



Méthodes formelles de conception : Système de contrôle de trafic aéroportuaire

Ruikun YUAN - Abdelkader BELDJILALI



Table des matières

Introduction	2
1 Pré-étude	3
1.1 Diagramme de contexte	3
1.2 Description graphique du méta-modèle	3
1.3 Données manipulées	4
2 Aspect fonctionnelle	4
2.1 Décomposition fonctionnelle	4
2.2 Scénario fonctionnel	5
3 Aspect produits	7
3.1 Description graphique de la décomposition produit	7
3.2 Matrice de traçabilité Fonctions / composants	8
3.3 Matrice de traçabilité fonctions/input/output	9
Conclusion	12

Introduction

L'exercice proposé¹ a pour finalité la modélisation et l'analyse d'un système ATC simplifié dans un cadre MBSE : Model Based System Engineering. Cette approche permet, en effet, des simulations et vérifications précoce intervenant lors de la phase décroissante du cycle en V, en amont de l'implémentation.

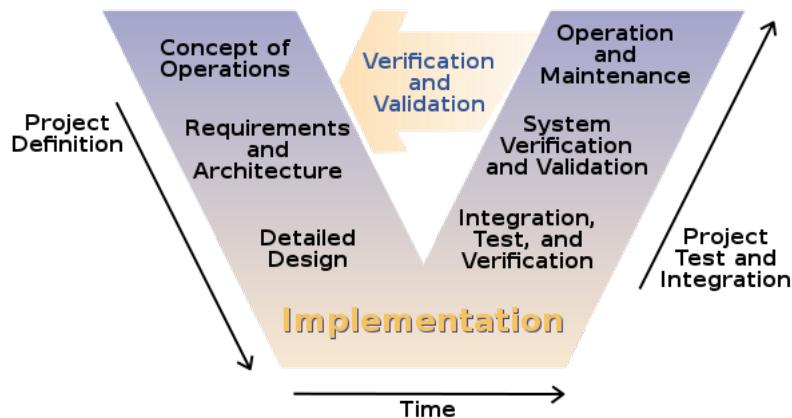


FIGURE 1 – Cycle en V

Les composants internes, constitutifs du système ATC considéré, comportent des acteurs humains, les contrôleurs, et des acteurs système, hardware et software. On citera, de façon non exhaustive, les radars primaires, secondaires, les logiciels de traitement et d'affichage des données radar et de plans de vol, sans oublier les filets de sauvegarde, les réseaux informatiques, les routeurs. Le NMOC européen, Network Management Operation Centre, et le système de traitement de plan de vol national sont inclus dans le système étudié car ils participent à la fourniture du service de contrôle. Par contre, les composants humains, matériels et logiciel assurant notamment le maintien en conditions opérationnelles des composants ne sont pas pris en compte dans le cadre de cet exercice.

Quant aux acteurs extérieurs, ce sont en particulier les pilotes, les compagnies aériennes, les aéronefs, le service météo. On pourrait ajouter les acteurs humains impactant la sûreté et la sécurité du système directement par le hacking du réseau ATC ou par brouillage des communications radio, par détournement de vols. Ceci impacte sur les contraintes que le système est susceptible de subir, contraintes qui doivent être prises en compte dans des fonctions additionnelles propres à empêcher les conséquences de malveillances et erreurs humaines et système. On peut aussi citer l'acteur environnemental "phénomènes météo". On choisit cependant de les ignorer pour se focaliser sur l'objectif pédagogique principal de cet exercice qui est d'appliquer une démarche MBSE sur un modèle simplifié.

1. Les livrables associés à cet exercice se trouvent à l'adresse : https://github.com/kad15/AF/tree/master/LIVRABLES_ATC_YUAN_BELEJILALI

1 Pré-étude

1.1 Diagramme de contexte

Le système ATC étudié ici interagit avec quatre acteurs externes qui permettent de définir la frontière du système :

- Les compagnies aériennes,
- Les pilotes,
- Les aéronefs,
- Le service météo.

