# Intergiciels et Sûreté de Fonctionnement
# Présentation des activités et centres d'intérêts

**Christophe Honvault**
christophe.honvault@astrium-space.com

## Sommaire

# Introduction

1

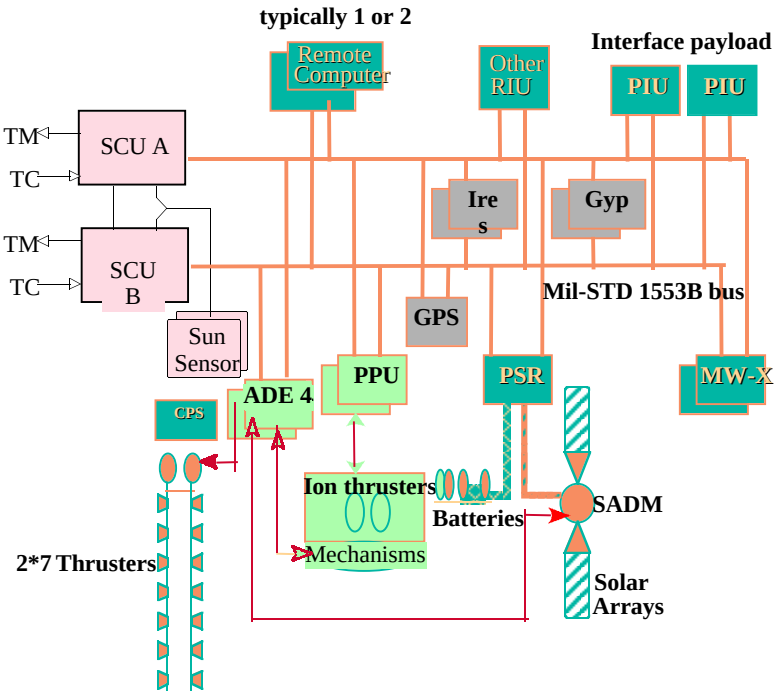


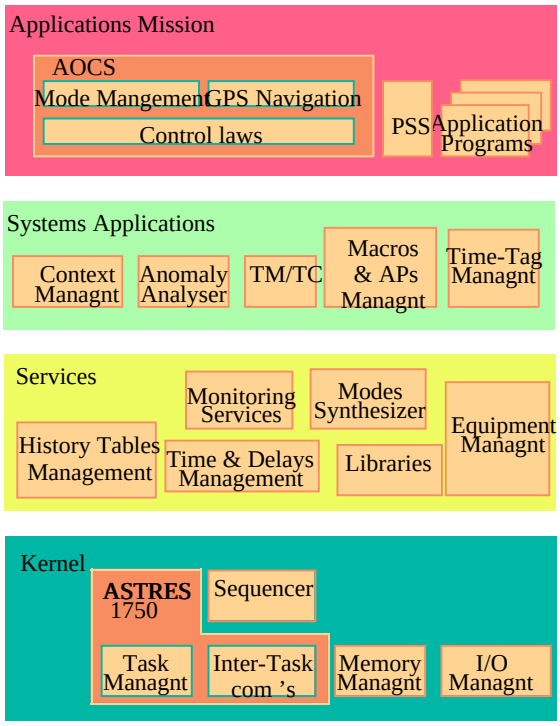

## Des intergiciels spécifiques

- **Les logiciels spatiaux sont découpés en couches :**
  - L'exécutif temps-réel :
    - ASTRES, VxWorks, RTEMS,
    - Séquenceur spécifique,
    - Gestion de la mémoire et des entrées/sorties, …
  - Les services de base (Data Management Software) :
    - Gestion des équipements,
    - Gestion des services de surveillance (Monitoring), ...
  - Les applications système :
    - Gestion des Télécommandes/Télémesures
    - Gestion des macros (interpréteur), …
  - Les applications mission :
    - Logiciels de contrôles d'attitude et d'orbite (SCAO)
    - Logiciels autonomes, …

