conditions résultantes de ces sections sont respectivement:

- $(P1 = ok) \vee (S1 = ok \wedge P3 = ok)$;
- $(P3 = ok) \vee (S1 = ok \wedge P1 = ok)$;
- $(S1 = ok) \vee (P1 = ok \wedge P2 = ok \wedge P3 = ok)$.

Dans les trois cas, le composant doit être réparé dans un délai de 10 jours.

4.1 Modélisation de la mission et du sous-système

La figure 3 donne une vue de haut niveau du modèle, qui est construit en utilisant le formalisme SAN. Nous décrivons seulement le modèle de la couche mission et sa connexion avec le modèle de la couche système ; une description plus détaillée peut être trouvée dans (Tiassou *et al.*, 2011a). La connexion est réalisée grâce à la modélisation des exigences système basées sur les états des lignes de commande PL1, PL2, PL3, SL1 et BCL, décrites dans les sous modèles correspondants. Le marquage de la place *Min_Sys_Req_fulfillment* est mis à jour par le tir des activités instantanées *Fulfilled* et *Not_Fulfilled*, suite aux changements d'état des sous-systèmes. Les conditions correspondantes sont encodées dans les portes d'entrée *IGN* et *IGFul*. Il est à noter que dans cet exemple, nous ne considérons pas les exigences spécifiques au profil de mission qui pourraient être associés à chaque vol.

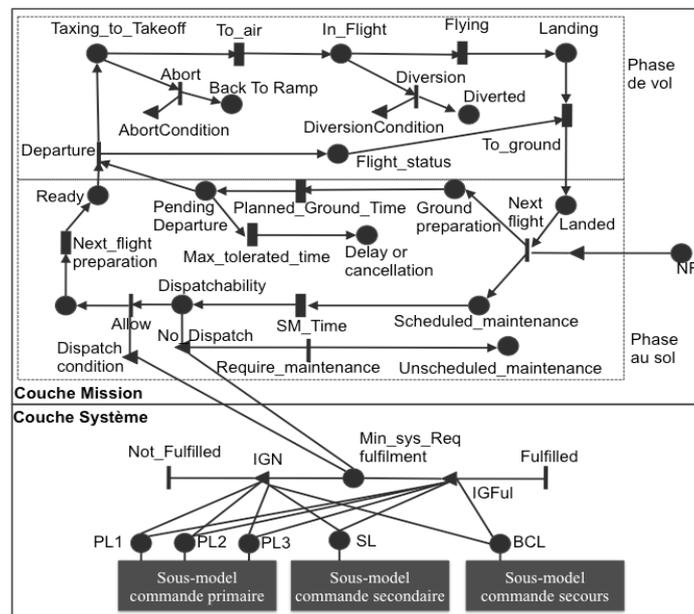


Figure 3. Aperçu du modèle

Considérant le modèle de la couche mission, il est composé de deux parties. La partie supérieure représente un vol et la partie inférieure représente les activités au sol, lors d'une escale. Un vol est représenté par trois phases *Taxing_to_Takeoff*, *In_Flight* et *Landing*. Pendant le décollage *Taxing_to_takeOff* le vol peut être annulé et il peut être dérouté pendant la phase *In_Flight*. Les portes d'entrée *AbortCondition* et *DiversionCondition* définissent les conditions conduisant à l'occurrence de ces interruptions.

