Introduction

Le contexte aéronautique[1] a depuis plusieurs années mis en évidence le besoin croissant de technologies de sécurité permettant d'éviter des utilisations malveillantes des matériels ou services installés à bord des avions par les compagnies pour leurs usagers et leurs besoins propres.

Avec l'apparition prochaine d'un service d'accès à bord à l'Internet cabine pour le plus grand nombre, ce besoin de sécurisation va devenir une priorité. A l'heure actuelle, il n'existe pas de solution de sécurité[2] permettant d'une part, de gérer ce nouveau type de trafic air-sol (appartenant à la famille de l'APC pour *Aeronautical Passenger Communication*) et d'autre part, de l'intégrer parmi les autres types de trafic échangés entre l'avion et le sol (trafics AOC pour *Aeronautical Operational Control*, AAC pour *Aeronautical Administrative Communication* et ATSC pour *Air Traffic Services Communication* par exemple), tout en maximisant le niveau de robustesse offert.

La plupart des approches de sécurisation « avion » se concentrent sur des méthodes et techniques permettant de sécuriser les échanges au sein de l'avion ou sur un lien dédié aux seules communications du contrôle aérien. Ainsi, le réseau avionique[3] embarqué de type AFDX est physiquement inaccessible aux passagers,

1. L'aéronautique désigne les sciences et les technologies ayant pour but de construire et de faire évoluer un aéronef dans l'atmosphère terrestre.

2. Dans le contexte du transport aérien, la sécurité est la propriété d'innocuité du système, elle vise à protéger le système contre les défaillances et les pannes. Le terme anglais est *safety*.

3. L'avionique est l'ensemble des équipements électroniques, électriques et informatiques des aéronefs. C'est donc un sous-ensemble du domaine aéronautique : l'avionique concerne uniquement l'intérieur de l'avion, tandis que l'aéronautique englobe le domaine avionique plus son environnement, incluant les installations terrestres de contrôle et de navigation.

cette ségrégation garantissant sa sûreté[4]. Concernant les flux ATC air-sol, ceux-ci exploitent des fréquences dédiées aux communications aéronautiques civiles, interdites par la loi à tout autre usage.

Cette problématique de sécurisation, bien que nécessaire, ne suffit plus à l'heure où l'interconnexion du réseau avionique avec le reste des réseaux de communication tels que le réseau Internet, apparaît de jour en jour comme une étape incontournable. En effet, la demande des passagers pour accéder à leurs outils de travail depuis leur siège en cabine devient de plus en plus pressante, ceux-ci étant aujourd'hui habitués à disposer d'accès terrestres à Internet omniprésents.

Le problème qui est abordé dans ce livre vise donc à proposer une méthode d'ingénierie logicielle pour permettre le développement d'une architecture de sûreté pour l'ensemble des communications aéronautiques qui viendra en complément de l'architecture de sécurité utilisée dans le réseau avionique et qui permettra de plus une interconnexion sécurisée entre le monde « avion » et le monde extérieur (réseau Internet par exemple).

La solution architecturale proposée dans ce travail repose principalement sur un composant central de routage, de filtrage et de sécurisation des flux de données aéronautiques. Grâce à la méthode d'ingénierie logicielle orientée modèle présentée dans cet article, un travail de conception et de développement a pu être mené. Cela a abouti à la proposition d'un composant avionique central appelé routeur sécurisé de nouvelle génération (routeur SNG). Les fonctionnalités mises en œuvre par le routeur SNG sont résumées dans la figure 1.

L'un des enjeux de ce travail a été de prendre en compte les problématiques de standardisation adoptées dans le monde avionique, les intégrer comme pré-requis et proposer une solution globale de sécurité intégrant le segment avion, le segment sol-bord et le segment sol.

En effet, ce travail ne peut avoir de pérennité scientifique et industrielle que s'il prend en compte l'ensemble des critères de sûreté et de sécurité qui caractérisent les divers environnements traversés et considère dès le départ les divers principes de standardisation retenus pour ces derniers.

4. Dans le contexte du transport aérien, la sûreté est la propriété d'immunité du système, elle qualifie la capacité d'un système à gérer les menaces et dangers externes au système. Le terme anglais est *security*.

