
Développement et validation
des logiciels de contrôle des véhicules spatiaux :
état de l'art et challenges

David LESENS

EADS LAUNCH VEHICLES, Route de Verneuil

BP 2, F-78133 Les Mureaux Cedex – France

Email : david.lesens@launchers.eads.net

Plan

👉 EADS LAUNCH VEHICLES

- Quinous som m es

👉 Méthodologie de développem ent d 'un systèm e véhicu le

- Développem ent
- Validation

👉 Les m éthodes form elles de spécification

- Pourquoi
- Com m ent

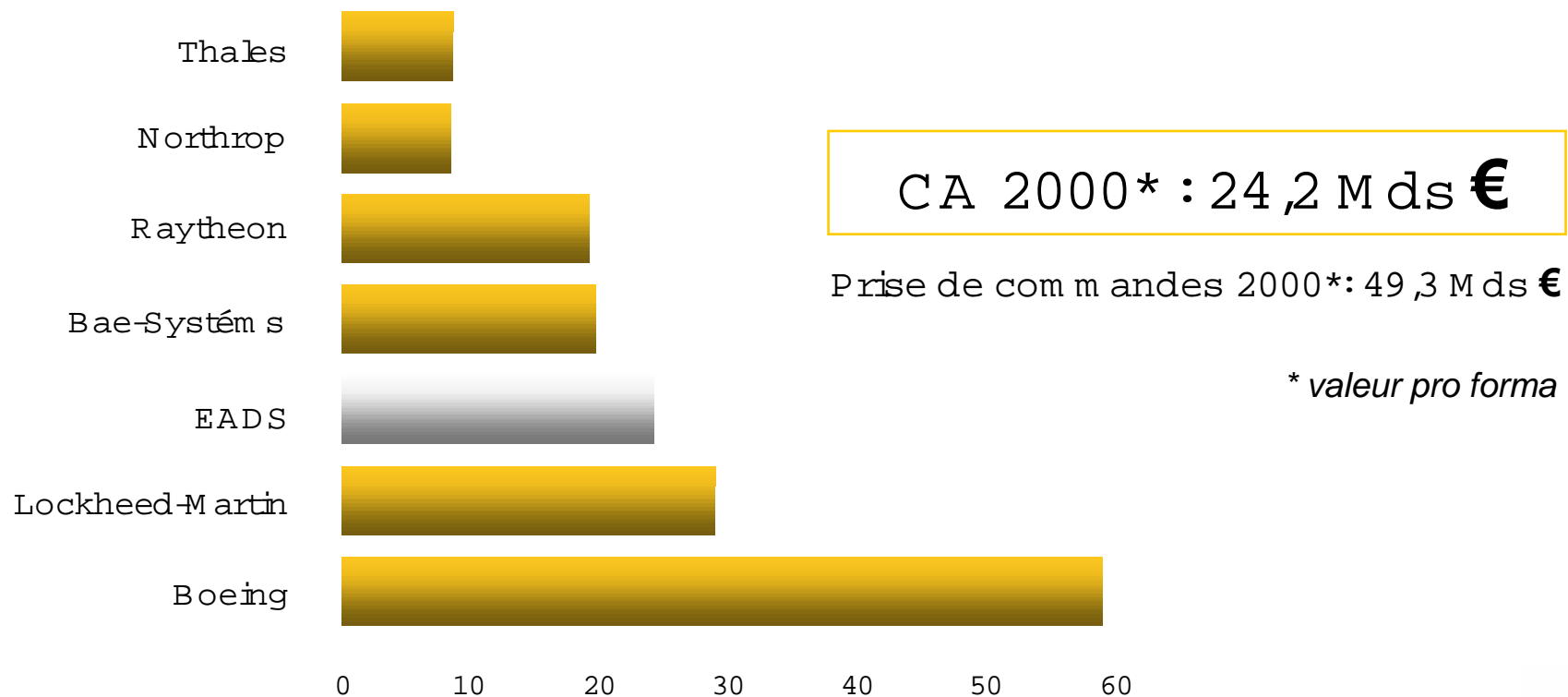
👉 Retour d 'expérien ce

- L 'Autom atic Transfer Vehicle
 - Spécification du logicièl M SU

👉 B ilan et challenges

EADS : Un acteur majeur de l'industrie aéronautique et de défense

n° 3 mondial - n° 1 européen



European Aeronautics Defence and Space company LAUNCH VEHICLES



07/2003 **SECC**

This document is the property of EADS LAUNCH VEHICLES and shall not be communicated to third parties and/or reproduced without prior written agreement. Its contents shall not be disclosed. © - EADS LAUNCH VEHICLES - 2003

Page 4



Activités phares d'EADS LAUNCH VEHICLES

Systemes
stratégiques



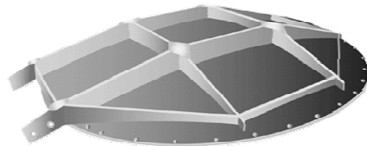
- ☞ M4 / M5
- ☞ M51
- ☞ Maîtrise de l'œuvre systèmes complets

Transport spatial



- ☞ Ariane 4
- ☞ Ariane 5
- ☞ ATV
- ☞ Soyuz
- ☞ Lanceurs complémentaires
- ☞ ARD
- ☞ ARES THEMIS

Equipements



- ☞ Equipements spatiaux
- ☞ Produits satellites
- ☞ Produits technologiques et divers