Le modèle de la phase au sol décrit la préparation pour le prochain vol. Le début de la préparation pour le prochain vol est représenté par le marquage des places *Ground_Preparation* et *Scheduled_Maintenance*, indiquant que la phase au sol a commencé avec les tâches de maintenance prévues d'avance (contrôles de routine, par exemple). Lorsque ces tâches sont terminées (franchissement de l'activité *SM_Time*), la place *Dispatchability* est marquée. L'activité instantanée *Allow* peut alors être franchie si les exigences pour autoriser le vol, exprimées dans *Dispatch_Condition*, sont satisfaites. Sinon l'activité instantanée *Require_Maintenance* est tirée si l'action corrective nécessite des tâches de maintenance (indiqué par la condition *No_Dispatch*). La place *Dispatchability* reste marquée jusqu'à ce que l'action corrective réussisse (le prédicat de *Dispatch_Condition* devient vrai) et le vol est autorisé. Dans la représentation actuelle, la satisfaction des conditions pour autoriser le vol consiste à tester le marquage de la place *Min_Sys_Req_fulfillment*. Jusque-là, le temps prévu pour la phase au sol pourrait être dépassé (franchissement de l'activité *Planned_Ground_Time* mettant le jeton dans place *Pending_Departure*) et le délai de retard maximum tolérable (*Max_tolerated_time*) pourrait être dépassé. Un retard ou une annulation peut ainsi advenir. L'activité temporisée *Next_flight_preparation* représente les autres activités (embarquement des passagers, traitement des bagages ...) qui peuvent consommer du temps, occasionnant un retard. La place *NF* (à droite) est une place étendue représentant la liste des vols à effectuer. La porte d'entrée reliée à cette place indique si il y a un prochain vol à effectuer ou non (fin de la mission ou non). Il est à noter que différentes distributions peuvent être spécifiées pour différents vols en ce qui concerne les activités temporisées, définies dans le modèle au niveau mission.

5 Résultats d'évaluation

Afin de montrer l'impact des changements introduits dans la section 2.2, nous avons défini une mission initiale typique composée de quatre vols identiques par jour, pendant une semaine, et nous avons évalué la fiabilité de mission, MR, en fonction du temps calendaire t . Nous supposons que, tant que MR est supérieure à une valeur donnée, dénommée MMRR, la mission peut être poursuivie. MMRR est fixée par l'exploitant de l'avion, en accord avec le constructeur de l'avion. Pour les exemples présentés dans cette section, nous considérons $MMRR = 0,975$. Il convient de mentionner qu'afin de préserver le secret industriel, les valeurs utilisées ici ont été choisies pour former un ensemble cohérent, sans être issues de l'observation en exploitation du système considéré.

Nous évaluerons dans un premier temps l'impact d'une défaillance d'un composant sur la fiabilité d'une mission, et nous montrerons comment ces résultats peuvent être utilisés en temps réel pour planifier la maintenance. Nous montrerons ensuite l'impact des changements dans les distributions des délais d'occurrence des défaillances (de l'exponentiel à Weibull) avant d'analyser l'impact des changements de profil de mission.

5.1 Défaillance d'un composant

La seule défaillance de P1 ou de S1 n'empêche pas la réalisation de la mission. Cependant, la défaillance simultanée des deux composants peut conduire à une interruption de la mission.

• Défaillance du calculateur primaire P1

La courbe 0 de la figure 4 montre la fiabilité de mission, MR, telle qu'évaluée avant la réalisation de la mission, en supposant que tous les composants sont opérationnels au début. On peut voir qu'à la fin de la mission, MR reste supérieure à MMRR.

La Courbe X, $X \in \{2,4,5\}$, correspond au cas où P1 a été diagnostiqué comme défaillant à la fin de la journée X. MR est donc réévaluée en considérant i) comme origine ($t = 0$), le jour $X+1$, et ii) que P1 est défaillant à l'instant $t = 0$. MR commence donc par la valeur 1 à chaque ré-évaluation, puisque l'état global du système, au moment où l'exécution du modèle est effectuée, est un état opérationnel.

