ASSERT: un processus d'ingénierie pour des systèmes logiciels aux propriétés garanties.

Dr Eric Conquet
ESA/ESTEC

Journées Neptune
Paris, Mai 2007

ASSERT en quelques chiffres

- **Un projet partiellement financé par la CE dans le 6ème Programme cadre sous le thème “systèmes embarqués”.**
- **Type d’instrument: Projet Intégré.**
- **Nombre de partenaires: 28**
- **Coût du projet: ~15 M€**
- **Financement CE: 8.3 M€**
- **Durée du projet: 3 ans.**
- **Démarrage le 01/09/2004.**

Copyright 2004-2007 © ASSERT Project

ASSERT: les partenaires.

- **Organisations internationales:**
  - ESA (Coordinateur), ESI
- **Partenaires industriels:**
  - ALCATEL ALENIA SPACE France (F) and Italy (I), ASTRIUM Satellites (F), Astrium Space Transportation (D+F) , CS – Systèmes d'Information (F) , DASSAULT Aviation (F) , EADS Corporate Research Center (D) , MBDA France (F)
- **Partenaires académiques:**
  - CNRS-VERIMAG (F), DIT/UPM university of Madrid (E) , ENST (F) ,ETH -Swiss Federal Institute of Technology (CH) ,ONERA (F), University of Padua (I)
- **PME:**
  - BSSE (D) , Dutch Space BV (NL) , ESTEREL Technologies (F) , INTECS (I) , PROVER (S) , SciScys (UK) , SEMANTIX (GR) , SoftwCare (E) , Terma A/S (DK) , TNI-EUROPE (UK), TNI-Software (F)

Copyright 2004-2007 © ASSERT Project

ASSERT: nous produisons des nectars technologiques

Dependability
Distribution
Hard Real Time
University of Padua

Development &Verification Tools
CS
VERIMAG

System Modelling and Verification
ESA

Process & Standardisation: **ASTRIUM Space Transportation**

MA3S Pilot Project
ASTRIUM Space Transp.

HRI Pilot Project
ALCATEL ALENIA SPACE

MPC Pilot Project
ASTRIUM Satellites

Openness & Exploitation: **ESA**

Copyright 2004-2007 © ASSERT Project

ASSERT: Les objectifs.

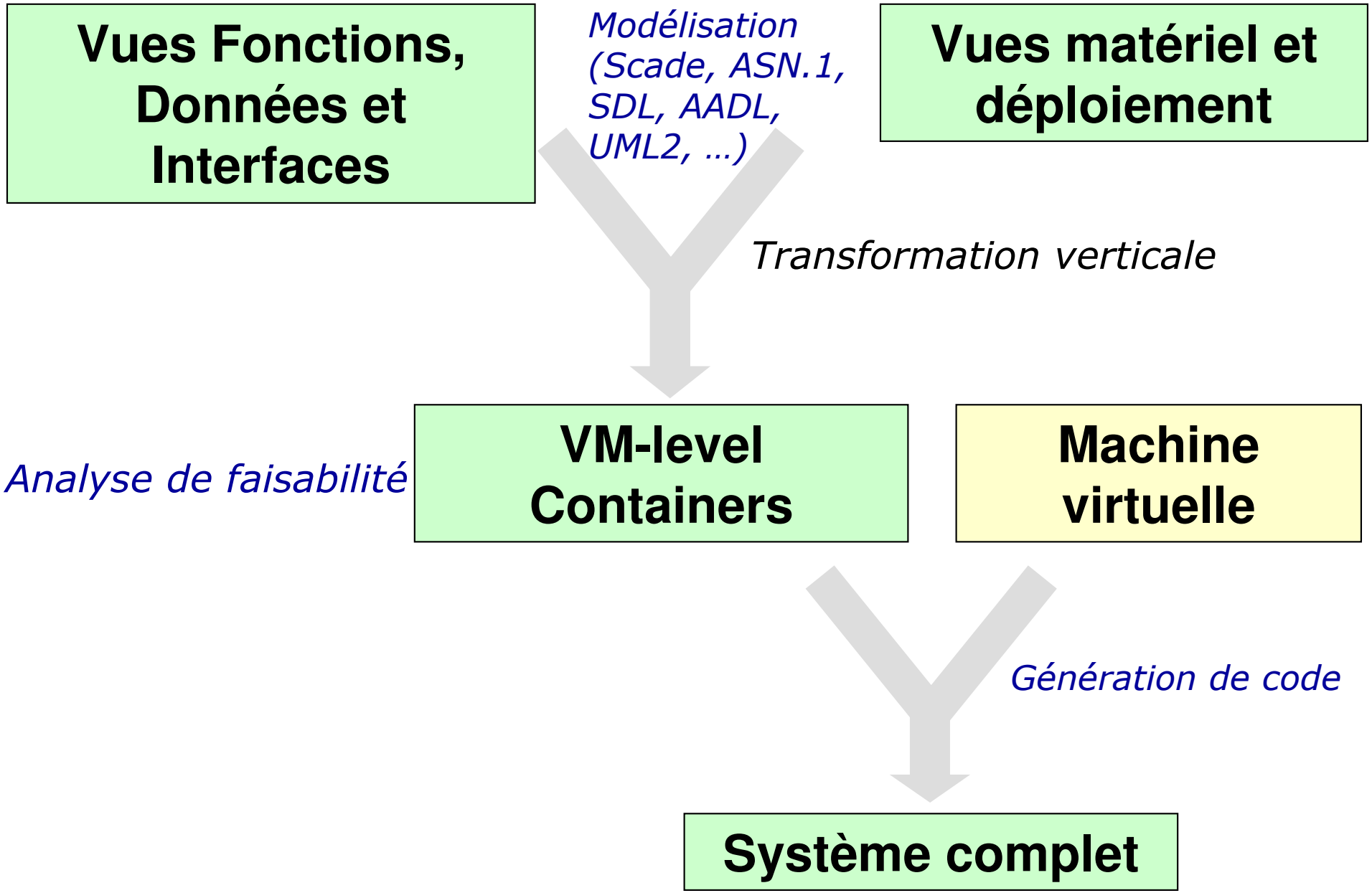
- **ASSERT doit développer des méthodes, processus et outils pour supporter une approche basée sur la preuve en continu depuis les premières spécifications systèmes jusqu'a la phase d'implémentation.**