Les acteurs environnementaux n'ont pas été pris en compte. La référence GPS de synchronisation est considérée comme appartenant au système

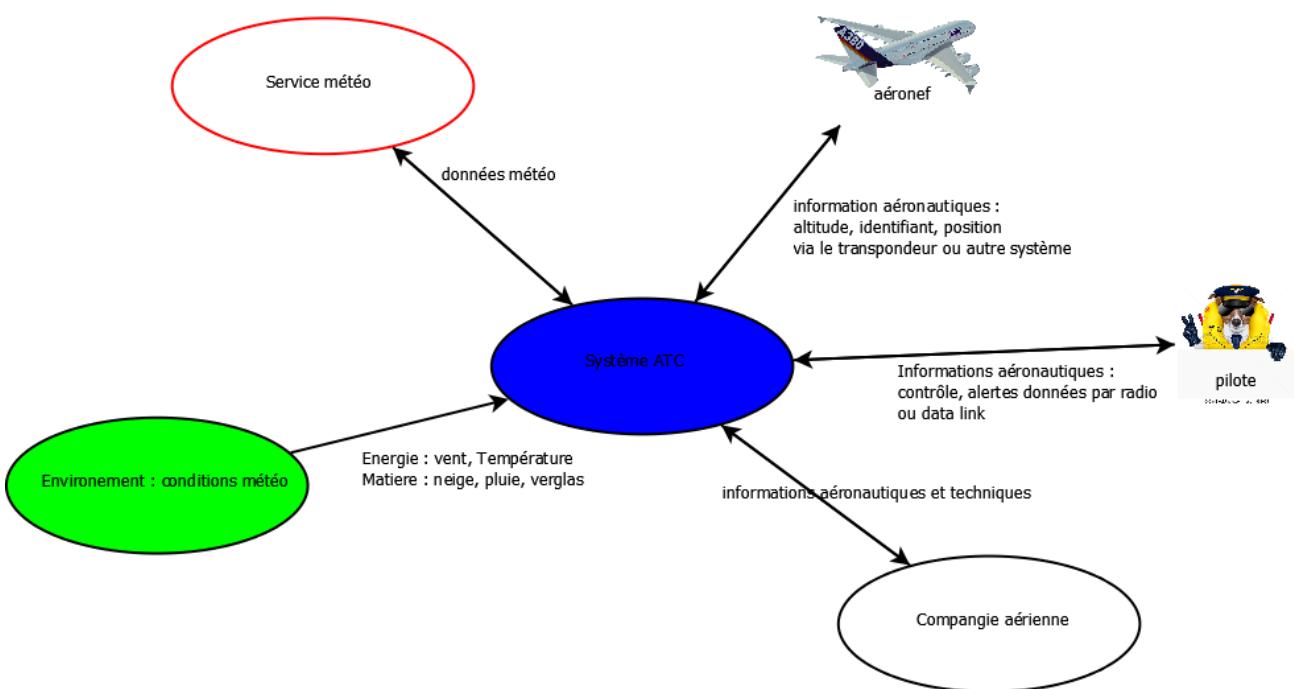


FIGURE 2 – Diagramme de contexte du système ATC

1.2 Description graphique du méta-modèle

Les fonctions, les items et les composants sont les principaux éléments du méta modèle de la figure 3. En particulier, une fonction peut recevoir en entrée, ou fournir en sortie, un item information ou être déclenchée par un item signal électrique. La classe Requirement est intéressante dans le sens où elle permet de vérifier que les exigences sont toutes "mapées" avec un fonction qu'elle spécifie.