**Embryon d'intergiciel**

# Architecture système E3000 (centralisée)

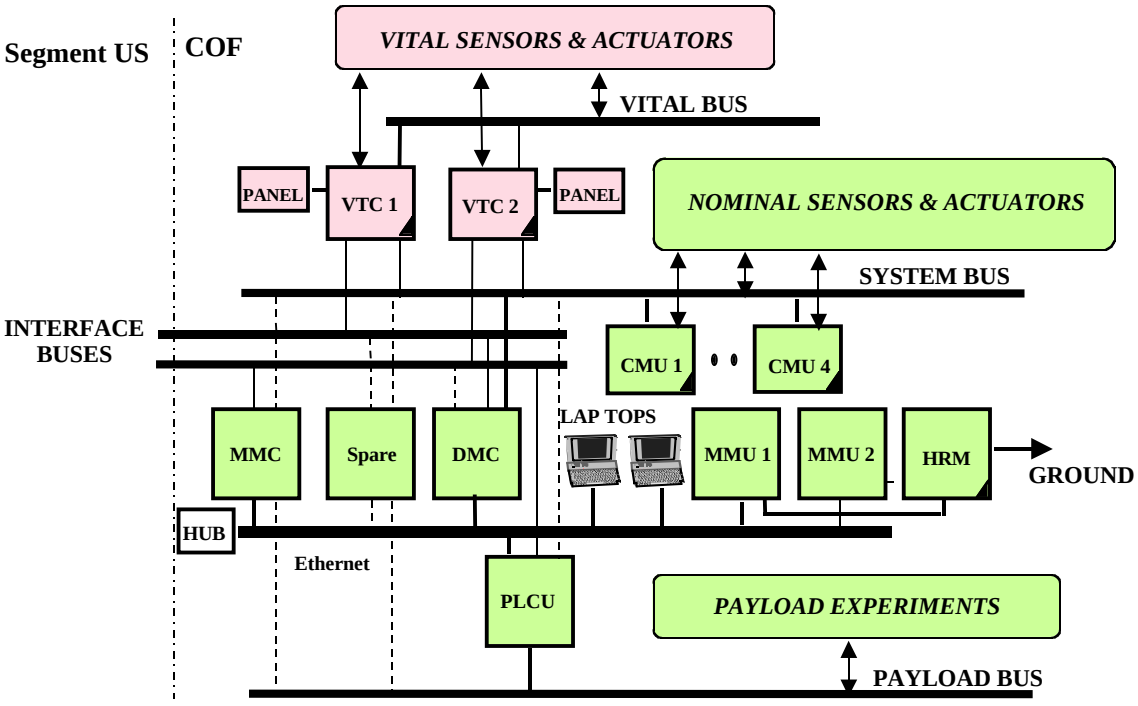


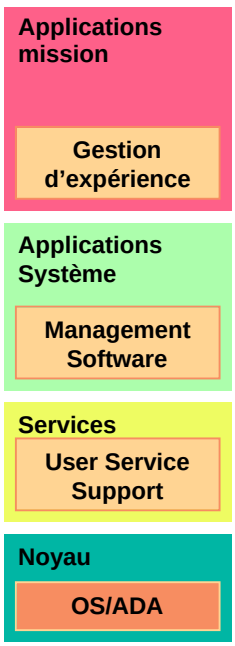







# Architecture système COF (distribuée)



# 2

# A3M: Advanced Avionics Architecture & Modules

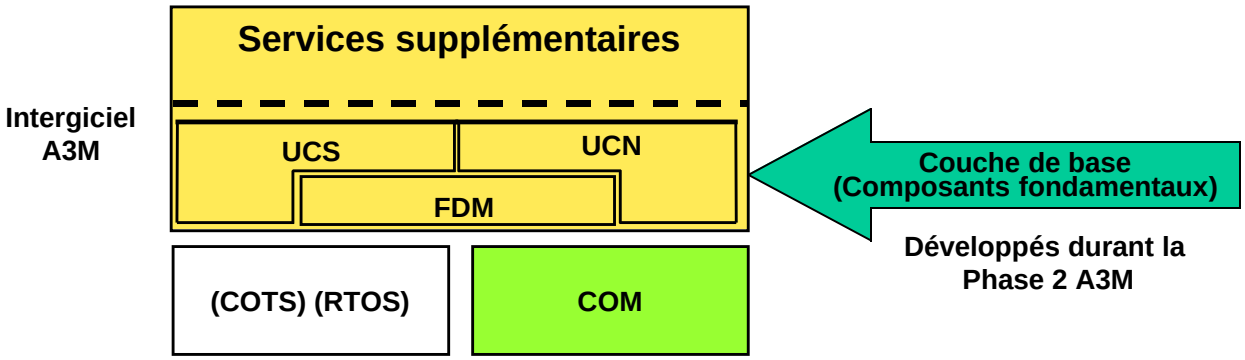
**ESTEC Contract 13024/98/NL/FM(SC)**




## Introduction et motivations

- **Missions**
  - Systèmes de gestion de données (DMS) complexes: vols habités, COF
  - Missions complexes avec systèmes hétérogènes (Aurora)
  - Systèmes comportant plusieurs engins (Darwin, LISA, SMART)
- **Évolution des systèmes embarqués**
  - Architectures de calcul configurables reposant sur des services d'Intergiciels
  - Utilisation de composants COTS au niveau exécutif
  - Exigence élevée en terme de temps-réel et de Sûreté de Fonctionnement
- **Objectifs d'A3M (Advanced Avionics Architecture & Modules)**
  - Définition et implémentation des services de base d'un intergiciel utilisé dans des systèmes spatiaux à fortes contraintes temporelles et de tolérance aux fautes
  - Mise à disposition des composants de base pouvant servir au développement d'intergiciels spécifiques aux applications spatiales distribuées
- **Organisation**
  - Phase 1: Analyse et modélisation du problème, identification des composants principaux liés au temps-réel et à la Sûreté de Fonctionnement
  - Phase 2: Implémentation d'un intergiciel simple et caractérisation sur une plate-forme de démonstration

# Architecture et composants




- **Architecture de l'intergiciel A3M**