Plan

☞ EADS LAUNCH VEHICLES

- Quinous som m es

☞ Méthodologie de développement d'un système véhicule

- Développement
- Validation

☞ Les méthodes formelles de spécification

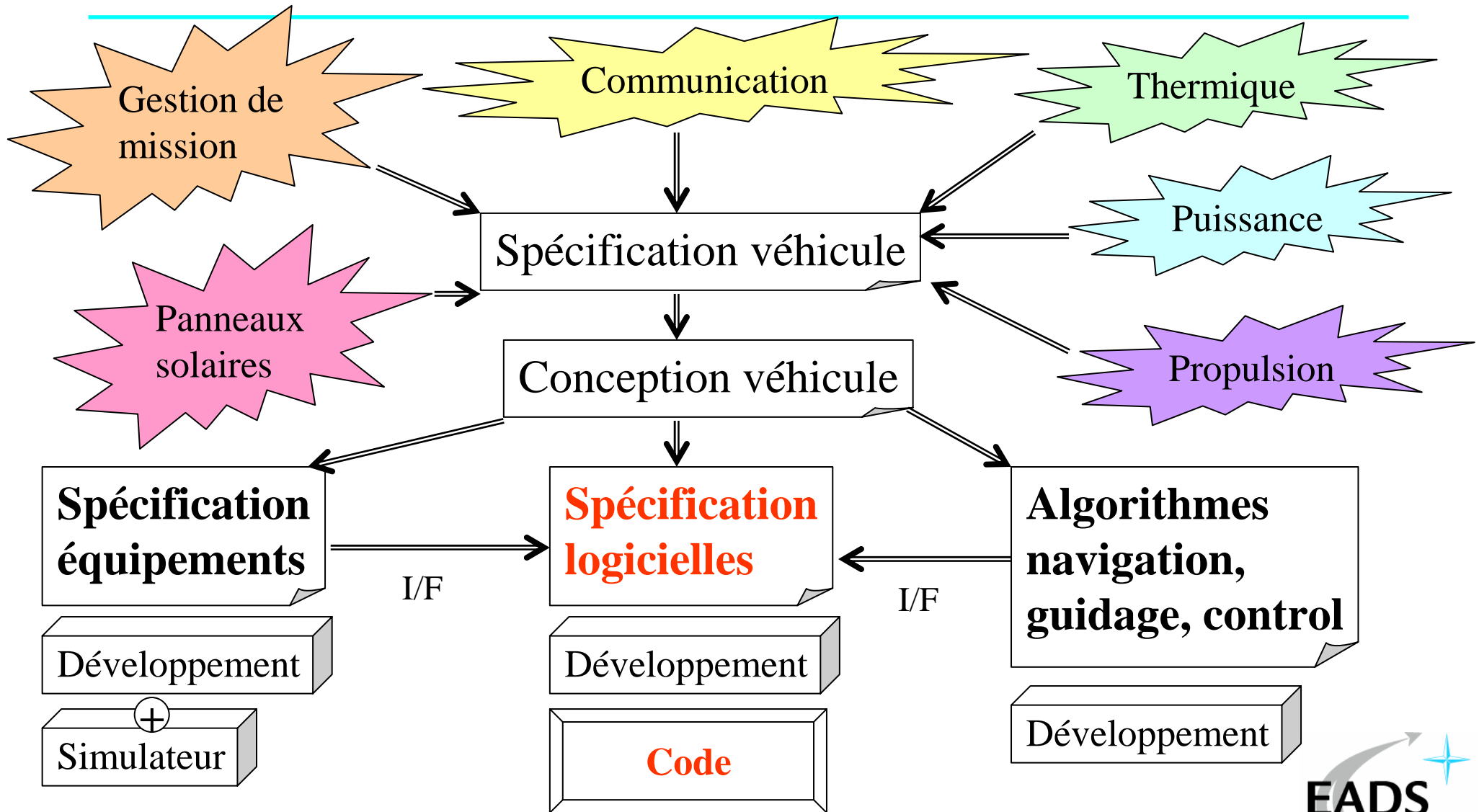
- Pourquoi
- Comment

☞ Retour d'expérience

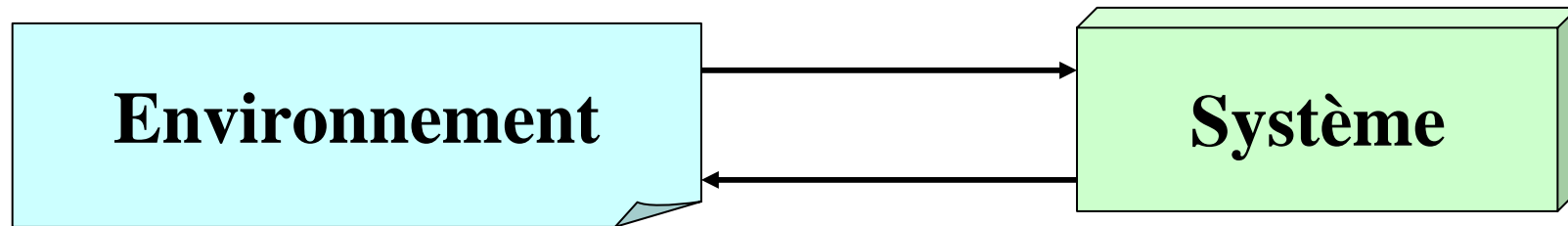
- L'Automatic Transfer Vehicle
 - Spécification du logiciel MSU

☞ Bilan et challenges

Développement d'un logiciel spatial



Un logiciel spatial est critique temps réel réactif



☞ La défaillance du système peut être **catastrophique**

- Perte **financière** > 100M € pour certains satellites
- Perte **humaine** Retombée d'un lanceur
Rendez-vous ISS