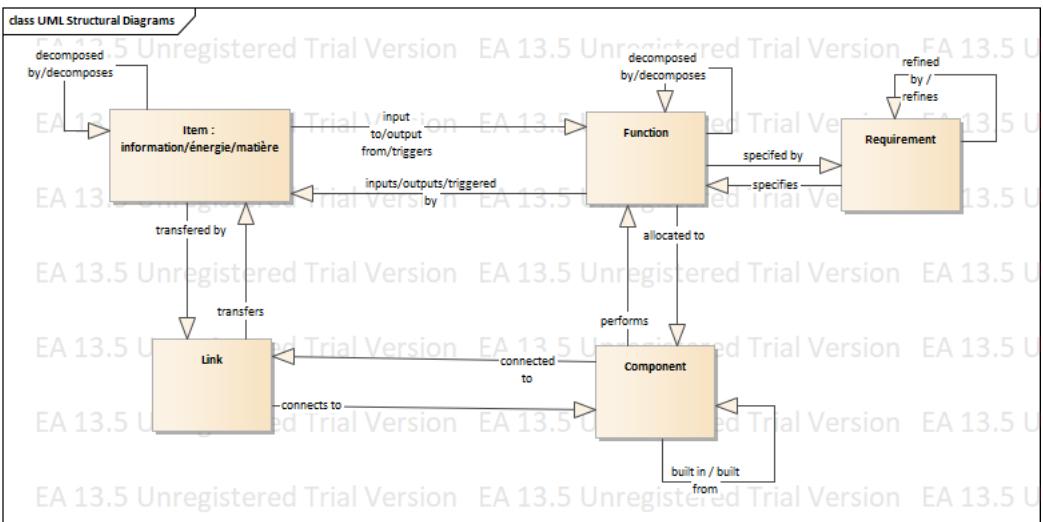


FIGURE 3 – meta modèle Vitech core conçu avec une version d'évaluation de l'outil Enterprise Architect

1.3 Données manipulées

Les données manipulées sont les suivantes :

- L'identifiant issu du plan de vol ou d'un radar secondaire,
 - La position de l'aéronef.

La position d'un aéronef vu par un radar primaire ne donne que la distance et l'azimut. Les radars secondaires donnent en outre l'altitude et l'identifiant de l'appareil. Les positions radar doivent être converties en longitude/latitude WGS84 pour pouvoir être affichées. Ce dernier point n'a pas été pris en compte explicitement dans le modèle. En outre, le modèle CORE ne distingue pas clairement entre position 2D des radars primaires et 3D des radars secondaires ; les fonctions de traitements spécifiques, ainsi que d'autres fonctions, ont été supprimées pour limiter la taille des graphes hiérarchiques et EFFBD. Ceci constitue un écart par rapport au cahier des charges de l'énoncé mais reste dans l'esprit de l'exercice.

2 Aspect fonctionnelle

2.1 Décomposition fonctionnelle

L'analyse du sujet a conduit à quatre fonctions principales décomposées en sous-fonctions selon le diagramme hiérarchique de la figure 4 :

- Acquérir les informations,
 - Traiter les informations,
 - Afficher les informations,
 - Communiquer i.e. Echanger des informations

L'analyse du modèle a mis en évidence, s'il en était besoin, le rôle crucial de la communication entre contrôleur et pilote dans la fourniture du service de contrôle, d'alerte et de surveillance. Sur le plan métier, la radio comme moyen de communication constitue le maillon faible des systèmes ATC actuel. En ce sens, la modélisation permet de mettre en évidence des failles du domaine réel ce qui constitue une source d'amélioration du système.