- **ASSERT développera et prouvera des architectures de référence pour des familles de systèmes afin de réaliser l'instanciation de ces familles dans un projet en réduisant les temps de développement**

- **Les résultats d'ASSERT seront constitués par:**
  - *Un processus d'ingénierie système autour de la notion de familles de systèmes,*
  - *Des architectures de références et des composants de base,*
  - *Des outils supportant le développement des fonctions de traitement de données bord pour des systèmes embarqués critiques caractérisés par des propriétés de tolérance aux fautes, de sécurité et de temps-réel dur.*

Copyright 2004-2007 © ASSERT Project

ASSERT : vers un nouveau processus



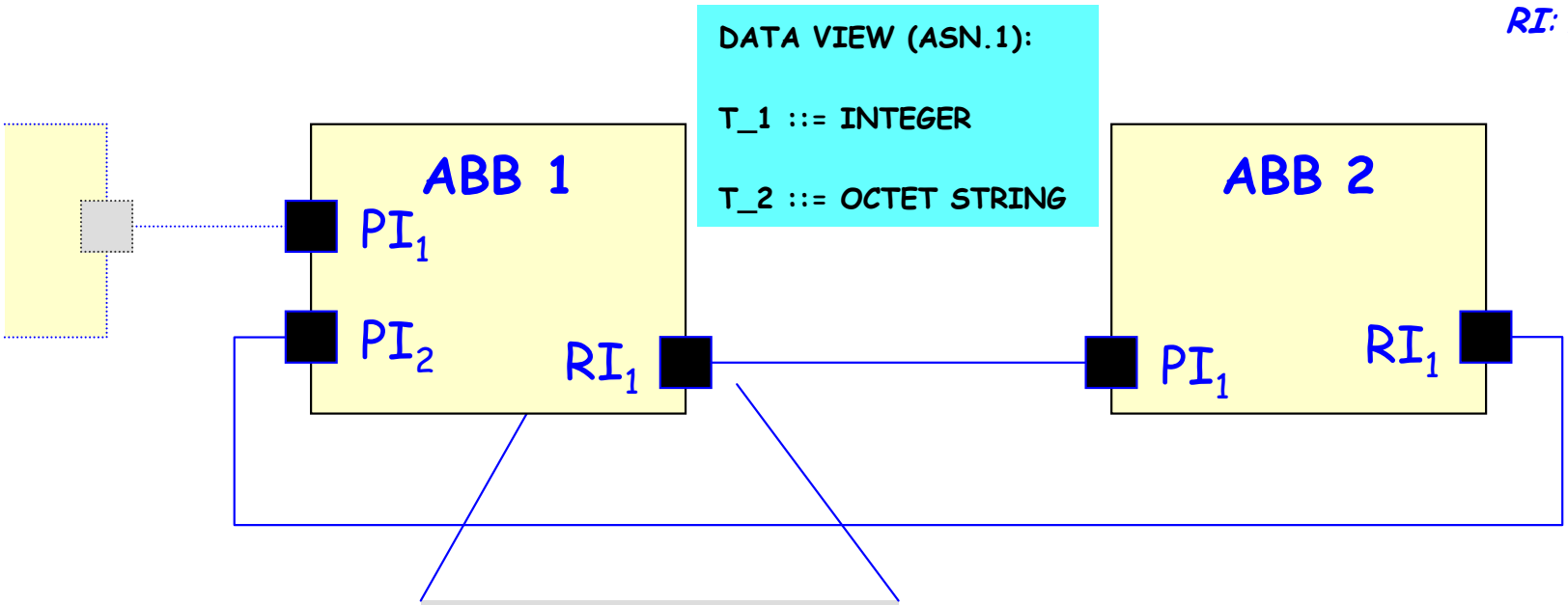
Copyright 2004-2007 © ASSERT Project

Vues données et Interfaces

Vues Interfaces et Données

Activité: capturer les interfaces des blocs applicatifs (ABB) et les connecter entre elles

PI: Provided Interface
RI: Required Interface



Attributs:
Paramètres et règles d'encodage, WCET, période, langage d'implémentation, …

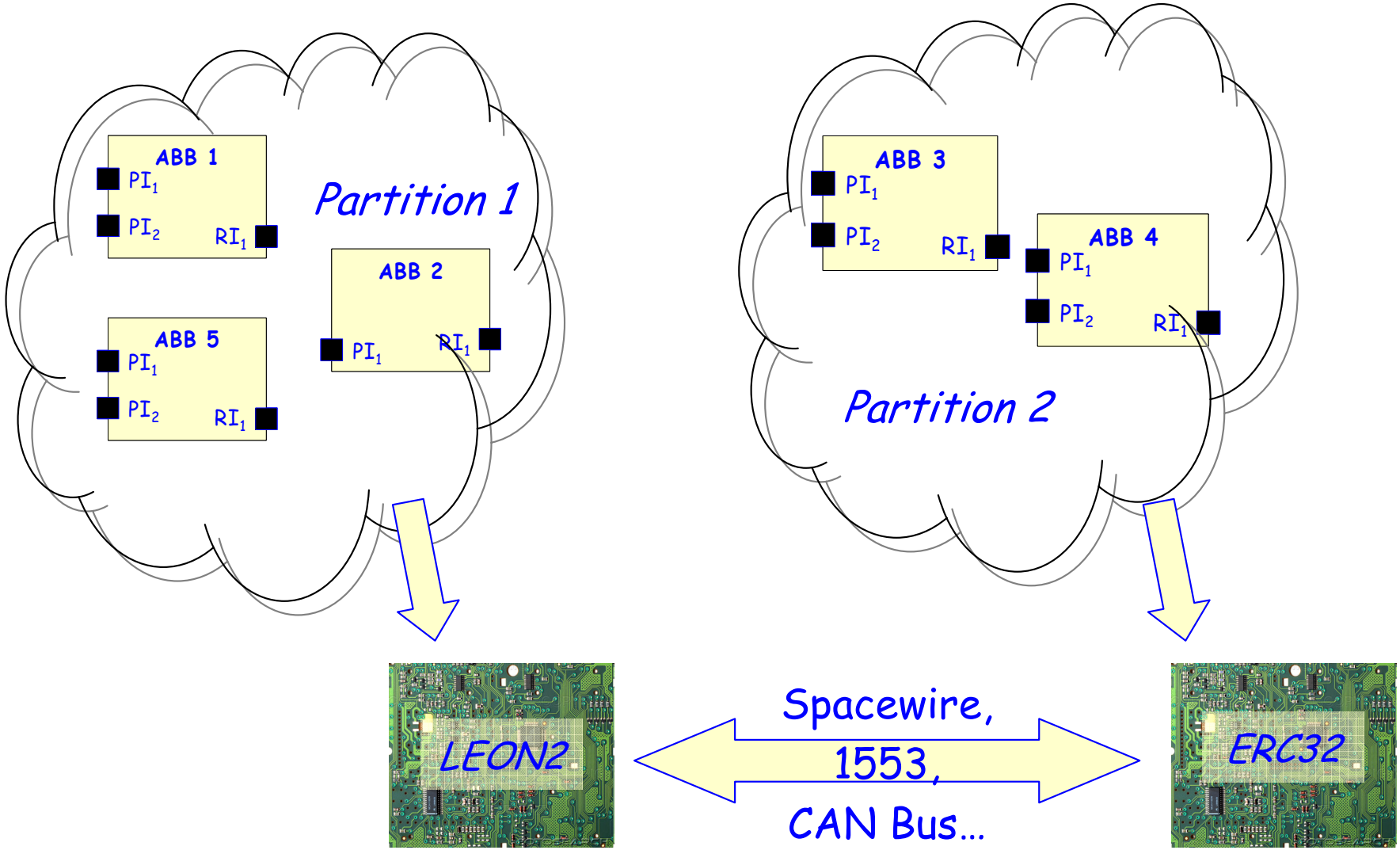
Chaque interface est enrichie de propriétés non fonctionnelles