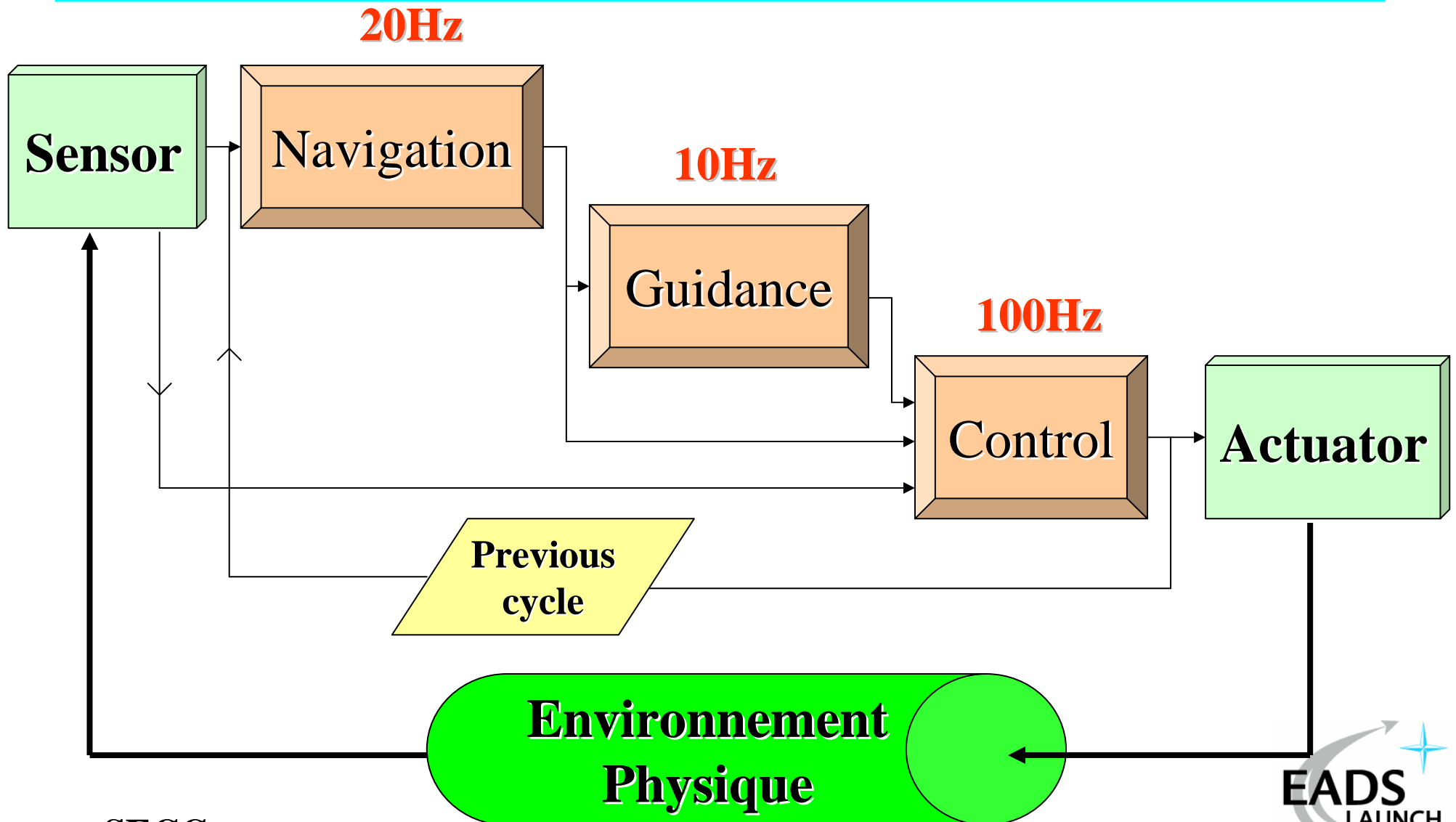
☞ Interactions système / environnement

➤ **Temps de réaction strict**

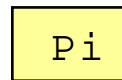
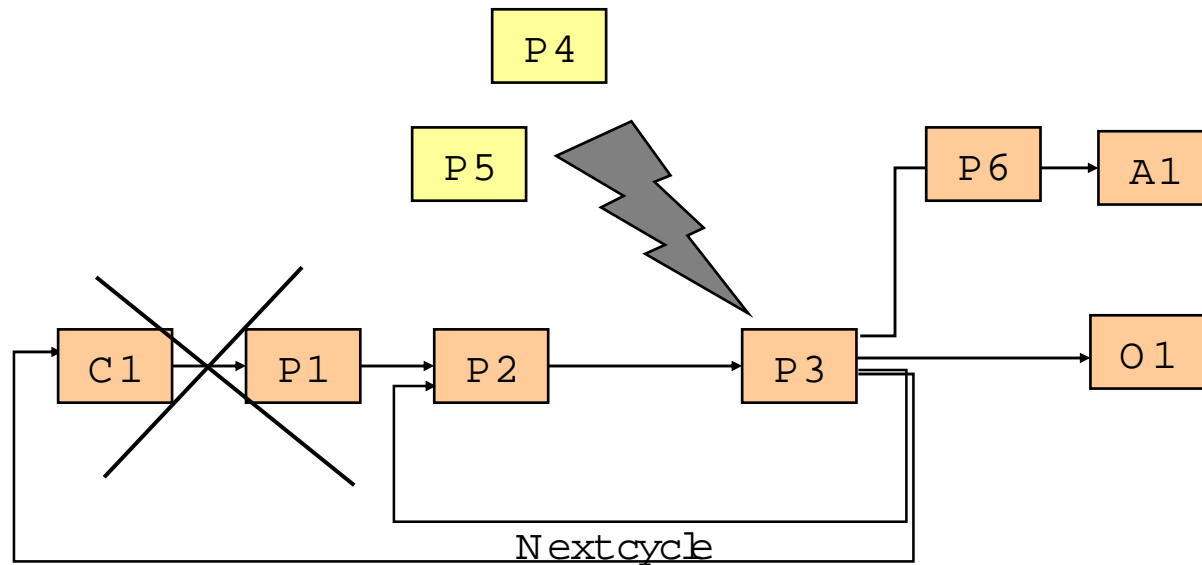
- **Contrainte de fréquence**
 - Traitement périodique type « ctrlcmd »
(précision du guidage, stabilité du pilotage)
- **Contrainte de réactivité**
 - Exigence de **sécurité**

Systèmes complexes
Plusieurs centaines
d'hommes-an
Sous-traitance

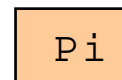
Navigation Guidance Control (GNC)