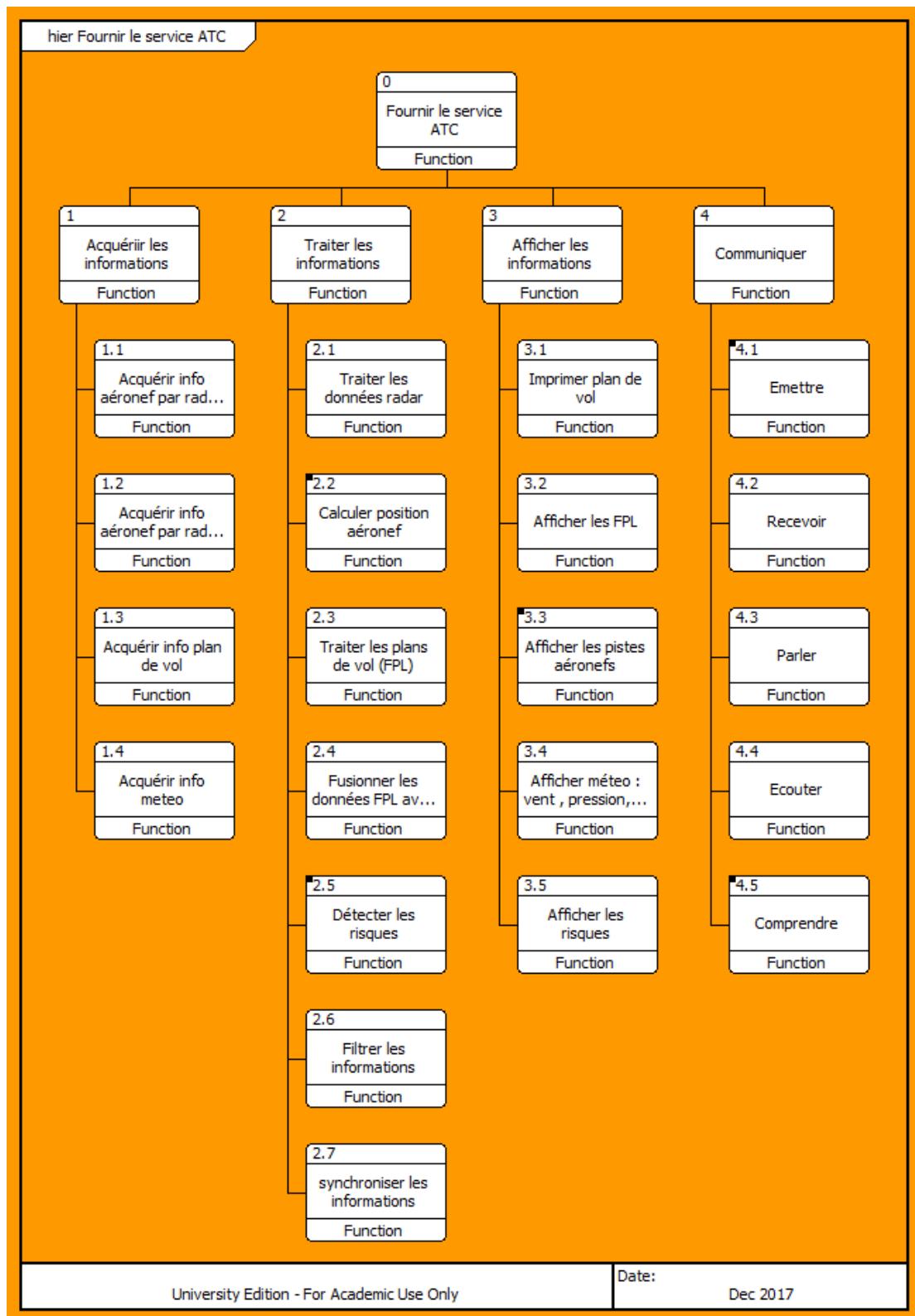


FIGURE 4 – Diagramme hiérarchique des fonctions

2.2 Scénario fonctionnel

Les diagrammes d'activités, EFFBD ou de séquence permettent de capturer un ou plusieurs scénarios du système modélisé. La démarche utilisée a consisté à créer un diagramme EFFBD dans CORE en utilisant uniquement les fonctions feuille puis de travailler sur le diagramme N2 pour l'ajout

des items. Un exemple est donné en figure 5.