  - Une couche élémentaire implémente les composants indispensables au développment d'applications tolérantes aux fautes et temps-réel
  - Des services supplémentaires supportant des standards (Corba)
- **Composants fondamentaux (développés à partir des algorithmes conçus par l'INRIA)**
  - UCS (Uniform ConsensuS) et UCN (Uniform CoordinatioN) sont des protocoles génériques permettant la prise de décision dans un système distribué, même en présence de défaillance
  - FDM (Failure Detection Module) implémente le modèle de défaillance



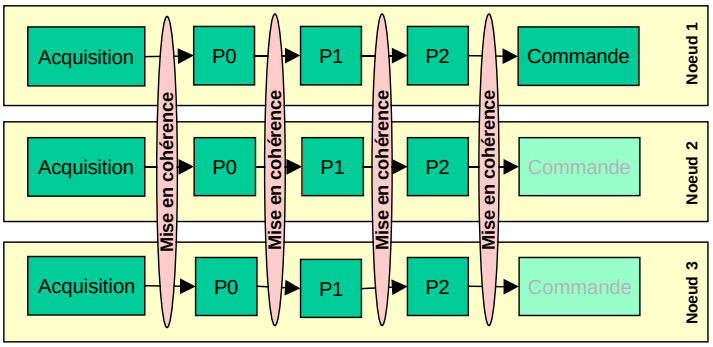

# Principes généraux de l'architecture

- **Les composants fondamentaux implémentent les services essentiels au développement de services supportant les défaillances.**
  - Ils sont utilisés pour s'assurer que toutes les instances des services reçoivent les mêmes entrées dans le même ordre. Si les instances sont déterministes, le traitement des mêmes informations aboutit au même résultat.
  - De plus, ils sont utilisés pour assurer la cohérence des décisions d'ordonnancement dans le système distribué.
  - Les processus distribués partageant des ressources communes peuvent être sérialisés en implémentant un séquenceur basé sur ces protocoles.
- **L'application à des applications spatiales pour traiter le problème de défaillance de processeurs :**
  - Processus dupliqués et sélection du résultat final (vote).
  - Mise en cohérence de données partagées par des processus distribués (datapool)