Change ment de phase



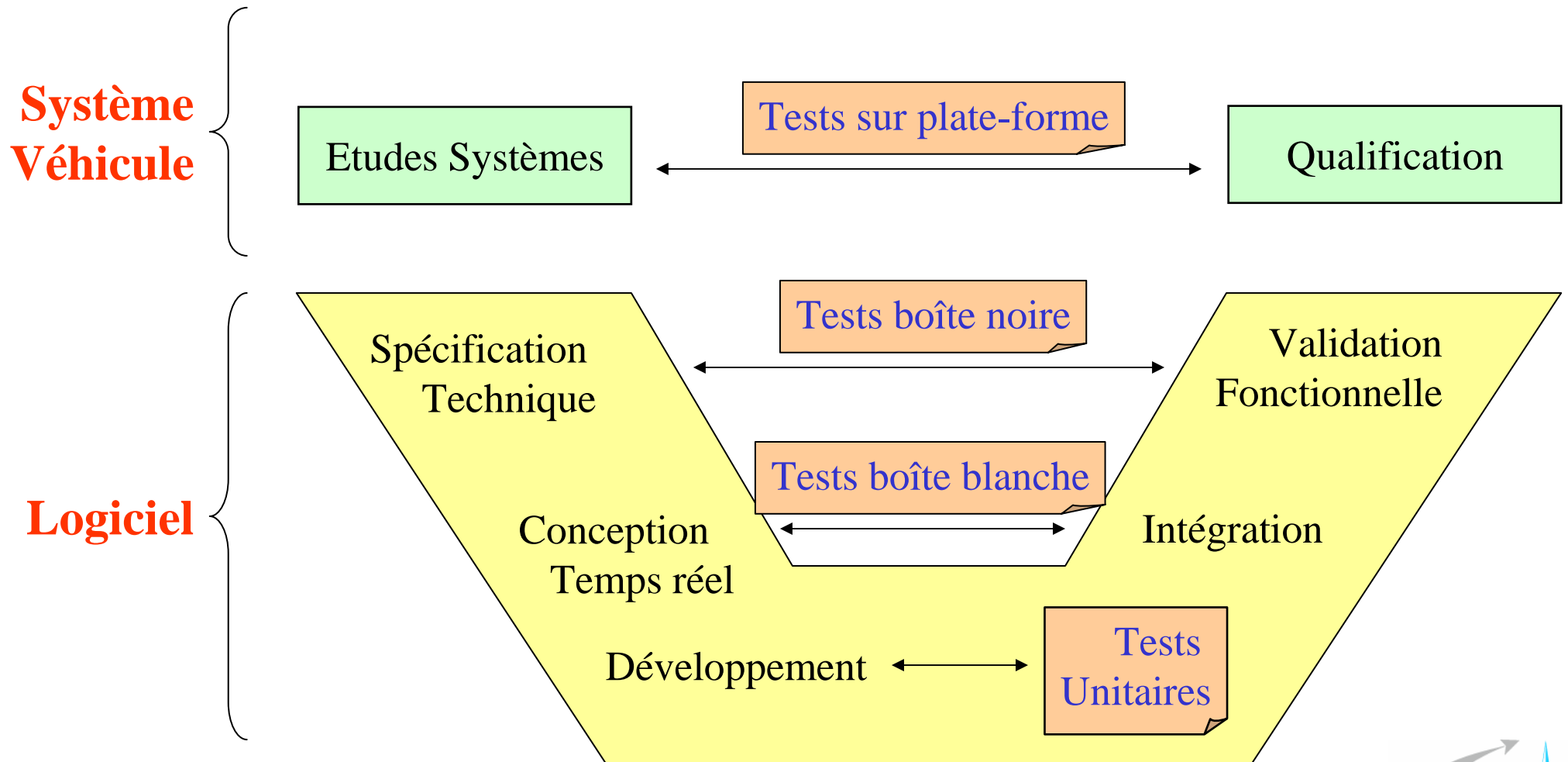
Asynchronous processes



Cyclical processes

Permanent working n°2

Cycle en V : Niveaux système / logiciel

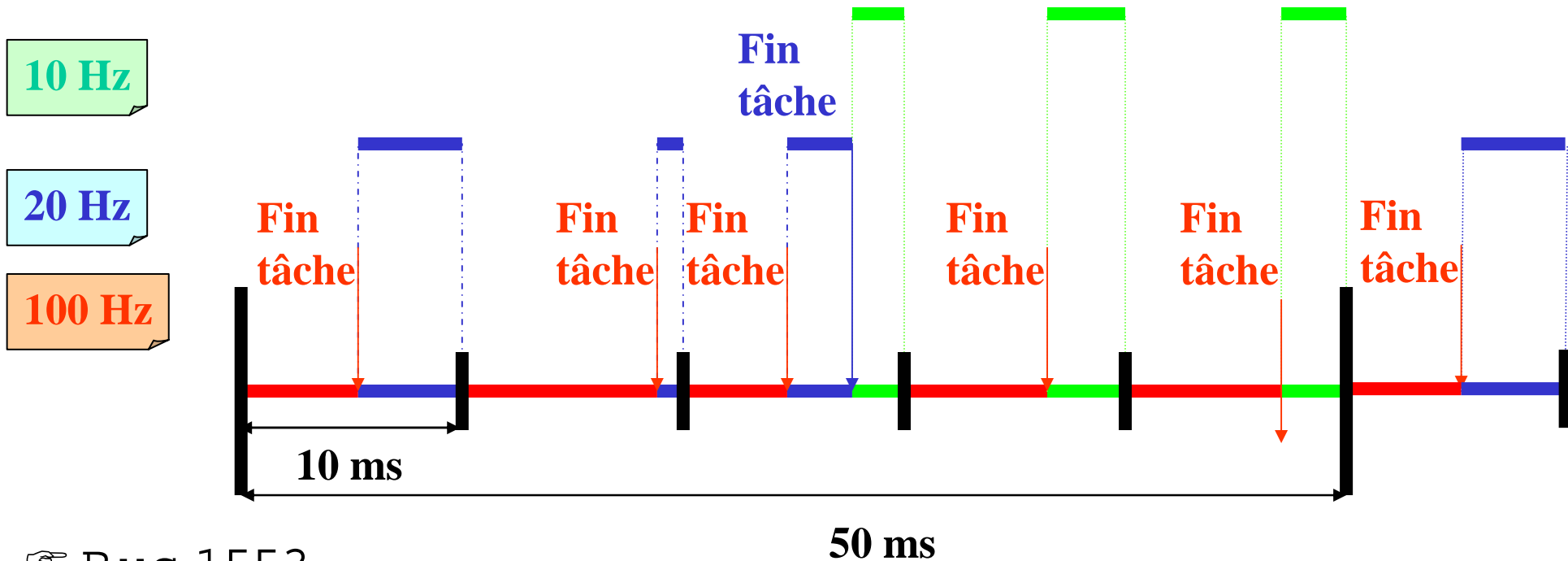


Développement du logiciel

Langage ADA

- Typage fort
- Multitâche avec priorité statique

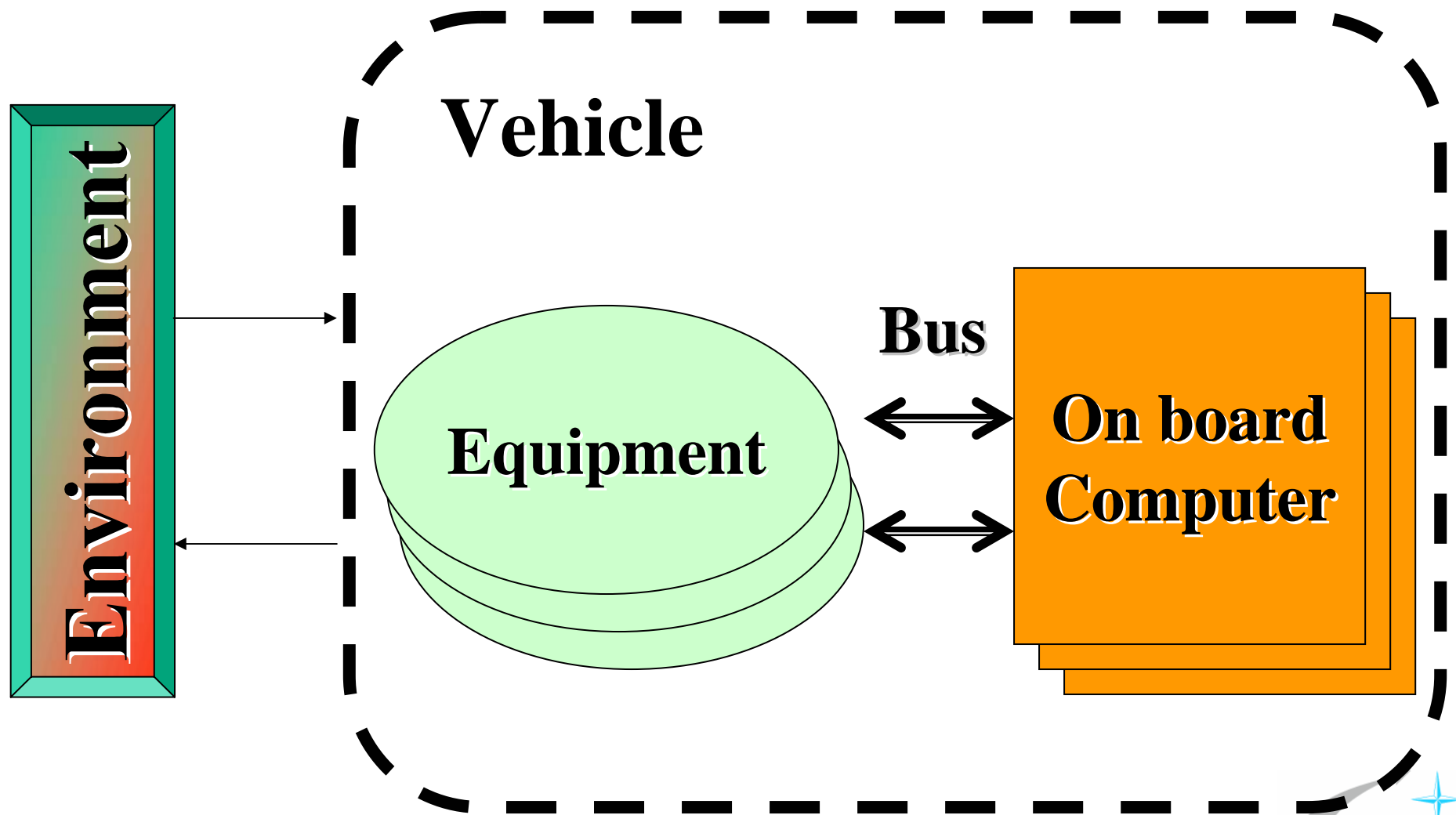
Déterminisme



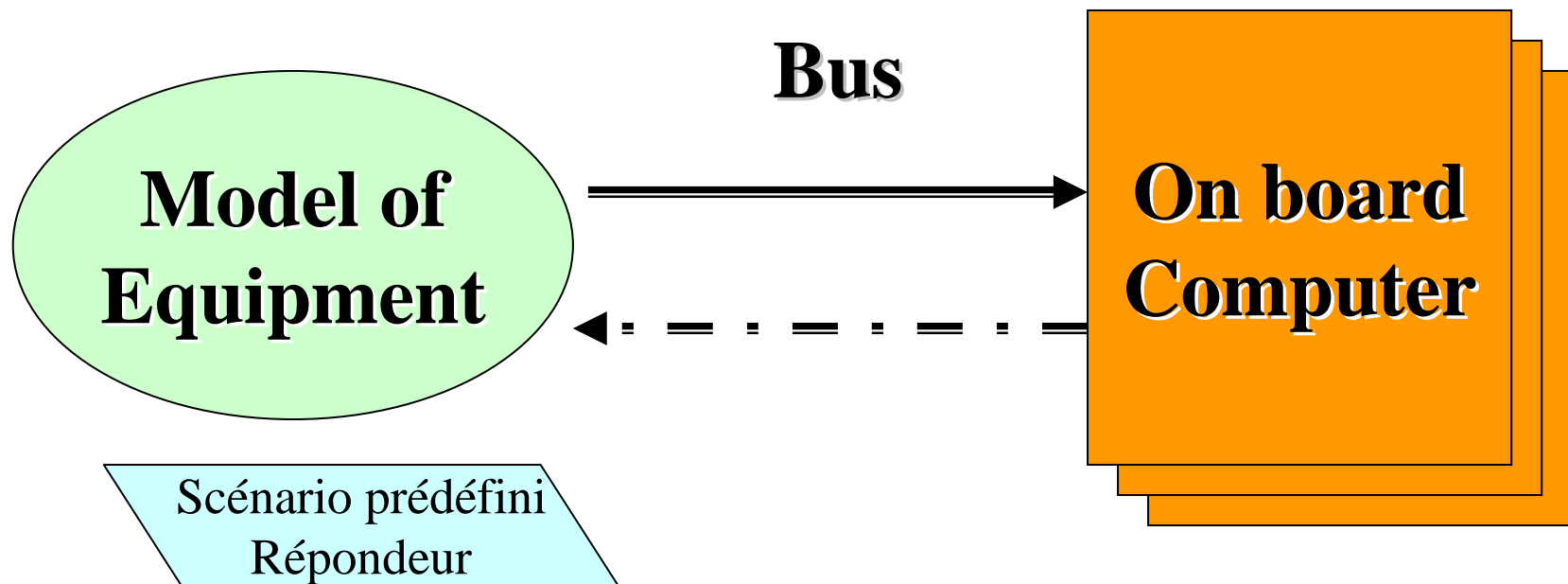
Bus 1553

- Cyclique synchrone cadencé par le BC

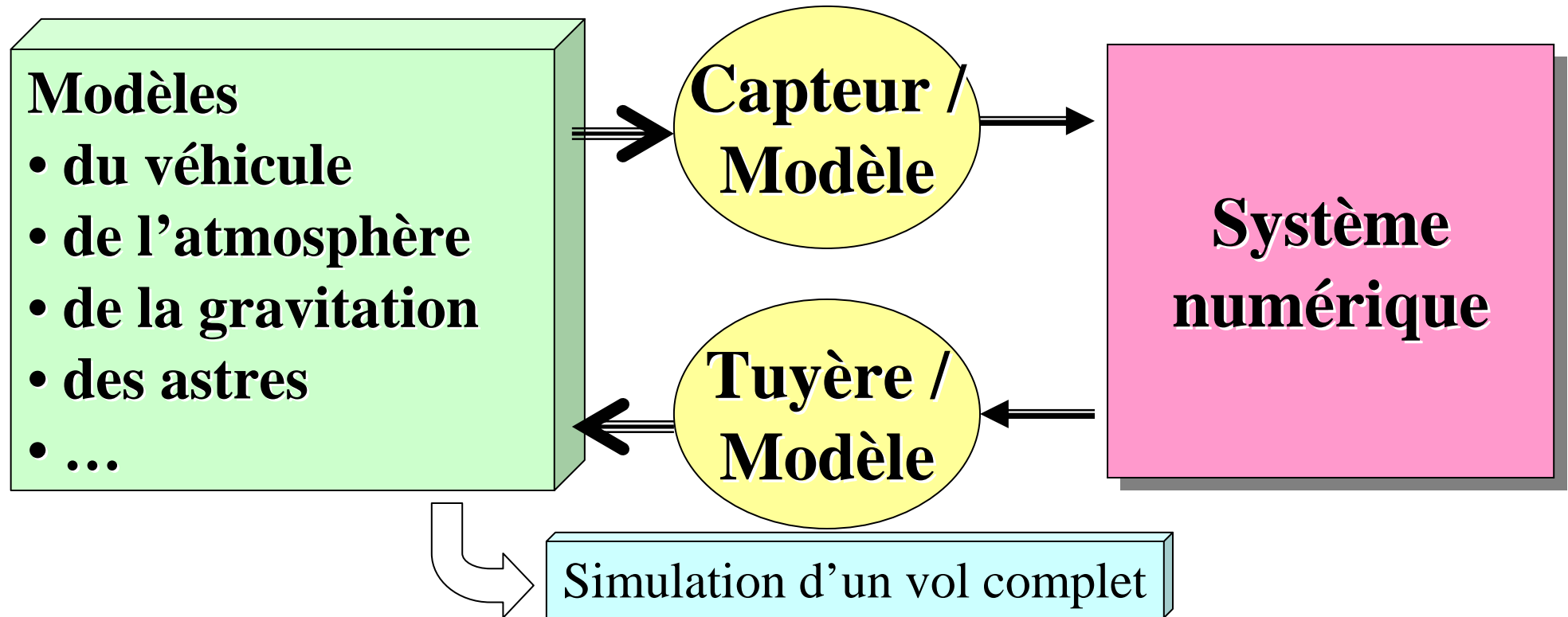
Validation : Le logiciel n'est qu'une brique d'un ensemble complexe



Simulation en boucle ouverte

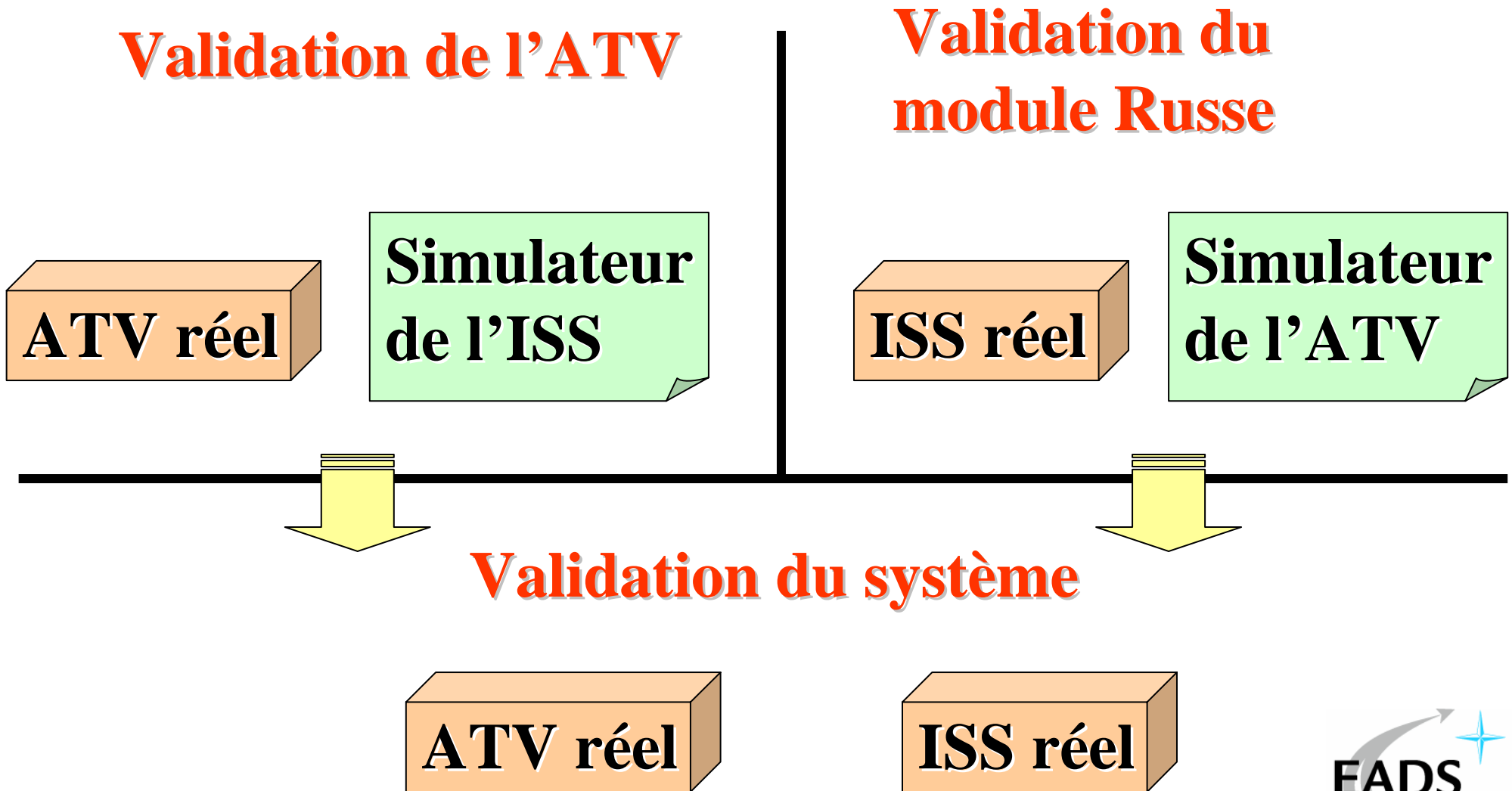


Simulation en boucle fermée



- **Pas de vol d'essai**
- **Le premier vol est un vol de qualification**

Qualification système : Utilisation de simulateur



Plan

☞ EADS LAUNCH VEHICLES

- Quinous som m es

☞ Méthodologie de développem ent d'un systèm e véhicule

- Développem ent
- Validation

☞ Les m éthodes form elles de spécification

- Pourquoi
- Com m ent

☞ Retour d'expérience

- L'Autom atic Transfer Vehicle
 - Spécification du logiciel M SU

☞ B ilan et challenges

Objectif de la spécification (logicielle)

☞ Capturer le besoin système / **Formalisation** du besoin

- Standard de communication :
 - Pour des informaticiens / **non informaticiens** (spécialistes métiers)
- Différents types d'application
 - Synchrones **et/ou** asynchrones **et/ou** algorithmiques