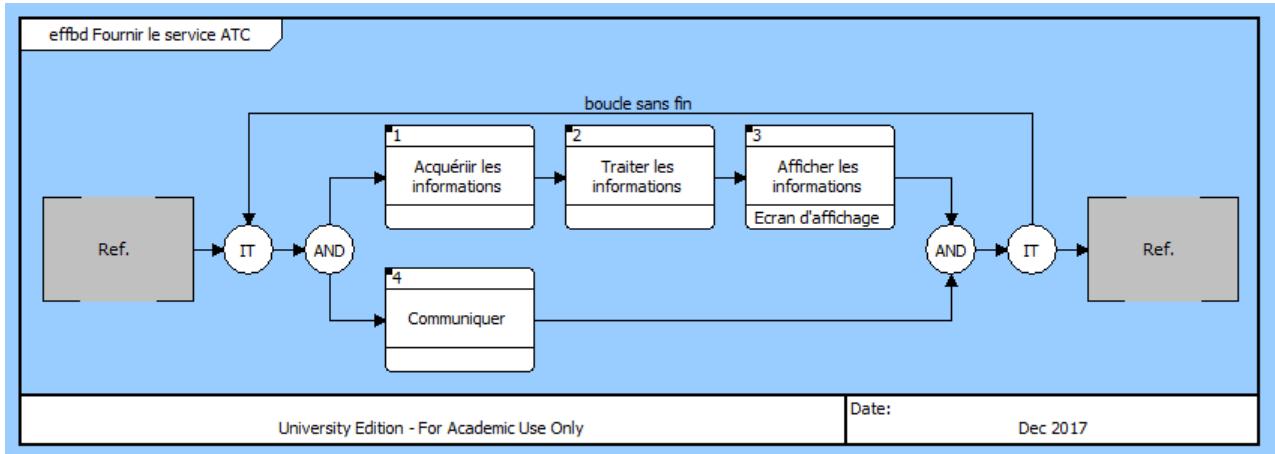


FIGURE 5 – Diagramme EFFBD simplifié du service ATC

Scénario complet : Le scénario associé à l'ensemble des fonctions feuille se trouve à l'adresse https://github.com/kad15/AF/blob/master/LIVRABLES_ATC_YUAN_BELDJILALI/question%207%20scenarios%20fonctionnel%20unique.png

3 Aspect produits

3.1 Description graphique de la décomposition produit

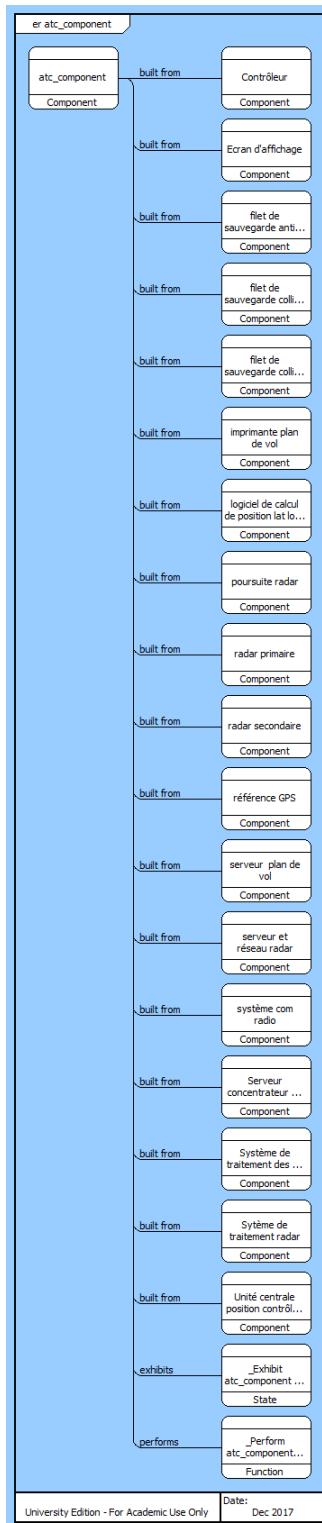


FIGURE 6 – Diagramme entité-relation des composants du système ATC

NB : Pour le tracé du diagramme ER, un composant conteneur abstrait **atc_component** a été créé.

3.2 Matrice de traçabilité Fonctions / composants

L'ensemble des fonctions vers l'ensemble des composants doit être une application surjective ; une fonction ne peut être assurée par deux composants différents dans le modèle Vitech core. Par contre, plusieurs composants peuvent effectuer la même fonction. La matrice de la figure 7 montre une couverture exhaustive des fonctions feuille par les composants du système. En particulier, la contrainte d'affichage sur un écran unique énoncée dans les spécifications est respectée.