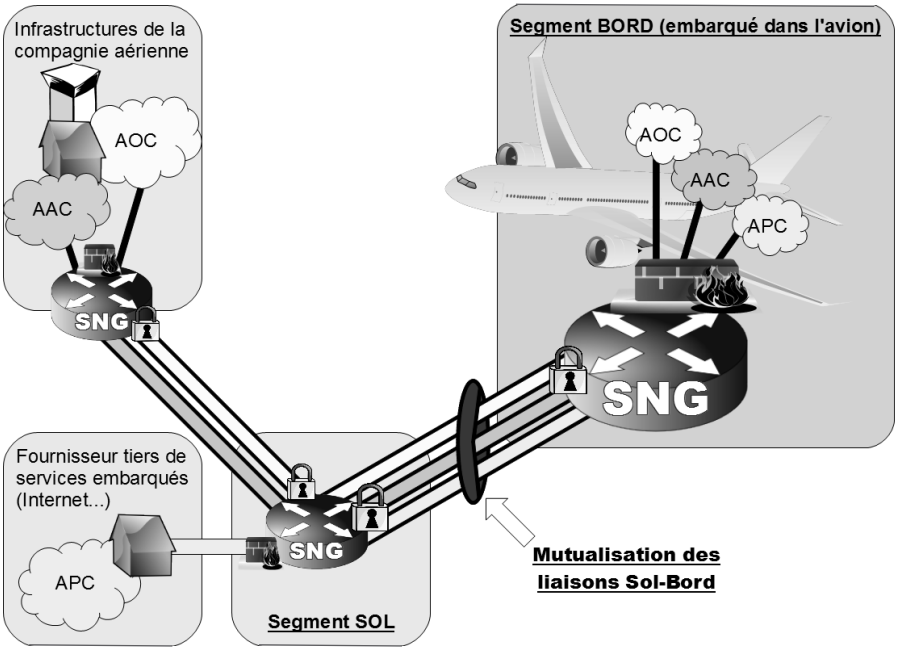

Figure 1. *Exemple de déploiement du routeur SNG dans le contexte aéronautique*

Utilisation des approches orientées modèle

La complexité des développements de systèmes embarqués avioniques nous a conduit à un travail préliminaire sur le processus de développement qui a abouti à la création d'une méthodologie générique de conception. Cette nouvelle méthodologie de développement de logiciel avionique et de prototypage rapide prend en compte dès l'établissement du cahier des charges, les contraintes de sûreté et de sécurité associées au système à mettre en œuvre.

Notre méthodologie de développement du routeur SNG est basée sur la modélisation des fonctionnalités, la transformation automatisée des modèles en code et l'utilisation de systèmes d'exploitation critiques mettant en œuvre la virtualisation. Les modèles présentent en effet des avantages non négligeables en termes de rapidité et de réutilisabilité du développement, ainsi qu'en vérification et en validation des systèmes modélisés. La transformation automatisée contribue à garantir la sécurité du code généré et donc du logiciel final. Les systèmes d'exploitation critiques sont une brique essentielle de la sûreté de l'exécution du logiciel généré avec notre méthodologie.

Ces modélisations permettent non seulement de vérifier formellement certaines propriétés sur les mécanismes modélisés pour le routeur SNG, mais elles permettent aussi de générer automatiquement un code source mettant en œuvre ces mécanismes. A notre connaissance, nous sommes les premiers, dans le domaine aéronautique, à avoir utilisé des modèles, formellement vérifiables, pour mettre en œuvre ces mécanismes réseaux *via* une transformation modèle vers code source.

La validation, abordée à la fin de ce chapitre, du logiciel du routeur sur émulateur puis sur un système embarqué réel et l'évaluation quantitative et qualitative des performances réseaux de ce routeur, ont ainsi permis de compléter et finaliser le cycle de développement industriel auquel est adossé ce travail de recherche.

Dans cette introduction il est fondamental de faire comprendre au lecteur l'importance que le développement orienté modèle a pris pour la conception des systèmes informatiques complexes. Cette importance s'est traduite par la prise en compte dans les procédures de certification des systèmes aéronautiques (voir documents RTCA DO-178C et DO-331 qui seront présentés dans la suite de cet ouvrage) de la possibilité d'utiliser des chaînes d'outils logiciels permettant, à partir de modèles de haut niveau, de pouvoir générer du code logiciel qui sera déployé à terme dans les systèmes aéronautiques critiques.

Plan de l'ouvrage

Afin de pouvoir comprendre l'intérêt de ces approches orientées modèles, il est nécessaire de les resituer dans un contexte plus large que le simple domaine aéronautique (ce sera l'objet du chapitre 1). Dès lors, dans un deuxième chapitre, les spécificités du domaine de la conception de systèmes aéronautiques et avioniques seront abordées et une méthode originale de conception orientée modèle sera présentée. Elle a été conçue pour répondre aux besoins particuliers de l'aéronautique. Ce chapitre détaille la contribution méthodologique de cet ouvrage qui propose une nouvelle méthode de prototypage rapide orientée modèle. Enfin, dans un dernier chapitre seront détaillées les différentes étapes de la méthode introduite précédemment. Cette méthode sera illustrée au travers d'un cas concret de développement de système embarqué critique : un routeur sûr et Sécurisé pour l'avionique de nouvelle génération (routeur SNG). Ce sera l'objet du dernier chapitre de cet ouvrage. Ceci représente un exemple concret de système embarqué complexe du domaine avionique. Nous introduirons les spécificités du domaine aéronautique auquel nous nous sommes intéressés pour ce travail d'ingénierie logicielle. Nous mettrons en avant la nécessité de nouveaux moyens d'interconnexion ainsi que le besoin de prendre en compte de façon conjointe les aspects sûreté et sécurité des communications. Nous illustrerons, en particulier, comment cette méthodologie peut être instanciée dans le cas précis du développement d'un routeur embarqué sécurisé. Nous détaillerons la chaîne d'outils

qui a été utilisée pour permettre d'appliquer notre méthodologie. Pour chacun d'eux, des exemples seront donnés. Nous conclurons ce dernier chapitre par une synthèse des performances obtenues pour le système développé par l'intermédiaire de notre méthodologie orientée modèle.

Dès lors, les apports et avantages de notre méthodologie pour la conception et le développement auront été explicités ainsi que les performances globales du système produit. Ces résultats permettent d'attester du haut niveau d'efficacité de la méthodologie qui est présentée dans cet ouvrage.