☞ Détecter les erreurs en **phase amont** de développement

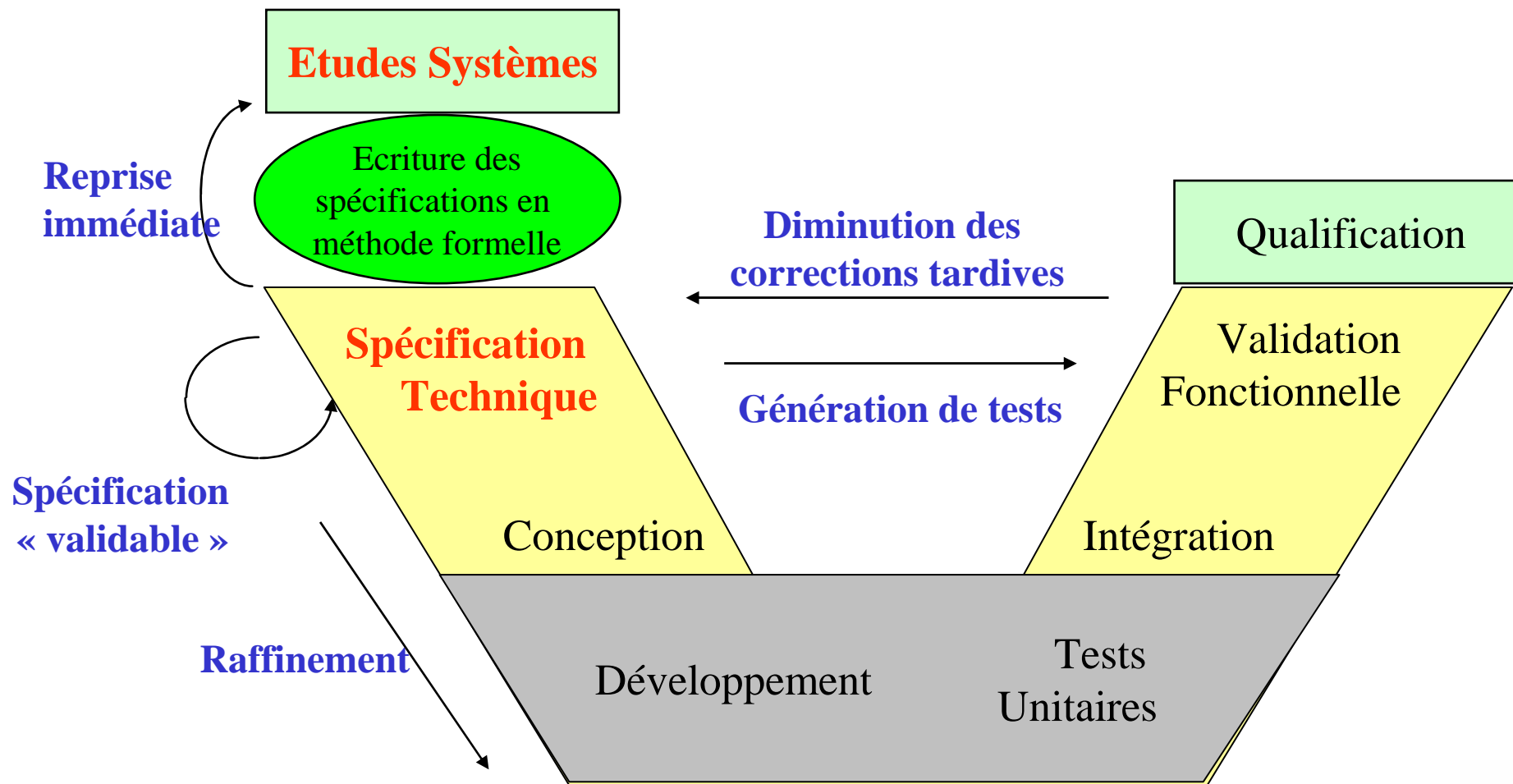
- Cohérence et complétude de la spécification
- Validation de la spécification / **système**
 - Relecture (interne + système)
 - Test / Preuve sur la spécification

☞ Faciliter le **raffinement** de la spécification vers une conception

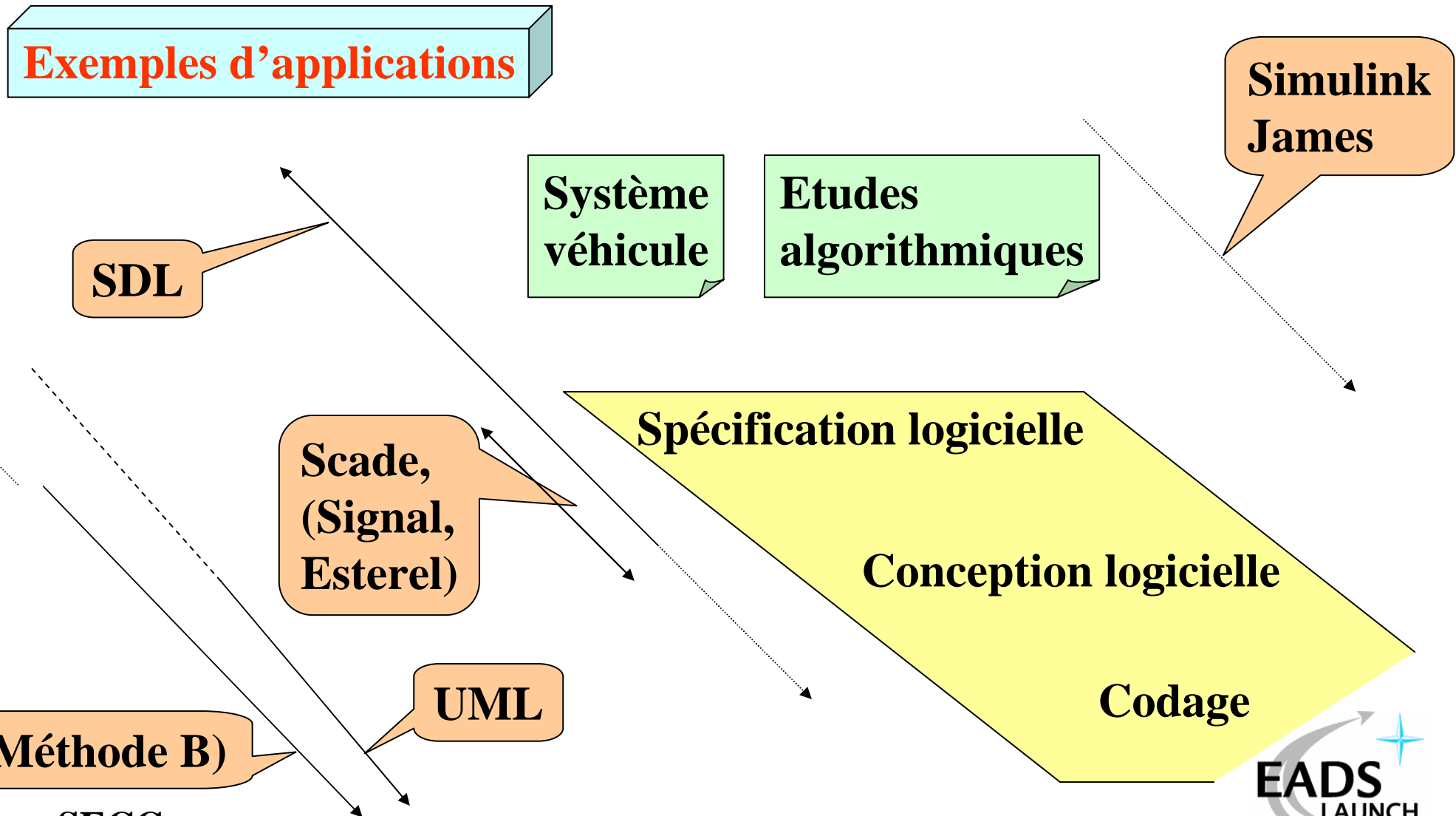
- Formalisation de la conception
- **Génération de code**

Importance de la spécification

Pourquoi utiliser des méthodes formalisées ?



Quelles méthodes « formelles » choisir?



Et en pratique ? Soyons pragmatiques !