	Number & Name	allocated to
0 Fournir le service ATC		
1 Acquérir les informations		
1.1 Acquérir info aéronef par radar secondaire	radar secondaire	
1.2 Acquérir info aéronef par radar primaire	radar primaire	
1.3 Acquérir info plan de vol	serveur plan de vol	
1.4 Acquérir info meteo	Serveur concentrateur données météo aéronautique	
2 Traiter les informations		
2.1 Traiter les données radar	Système de traitement radar	
2.2 Calculer position aéronef	logiciel de calcul de position lat lon WGS84 et altitude/FL	
2.3 Traiter les plans de vol (FPL)	Système de traitement des FPL	
2.4 Fusionner les données FPL avec radar primaires, secondaires	poursuite radar	
2.5 Déetecter les risques		
2.5.1 Déetecter les risques d'intrusion dans les zones interdites	filet de sauvegarde anti intrusion zone interdites	
2.5.2 Déetecter les risques de collision entre aéronefs	filet de sauvegarde collision entre aéronefs	
2.5.3 Déetecter les risques de collisions avec le sol	filet de sauvegarde collision sol	
2.6 Filtrer les informations	Unité centrale position contrôleur	
2.7 synchroniser les informations	référence GPS	
3 Afficher les informations	Ecran d'affichage	
3.1 Imprimer plan de vol	imprimante plan de vol	
3.2 Afficher les FPL	Ecran d'affichage	
3.3 Afficher les pistes aéronefs	Ecran d'affichage	
3.3.1 Afficher les pistes enrichies	Ecran d'affichage	
3.3.2 Afficher les plots radar primaires	Ecran d'affichage	
3.4 Afficher météo : vent , pression, T, Td	Ecran d'affichage	
3.5 Afficher les risques	Ecran d'affichage	
4 Communiquer		
4.1 Emettre	système com radio	
4.2 Recevoir	système com radio	
4.3 Parler	Contrôleur	
4.4 Ecouter	Contrôleur	
4.5 Comprendre	Contrôleur	
question 7 : scenario fonctionnel unique		

FIGURE 7 – Matrice de traçabilité Fonctions / composants

3.3 Matrice de traçabilité fonctions/input/output

La matrice de traçabilité présentée dans les figures 8 et 9 s'est avérée essentielle pour vérifier les entrées sorties des fonctions feuille. En effet, malgré l'utilisation du diagramme N2, des oubliers ont persisté ; seules les vues tabulaires permettent l'exhaustivité en mettant en évidence les manques. Ceci facilite l'approche récursive ou itérative propre à tout processus de conception ou développement.

On regrettera le fait que les tables dans CORE ne puissent pas être directement générées au format L^AT_EX.

Enfin, nous avons noté que le processus itératif se nourrit aussi des divergences potentielles entre l'ensemble des composants et celui des fonctions. On peut ainsi être amené à décomposer une fonction en sous fonctions ou un composant en sous composant. On arrive ainsi à une granularité optimale du FBS et du PBS par "convergence des deux mondes".

Number & Name	inputs	outputs
0 Fournir le service ATC		
1 Acquérir les informations		
1.1 Acquérir info aéronef par radar secondaire	Informations récupérées par radar secondaire	données radar secondaire brutes
1.2 Acquérir info aéronef par radar primaire	echolocalisation par radar primaire	données radar primaire brutes
1.3 Acquérir info plan de vol	info système plan de vol	données FPL brutes
1.4 Acquérir info meteo	info serveur météo	données météo
2 Traiter les informations		
2.1 Traiter les données radar	données radar primaire brutes données radar secondaire brutes	données radar primaire traitées données radar secondaire traitées
2.2 Calculer position aéronef	données radar primaire traitées données radar secondaire traitées	position aéronef
2.3 Traiter les plans de vol (FPL)	données FPL brutes	données FPL traitées
2.4 Fusionner les données FPL avec radar primaires, secondaires	données FPL traitées données radar primaire traitées données radar secondaire traitées	piste radar enrichie
2.5 Déetecter les risques		
2.5.1 Déetecter les risques d'intrusion dans les zones interdites	données cartographiques position aéronef	alarme intrusion zone interdite
2.5.2 Déetecter les risques de collision entre aéronefs	position aéronef	alarme collision entre aéronef
2.5.3 Déetecter les risques de collisions avec le sol	position aéronef	alarme collision avec le sol
2.6 Filtrer les informations	données FPL traitées position aéronef	IHM affichage FPL IHM d'alerte IHM radar
2.7 synchroniser les informations	données radar primaire traitées données radar secondaire traitées piste radar enrichie	données synchronisées
3 Afficher les informations		
3.1 Imprimer plan de vol	données FPL traitées	identifiant aéronef informations plan de vol sur papier
3.2 Afficher les FPL	données FPL traitées	IHM affichage FPL
3.3 Afficher les pistes aéronefs		
3.3.1 Afficher les pistes enrichies	piste radar enrichie	IHM radar
3.3.2 Afficher les plots radar primaires	données radar primaire traitées position aéronef	IHM radar
3.4 Afficher météo : vent, pression, T, Td	données météo	IHM information meteo