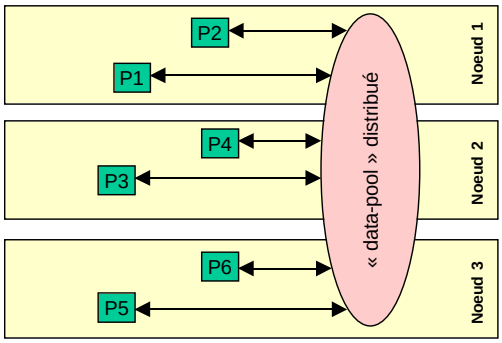
➢ **Nécessite le développement de services supplémentaires (développés dans le cadre de la phase 2).**

# Applications d'évaluation

- **Problème 1 : mise en cohérence de données dans un système distribué (avec fonction de vote répliquée et configurable)**



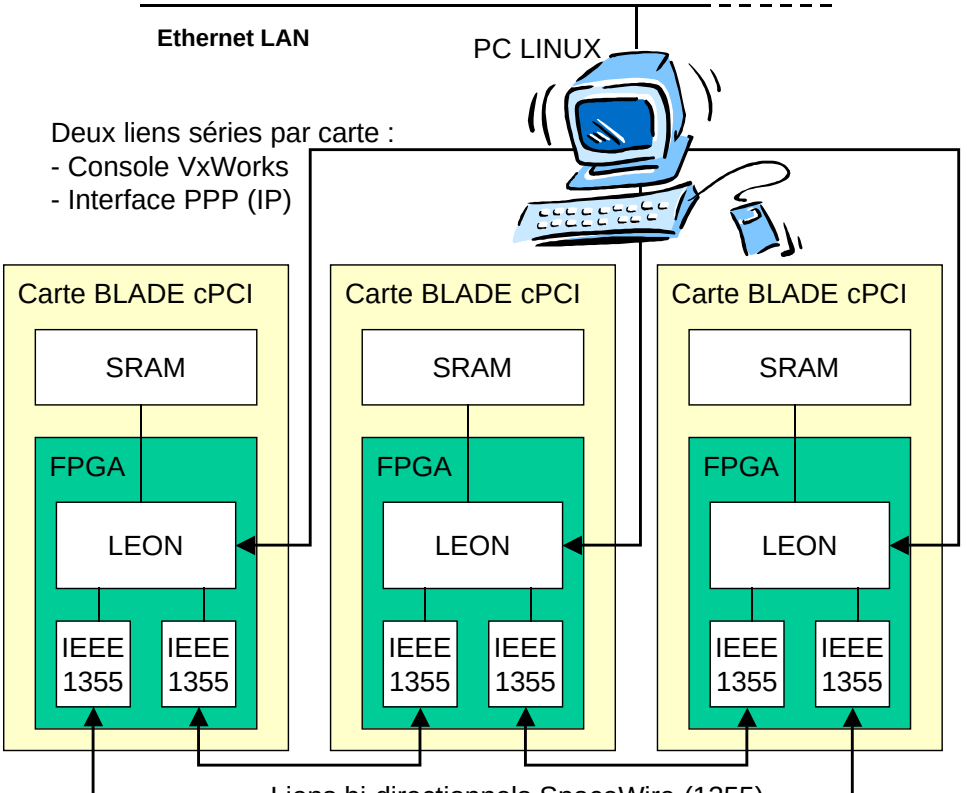

- **Problème 2 : cohérence de données partagées dans un système distribué**





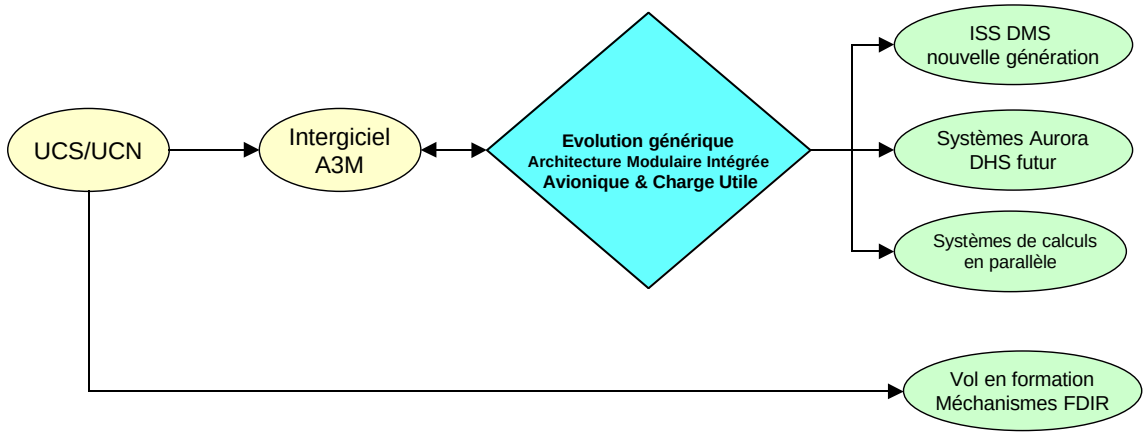


# Plate-forme d'évaluation




# Perspectives

- **Trois axes pour de futurs développements :**
  - Amélioration des algorithmes UCS/UCN/FDM (ajout de mécanismes supportant la réinsertion de processeurs ayant défailli) et de leur implémentation (performance).
  - Développement de services supplémentaires au dessus des algorithmes UCS/UCN/FDM.
  - Consolidation des services A3M en prenant en compte les plates-formes logicielles, les exigences des projets futurs et une nécessaire standardisation ECSS.







# Prospectives

3

# Intergiciels et Sûreté de Fonctionnement
# Utilisation dans le domaine spatial

- **Avionique distribuée, adaptée aux missions complexes où plusieurs systèmes collaborent :**
  - Constellation, vol en formation
    - distribution d'applications
    - gestion des défaillances d'un satellite de la constellation
    - synchronisation des engins (par exemple pour des expériences d'interférométrie)
  - Télé-opération
    - Accès transparent aux fonctions des systèmes spatiaux
    - Gestion cohérents des systèmes comportant plusieurs engins