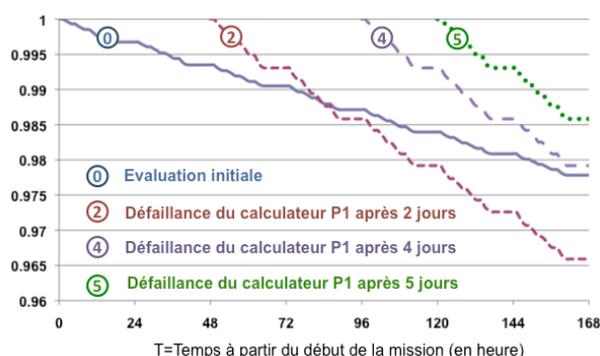


Figure 4 Impact de la défaillance de P1 durant la mission

Le pire cas correspond à $X = 2$, puisque MR est inférieure à MMRR à partir du 5^e jour. Les courbes 4 et 5 montrent que, si la défaillance de P1 est diagnostiquée après le 4^e jour, la mission peut être poursuivie sans maintenance jusqu'à sa fin. La défaillance de P1 est dès lors réparée.

La courbe 2 montre que l'on doit envisager la maintenance de P1 pour pouvoir satisfaire MMRR, au cas où une défaillance de P1 survient durant les deux premiers jours de mission. Basé sur ce résultat, la figure 5 montre l'impact de la maintenance de P1, entreprise respectivement au soir du 3^e jour (2a), du 4^e jour (2b) ou du 5^e jour (2c). Les courbes 2a et 2b montrent que MR est toujours au-dessus de MMRR pour tout le reste de la mission, tandis que le scénario 2c (maintenance au soir du 5^e jour) conduit à une fiabilité MR plus faible que MMRR. Les courbes 0 et 2 sont les mêmes sur les deux figures.

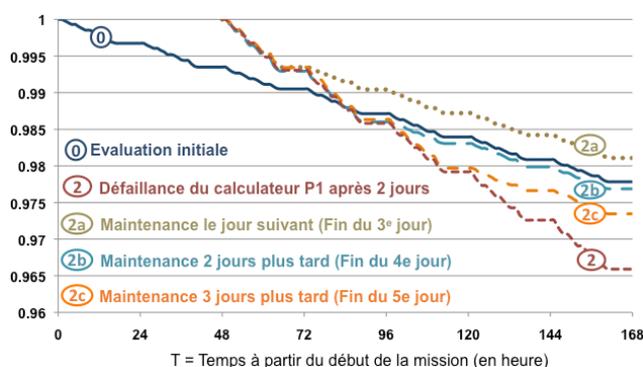


Figure 5 Impact de scénarios de maintenance

• Défaillance du calculateur secondaire S1

La figure 6 montre MR en considérant la défaillance du calculateur secondaire S1 pendant la réalisation de la mission. Ces courbes sont à comparer à celles de la figure 4. Elles montrent que S1 a plus d'impact sur la fiabilité du reste de la mission que

P1. Cela est dû au fait que le taux de défaillance de P1 est plus élevé que le taux de défaillance S1. Les exigences sont telles que l'un des calculateurs, P1 ou S1, doit être opérationnel pour pouvoir réaliser la mission. Par conséquent, le risque d'interrompre la mission est plus élevé lorsque S1 est défaillant que lorsque P1 est défaillant. Il est à noter que si S1 défaille à la fin de la 4^e journée (96 heures), la valeur de la fiabilité à la fin de la mission reste la même que l'estimation faite au début pour la mission tout entière.

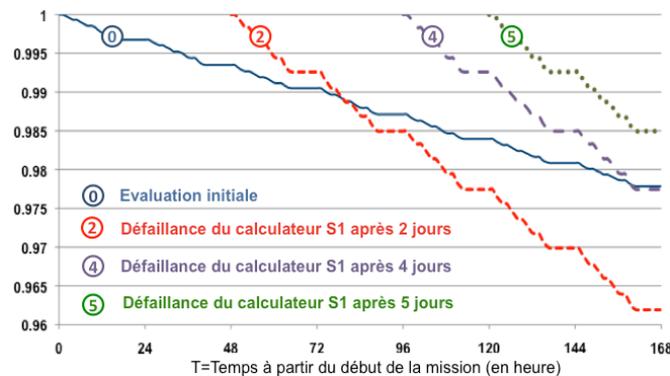


Figure 6 Impact de la défaillance de S1 durant la mission

5.2 Changement de distribution de défaillance

Le calculateur primaire P2 doit nécessairement être opérationnel pour autoriser l'avion à voler. Supposons qu'une distribution exponentielle a été d'abord attribuée à son processus de défaillance, avec un temps moyen jusqu'à défaillance MTTF = 5000 heures de vol. Si le module de pronostic notifie une autre distribution au cours de la mission, la fiabilité de mission devrait être réévaluée.