👉 Les méthodes formelles sont lourdes à utiliser

➤ Utiliser selon les **besoins**

👉 Modélisation **statique**

➤ Type SADT ou SART

- Vérification de la cohérence des flots de données

👉 Modélisation **dynamique**

➤ Meux comprendre un point dur

➤ Simulation / validation

En support
d'une spécification
ou d'une analyse

👉 **Spécification**

👉 **Développement complet**

➤ Spécification véhicule

➤ Code embarquable

Nos challenges

Plan

☞ EADS LAUNCH VEHICLES

- Quinous som m es

☞ Méthodologie de développem ent d 'un systèm e véhicule

- Développem ent
- Validation

☞ Les m éthodes form elles de spécification

- Pourquoi
- Com m ent

☞ Retour d 'expérience

- L 'Autom atic Transfer Vehicle
 - Spécification du logiciel M SU

☞ Bilan et challenges

The Automated Transfer Vehicle (ATV) context

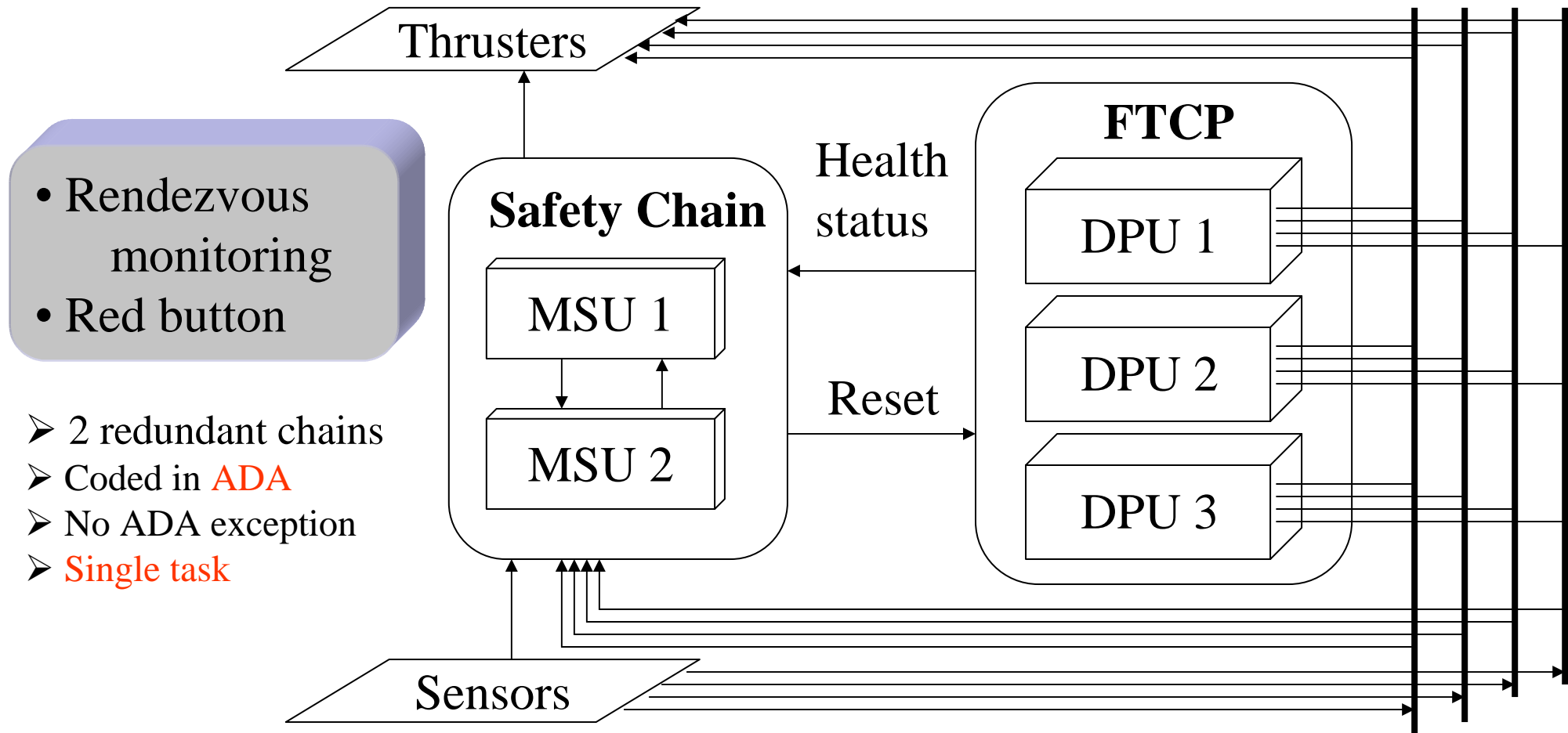
One of the European contributions to the International Space Station (ISS).

It will supply from 2004 onward the following services to the ISS :

- Refuelling ,
- ISS orbit correction ,
- Freight delivery ,
- ISS trash destruction .



ATV safety chain and Collision Avoidance maneuver



- Rendezvous monitoring
- Red button

- 2 redundant chains
- Coded in **ADA**
- No ADA exception
- **Single task**

Responsible of ISS safety by triggering a CAM

How the MSU software is specified ?