FIGURE 8 – Matrice de traçabilité Fonctions / in / out

Number & Name	inputs	outputs
3.5 Afficher les risques	alarme collision avec le sol alarme collision entre aéronef alarme intrusion zone interdite	IHM d'alerte
4 Communiquer		
4.1 Emettre	informations émises par le contrôleur	informations arrivées au niveau de la radio de l'aéronef
4.2 Recevoir	information arrivées sur la radio du contrôleur	informations entendues par le contrôleur
4.3 Parler	informations interprétées par le contrôleur informations plan de vol sur papier IHM affichage FPL IHM d'alerte IHM information meteo IHM radar	parole contrôleur
4.4 Ecouter	information arrivées sur la radio du contrôleur	informations entendues par le contrôleur
4.5 Comprendre	informations entendues par le contrôleur	informations interprétées par le contrôleur
question 7 : scenario fonctionnel unique		

FIGURE 9 – Matrice de traçabilité Fonctions / in /out (suite)

Conclusion

La démarche employée est itérative. Dans l'approche MBSE, on divise le système en fonctions et sous fonctions, pour obtenir une structure d'arbre enraciné, que l'on confrontent d'un côté aux exigences et de l'autre aux composants qui assurent/perform ces fonctions. Le tracé de diagrammes dynamiques comme les EFFBD aident à visualiser le système en action, à décrire des scenarii, et donc à découvrir des fonctions qui auraient pu être oubliées et à régler le niveau de granularité optimal au même titre que le reporting permis par CORE qui confronte functions, components, item et link dans une vue tabulaire efficace lors de la phase de détection des manques.

Le reporting de CORE est aussi une aide précieuse pour la validation du projet en amont par le client et l'évaluation financière et ressources nécessaires à ce dernier. CORE est donc aussi un outil de communication convaincant.

Par manque de temps, les aspects "link" et "requirement" n'ont pu être traités pour aller au delà des objectifs de l'énoncé. Il manque probablement de plus à ce projet encore un certain nombre d'itérations.

L'aspect Maintien en Conditions Opérationnelles(MCO) du système ATC n'a pas été abordé, celui du développement de ces systèmes non plus. En France, le MCO du système est assuré par les maintenances de la Direction des Opérations (DO) de la DGAC. Quant au développement, il relève de la Direction Technique et de l'Innovation(DTI) qui assure la MOA vis à vis des prestataires externes et le lien avec les partenaires, notamment dans le cadre de sa participation à certains "Work Package" du programme SESAR. En outre, comme indiqué dans l'introduction, nous avons choisi de faire abstraction des environnements "safety/security" et "phénomènes météo".

Enfin, un dernier mot sur l'outil utilisé. CORE est un outil efficace pour aider à construire "the right system and the system right" mais trop lié au monde Windows. En particulier, une meilleure connaissance de l'outil auraient permis un gain de temps important dans le cadre du projet ROBAFIS bien que la version "university" n'autorise pas le travail collaboratif. CORE permet, en effet, d'assurer l'exhaustivité de la prise en compte des exigences par les fonctions et la création automatique des tableaux pour alimenter le rapport de développement Encore faut-il s'assurer que les exigences traduisent correctement les besoins.