Supposons que la nouvelle distribution est une distribution de Weibull, avec comme paramètre de forme $\alpha = 2,5$ ($\alpha > 1$ représente un taux de défaillance croissant) et comme paramètre d'échelle $\beta = 5635$, conditionnée par un temps de fonctionnement déjà cumulé $T_e = 5000$. La figure 7 montre l'impact du changement de la distribution, de l'exponentiel (courbe 0) à Weibull (courbes 2 à 5). Les courbes X = 2, 4, 5 correspondent à un pronostic émis au jour X de la mission. Il convient de mentionner que ces courbes ont la même pente, mais décalée dans le temps ; ce qui n'est pas surprenant du fait qu'ils ont été obtenus à partir du même modèle, avec les mêmes états initiaux des composants et les mêmes distributions. La diminution rapide de la fiabilité des courbes X par rapport à la courbe 0 résulte de l'augmentation du taux de défaillance. La courbe 2, en particulier montre qu'avec une distribution de Weibull, MR est en dessous de MMRR après 5 jours. Les courbes 4 et 5 montrent que si le pronostic lié au changement de distribution a lieu à la fin du quatrième jour, MR est meilleure que la valeur initialement prédite.

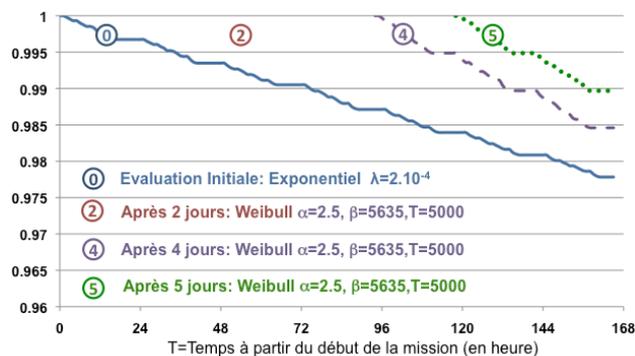


Figure 7 Impact de la distribution de défaillance

5.3 Changement dans le profil de mission

Comme les opérations dépendent de divers facteurs externes, il peut arriver qu'on change le profil de la mission initiale, afin de gérer certains événements imprévus qui n'ont pas nécessairement affecté directement l'avion lui-même. Par exemple, on peut avoir à réaliser un ou plusieurs vols supplémentaires qui ont été initialement prévus pour un autre avion. De tels changements exigent une réévaluation de la fiabilité de la mission. La figure 8 illustre un cas où, à partir de la deuxième journée, un vol est ajouté au programme journalier, faisant passer le nombre de vols à réaliser par jour de 4 à 5. On peut voir que les valeurs de fiabilité pour le nouveau profil de mission, sont devenues inférieures aux valeurs correspondant au profil initial, à partir du point 144 (au bout de 6 jours) de l'axe des temps. Cependant, l'exigence minimale de fiabilité (MMRR= 0,975) est toujours satisfaite.

