| Titre de la thèse : | Thématique : |
|---|---|
| **Vérification formelle de contraintes de vol** | ISL |
| Encadrant ONERA :<br>Romain Kervarc (MIDL) | Directeur de thèse :<br>Ch. Choppy (U. Paris XIII – LIPN)<br>ou L. Petrucci (U. Paris XIII – LIPN) |

## Résumé du sujet et démarche envisagée

Pour faire face à l'augmentation du trafic aérien général, diverses pistes sont proposées visant à enrichir de davantage de données les échanges entre contrôle aérien et aéronefs. Cett approche permet de donner aux aéronefs une marge de manœuvre à l'intérieur de contraintes fournies par le contrôle, et à ce dernier de se focaliser sur sa mission de régulation et de supervision d'ensemble, ce qui allège sa charge globale. Un tel exemple de système plus distribué a été proposé à l'ONERA sous la forme de contrats 4D [1], i.e. des trajectoires d'avion délimitée dans l'espace et dans le temps, respectant un certain nombre de contraintes (spatiales, temporelles, internes ou externes).

Les contraintes fournies par le contrôle aux aéronefs doivent pouvoir à la fois être planifiés à l'avance pour un espace aérien donné, mais également être adaptés en temps réel à la situation lorsqu'ils sont exécutés [2] : évitement de zones dangereuses, compensation de retard, ... La planification doit également inclure une certaine robustesse à l'égard des retards ou des possibles situations d'urgence. Bien sûr, cela implique une grande quantité de vérifications à effectuer, qui ne peuvent l'être que par l'usage de méthodes formelles [3, 4].

Une difficulté particulière réside dans le fait que les propriétés à vérifier ne sont pas seulement symboliques, mais incluent des contraintes physiques et géométrique : c'est par exemple le cas des propriétés de volabilité des trajectoires, qui visent à s'assurer que l'aéronef peut toujours inscrire une trajectoire volable dans les contraintes qui lui sont envoyées par le contrôle. Diverses approches ont été proposées pour faire du model-checking face à un système complexe et des propriétés continues. Elles consistent en général à faire abstraction de certains détails afin de limiter la complexité des modèles et faciliter les raisonnements et les vérifications, puis à réintroduire ces détails ultérieurement par des opérations de raffinement qui doivent respecter certaines règles afin de préserver la sémantique des modèles [5].

L'objectif de la thèse proposée est de démontrer que ces méthodes de model-checking permettent de vérifier ces propriétés, malgré la difficulté posée par la perte de performance qu'induit en général la discrétisation de propriétés continues portant sur un grand nombre d'objets, en l'illustrant sur le cadre applicatif des contrats 4D.

Il s'agira dans un premier temps d'analyser les contraintes du système en vue de sa formalisation : sur la base de scenarii représentatifs, il faudra identifier des propriétés et appréhender la dynamique du système en traduisant des contraintes physiques sous la forme de propriétés discrètes vérifiables. Dans un second temps, il s'agira d'extraire de ce travail des spécifications formelles et à mettre en œuvre des techniques pour réduire la complexité du modèle [6, 7, 8] (abstraction, symétries, parallélisation, compositionnalité, ...) afin de maîtriser la complexité des

vérifications à effectuer. Enfin, dans un troisième temps, il s'agira, sur la base de ce travail, d'identifier des études de cas d'intérêt et de les analyser. Cette analyse pourra consister à développer un module de réaffectation de contrats 4D à vérifier formellement et à intégrer dans une simulation de trafic aérien. Les résultats de cette analyse pourront le cas échéant permettre de faire évoluer les propriétés et les modèles à vérifier.

Cette thèse s'inscrit dans une collaboration ONERA / LIPN (U. Paris XIII : C. Coti, Ch. Choppy, L. Petrucci) / LIP6 (U.Paris VI : F. Kordon).

## Références


[1] 4DCO-GC Consortium. *Contract Definition for the 4DCo-GC project*. Technical report, 2011 (http ://www.4dcogc-project.org).

[2] D. Gekht & M. Idan. Tactical re-planning within the 4D contracts ATC concept. In *Proc. AIAA Guidance, Navigation and Control Conference*. 2013.

[3] P. Carle, Ch. Choppy, R. Kervarc, & A. Piel. A formal coloured Petri net model for hazard detection in large event flows. In *Proc. 20th Asia-Pacific Software Engineering Conference*, p. 323-330. IEEE Computer Society, 2013.

[4] L. M. Kristensen, J. Billington, L. Petrucci, Z. Qureshi, & R. Kiefer. Formal specification and analysis of airborne mission systems. In *Proc. 21st IEEE Digital Avionics Systems Conference*, p. 4.D.4-1-4.D.4-13. 2002.

[5] É. André, C. Coti, & H. G. Nguyen. Enhanced distributed behavioral cartography of parametric timed automata. In *Proc. 17th International Conference on Formal Engineering Methods*. 2015.

[6] S. Haddad, F. Kordon, L. Petrucci, J-F. Pradat-Peyre, & N. Trèves. Efficient State-Based Analysis by Introducing Bags in Petri Net Color Domains. In *Proc. American Control Conference*, p. 5018-5025. IEEE Computer Society Press, 2009.

[7] Ch. Choppy, M. Mayero, & L. Petrucci. Coloured Petri net refinement specification and correctness proof with Coq. *Journal of Innovations in Systems and Software Engineering*. Springer & NASA, 2010.

[8] Ch. Choppy, L. Petrucci, & A. Sanogo. Coloured Petri Nets Refinements, in D. Moldt (editor), *Proc. Workshop on Petri Nets and Software Engineering*, p. 187-201. 2013.