Copyright 2004-2007 © ASSERT Project

Vue déploiement

Activity: Grouper les blocs fonctionnels en partitions, décrire le matériel, et associer les partitions aux noeuds physiques

Vue Déploiement



Copyright 2004-2007 © ASSERT Project

Containers de niveau VM

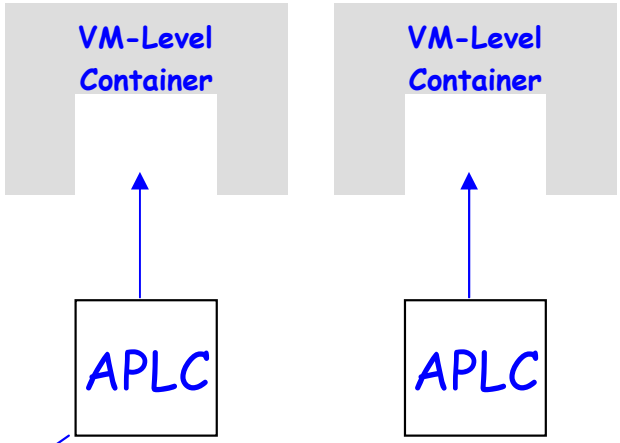
Activité: Création automatique de (groupes de) containers de niveau VM pour chaque bloc applicatif

Vues Interfaces, Données, et Déploiement décrivant les propriétés du système et sa répartition sur le matériel

Generation of VM-Level Containers

Les containers de niveau VM font le lien entre les blocs applicatifs et la machine virtuelle en préservant les propriétés non fonctionnelles.

L'outil génère des containers de niveau VM et réalise une **analyse de faisabilité** du système.



APLC: Bloc applicatif

Copyright 2004-2007 © ASSERT Project

Generation du système

Activité: Génération automatique du système final intégrant les containers de niveau VM et la machine virtuelle adaptée aux contraintes de distribution.

Génération du système

Containers de niveau VM

Machine Virtuelle

La machine virtuelle est configurée à partir des données de la vue Déploiement

Système complet

Copyright 2004-2007 © ASSERT Project

Implementation du processus ASSERT.

- **Support d'outils de modélisation:**
  - SCADE est supporté
  - ASN1c est supporté
  - Prochaine étape: Rhapsody, Matlab-Simulink, outil SDL
- **Support pour la modélisation spécifique à ASSERT:**
  - La vue Interfaces est supportée par un outil graphique
  - La vue Déploiement est en cours de développement avec AADL
- **Support de la Machine Virtuelle:**
  - La version centralisée fonctionne
  - La version distribuée fonctionne partiellement (en cours de finition)
  - Les principes de configuration sont en cours de développement

Copyright 2004-2007 © ASSERT Project

Les bénéfices du processus ASSERT

- Le processus ASSERT s'appuie sur des outils de modélisation pour capturer les exigences fonctionnelles et non-fonctionnelles
- La vision "zéro programmation" est largement supportée
- De nombreux langages et formalismes "propriétaires" sont déjà supportés: Scade, UML, AADL, SDL, ASN.1
- L'approche est centrée sur la préservation des propriétés à toutes les étapes du processus
- La machine virtuelle supporte les systèmes centralisés et distribués

Copyright 2004-2007 © ASSERT Project

ASSERT: des avancées vers l'objectif.

- **Familles de systèmes:**
  - Résultats partiels à consolider,
  - Impact sur l'organisation du secteur industriel à clarifier,
  - Ne sera pas implémenté au niveau attendu initialement,
- **Processus de développement:**
  - Une première solution mature et robuste existe,
  - Elle a déjà été implémentée par les projets pilotes,
  - Elle a démontré sa flexibilité par rapports aux besoins et aux technologies,
  - Un premier ensemble d'outil supporte le nouveau processus.
- **Composants de base:**
  - La technologie est disponible pour supporter l'adaptation des composants,
  - Certains composants de base sont utilisés dans les études de cas.

Copyright 2004-2007 © ASSERT Project

ASSERT: Conclusion et chemin pour le futur.

- **Des éléments d'un succès:**
  - De nombreux résultats techniques,
  - Un processus nouveau fait l'objet dans consensus dans le consortium et illustre la démarche en s'appuyant sur un ensemble de technologies,
  - Un niveau d'intégration élevé et une forte implication des industriels.
- **Et maintenant…**
  - Les résultats doivent être consolidés,
  - La dissémination des résultats va être accélérée, visant la communication autour du projet mais aussi la commercialisation des outils nouveaux.

En complément de nombreux résultats techniques, ASSERT a créé une communauté vivante dont l'exemple et la performance illustrent la force du collectif.

Copyright 2004-2007 © ASSERT Project