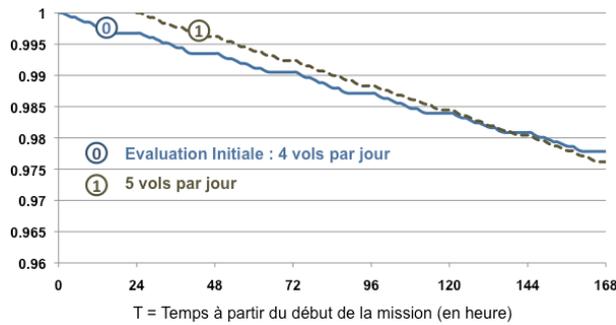


Figure 8 Changement de la mission : de 4 vols par jour à 5 par jour

Dans le cas de la figure 8, tous les vols ont une durée de 3 heures. La courbe 1a de la figure 9 montre un cas où la mission change à la deuxième journée, de 4 vols (3 heures chacun) par jour, à 2 vols d'une durée de 9 heures chacun. Ce changement conduit à une diminution de la fiabilité par rapport aux prévisions initiales. La fiabilité de la mission devient inférieure à MMRR.

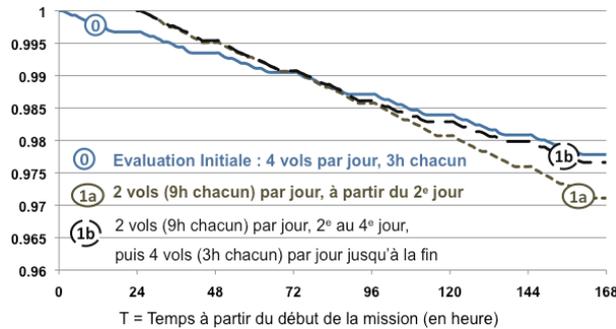


Figure 9 Changement et ajustement de la mission

On peut envisager un ajustement du profil résultant de ce changement pour améliorer la fiabilité de la mission. Une possibilité d'ajustement pourrait correspondre au profil suivant : 2 vols (9 heures chacun) par jour, du 2^e jour au 4^e jour, puis 4 vols par jour à partir du 5^e jour jusqu'à la fin. La fiabilité du profil de mission obtenu est donnée par la courbe 1b de la figure 9. La fiabilité du nouveau profil de mission devient approximativement la même que celle du profil initialement défini, et le seuil MMRR est de nouveau respecté.

6 Conclusion

Ce papier a présenté une approche de modélisation et des exemples illustrant comment les modèles stochastiques de sûreté de fonctionnement peuvent être utilisés : i) pour évaluer la fiabilité opérationnelle des avions au cours de leur mission et ii) pour ajuster les évaluations lorsque des changements significatifs, affectant l'état des composants avions, l'environnement ou le profil de la mission, se produisent. Un prototype mettant en œuvre l'approche proposée est actuellement en cours de développement. L'interaction humaine avec l'outil consistera principalement en la spécification des paramètres de mise à jour qui caractérisent le profil de la mission (nombre de vols, durée de vol et la période au sol, les stratégies de maintenance, etc.) Les paramètres du modèle liés aux défaillances des composants et les durées de maintenance seront mis à jour en utilisant les informations fournies par des modules de diagnostic et de pronostic, qui surveillent l'état de l'avion en temps réel, et des informations provenant de la maintenance.

Les résultats fournis par l'outil, qui sont illustrés à travers les exemples numériques présentés dans ce papier, visent à donner un aperçu de l'impact des changements signalés, sur la fiabilité opérationnelle du reste de temps de mission. Ils devraient être utiles pour ajuster la mission si nécessaire. A notre connaissance, il n'y a pas d'outil similaire, existant, qui fournit de telles informations.