  - Robotique
    - Systèmes collaboratifs : orbiteur/atterrisseur, robots multiples
- **Gestion des défaillances pour des systèmes sûrs ou nécessitant de grandes puissances de calcul :**
  - Utilisation de composants COTS (processeurs, RAM)
  - Calculs distribués sur plusieurs processeurs COTS ou non (LEON)
  - Nécessité de réinsérer les calculateurs ayant défailli temporairement




# Axes d'étude

- **Identification des besoins système en collaboration : communication, performance, routage, gestion des reconfigurations, télé-opération, télé-maintenance.**
- **Définition de l'architecture logicielle et matérielle correspondante permettant la répartition performante des fonctions sur des processeurs séparés.**
- **Identification des fonctions de gestions de systèmes distribués.**
- **Identification et spécification des services de base des intergiciels adaptés aux standards du spatial (CCSDS, PUS, etc.) ainsi que des solutions COTS adaptées.**
- **Identification des fonctions à implémenter en matériel pour des raisons de performance ou de sécurité.**
- **Identification des solutions permettant la distribution entre plusieurs systèmes physiquement disjoints (constellations, liaison sol/bord ou sonde/orbiteur) et estimation de leur performance.**
- **Étude et développement de solutions permettant la réinsertion d'un calculateur ayant défailli temporairement.**
- **Prototypage de la solution retenue avec des composants COTS ou logiciels libres de façon à évaluer la faisabilité de l'approche retenue.**