Références

- Ahmadi A., Soderholm P., 2008. Assessment of Operational Consequences of Aircraft Failures: Using Event Tree Analysis. Proc. 2008 IEEE Aerospace Conference, 1–14. Big Sky, MT, USA.
- Arnold A., Point G., Griffault A., Rauzy Antoine, 1999. The AltaRica formalism for describing concurrent systems. *Fundamenta Informaticae*, 40, 109–124.
- Bineid M., Fielding J.P., 2003. Development of a civil aircraft dispatch reliability prediction methodology. *Aircraft Engineering and Aerospace Technology*, 75, 588-594.
- Boiteau M., Dutuit Y., Rauzy A., Signoret J.-P., 2006. The AltaRica Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System. *Reliability Engineering and System Safety*, 91, 747–755.
- Chew S.P., Dunnett S.J., Andrews J.D., 2008. Phased mission modelling of systems with maintenance-free operating periods using simulated Petri nets. *Reliability Engineering & System Safety*, 93, 980 - 994.
- Daly D., Deavours D.D., Doyle J.M., Webster P.G., Sanders W.H., 2000. Möbius: An Extensible Tool for Performance and Dependability Modeling. Proc. 11th International Conference on Computer Performance Evaluation: Modelling Techniques and Tools, 332–336. TOOLS '00. London, UK, Springer-Verlag.

- Kehren C. *et al.*, 2004. Advanced simulation capabilities for Multi-systems with Altarica. Proc. 22nd International System Safety Conference, 489-498, International System Safety Society.
- Meyer J.F., Movaghar A., Sanders W.H., 1985. Stochastic Activity Networks: Structure, Behavior, and Application. Proc. International Workshop on Timed Petri Nets, 106-115. Washington, DC, USA, IEEE Computer Society.
- MMEL, 2008. Master Minimum Equipment List - AIRBUS A-340-200/300. Consultable : <http://fsims.faa.gov/wdocs/mmel/a340-200-300original05-30-08.pdf> [Consulté 10 avril 2012].
- Mura I., Bondavalli A., Zang X., Trivedi K.S., 1999. Dependability Modeling and Evaluation of Phased Mission Systems: A DSPN Approach. Proc. Conference on Dependable Computing for Critical Applications, 319-337. DCCA '99. Washington, DC, USA, IEEE Computer Society.
- Papakostas N., Papachatzakis P., Xanthakis V., Mourtzis D., Chryssolouris G., 2010. An approach to operational aircraft maintenance planning. Decision Support Systems, 48, 604-612.
- Prescott D.R., Andrews J.D., 2005. Aircraft safety modeling for time-limited dispatch. Proc. Annual Reliability and Maintainability Symposium, 139-145. Alexandria, VA, USA.
- Ramesh A., Twigg D., Sharma T., 2008. Advanced methodologies for average probability calculation for aerospace systems. Proc. 26th international congress of the aeronautical sciences, 1-9. Anchorage - Alaska, USA. Consultable : http://www.icas.org/ICAS_ARCHIVE_CD1998-2010/ICAS2008/PAPERS/332.PDF.
- Sachon M., Paté-Cornell E., 2000. Delays and safety in airline maintenance. Reliability Engineering & System Safety, 67, 301-309.
- Saintis L., Hugues E., Bes C., Mongeau M., 2009. Computing in-service aircraft reliability. Int. J. Rel. Qual. Saf. Eng., 16, 91-116.
- Sanders W., Meyer J., 2001. Stochastic Activity Networks: Formal Definitions and Concepts. Lectures on Formal Methods and Performance Analysis, 315-343. Lecture Notes in Computer Science, Springer Berlin / Heidelberg.
- Tiassou K., Kanoun K., Kaâniche M., Seguin Christel, Papadopoulos C., 2012. Online model adaptation for aircraft operational reliability assessment. ERTS2 2012, Toulouse.
- Tiassou K., Kanoun K., Kaâniche Mohamed, Seguin Christel, Papadopoulos C., 2011a. Modeling aircraft operational reliability. Proc. 30th international conference on Computer safety, reliability, and security, 157-170. SAFECOMP'11. Naples, Italy, Springer-Verlag, ISBN 978-3-642-24269-4.
- Tiassou K., Kanoun K., Kaâniche Mohamed, Seguin C., Papadopoulos C., 2011b. Operational reliability of an aircraft with adaptive missions. Proc. 13th European Workshop on Dependable Computing - EWDC '11, 9-14. Pisa, Italy.