Technical Specification of the MSU SW

- State automaton
- MSU SW architecture
- CAM sequencer

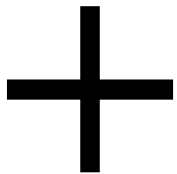
SCADE modeling

- Non functional requirements
- Functional requirements

FrameMaker editor

Algorithms Reference Documents

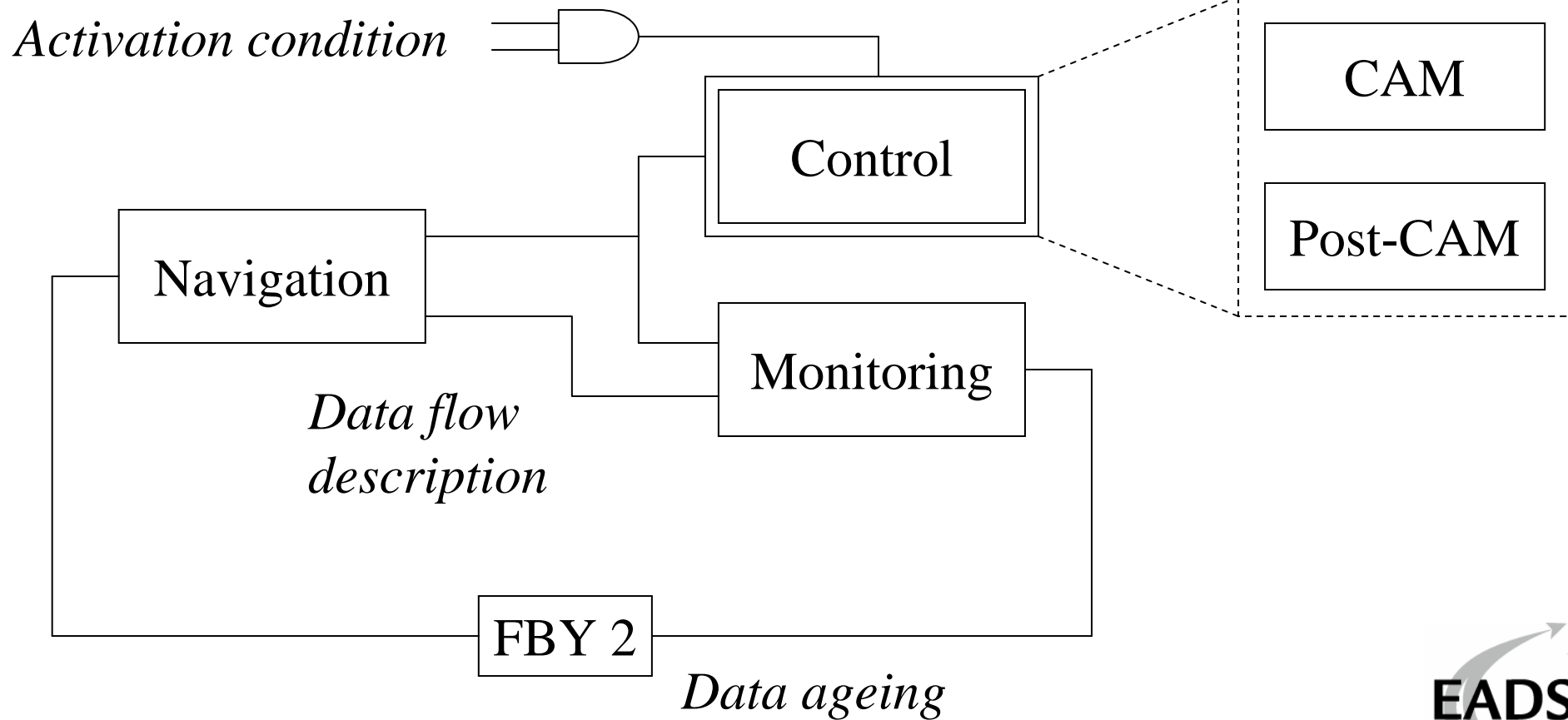
GNC algorithms



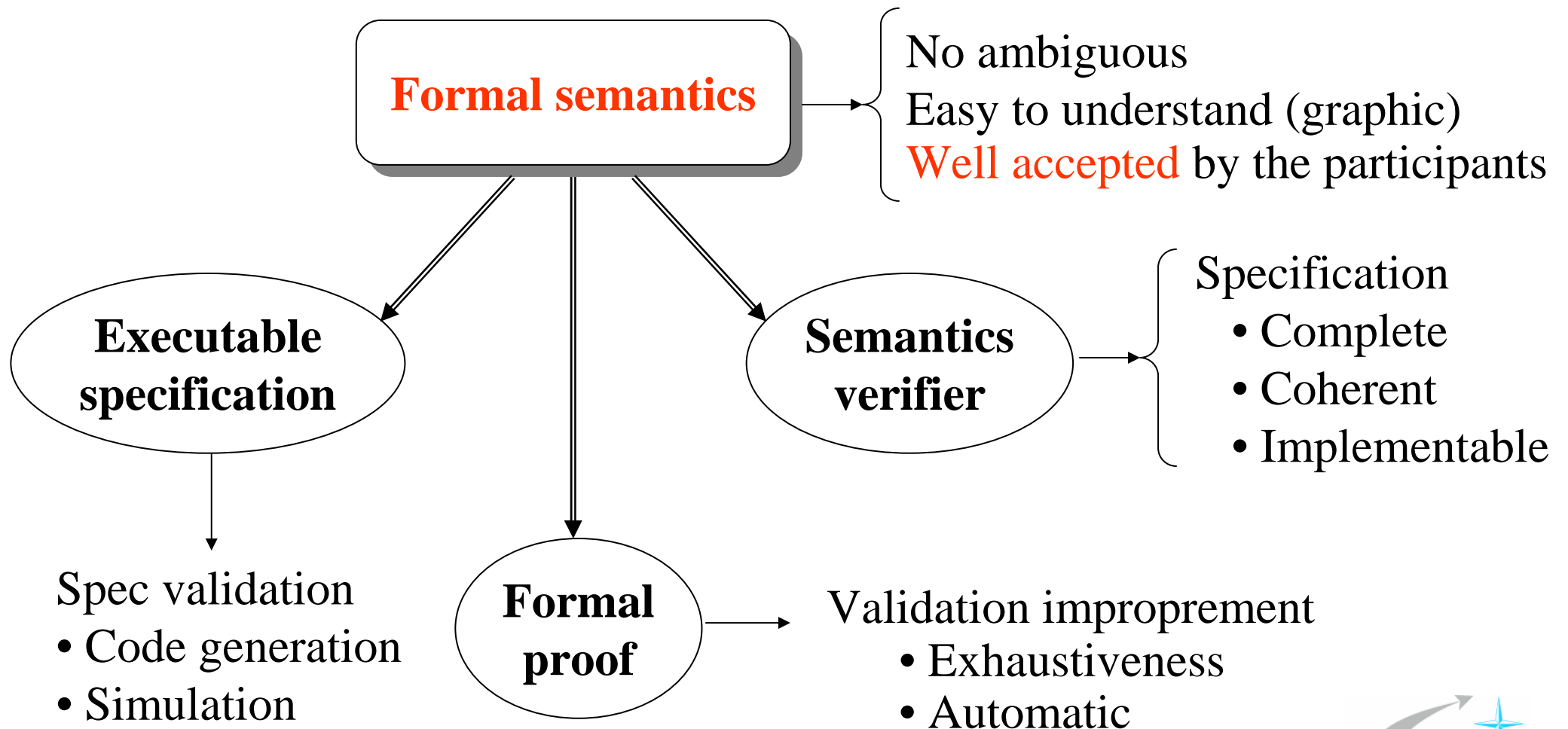
Contents of the MSU SW SCADE model

Synchronous and cycle architecture

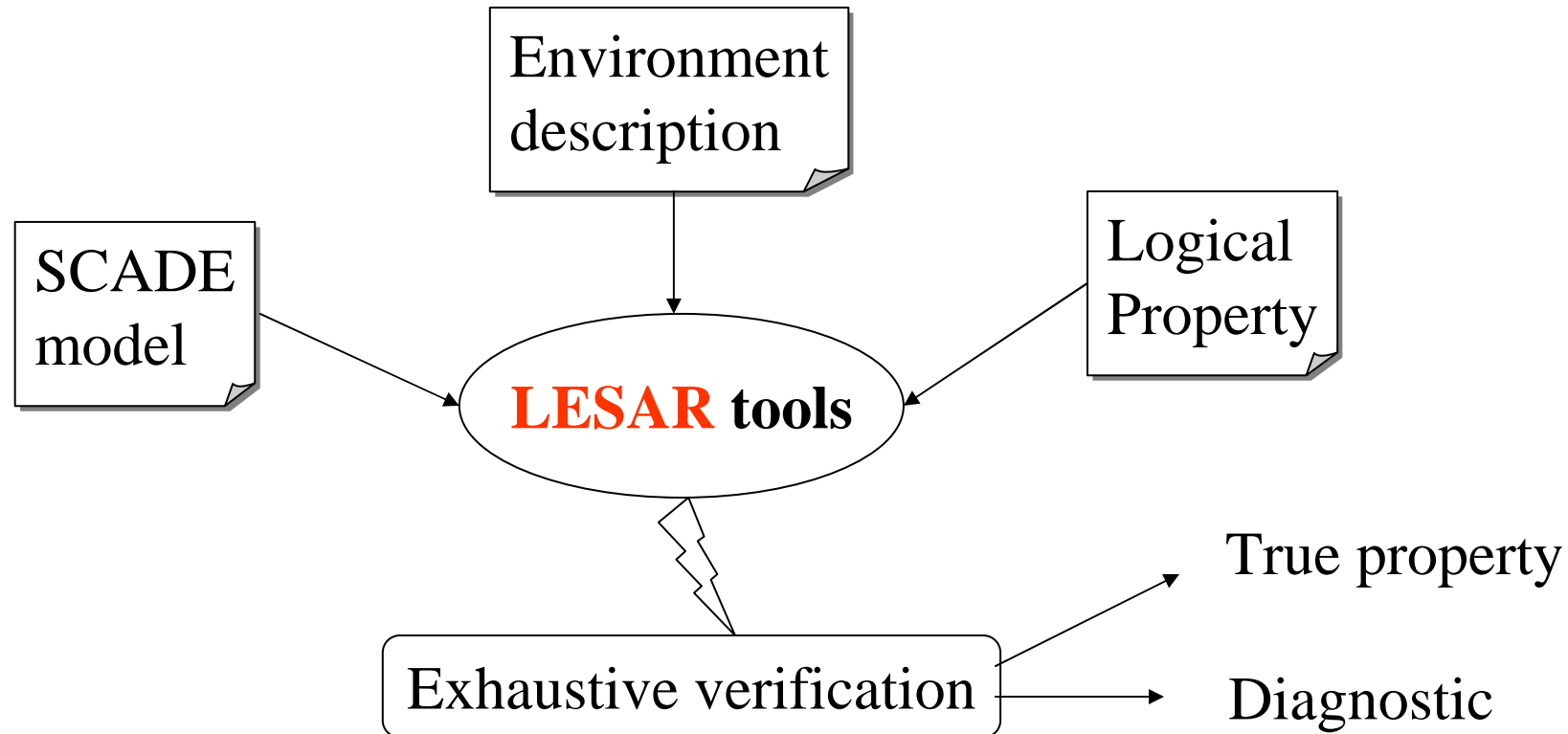
Hierarchical decomposition



Validation of a SCADE specification



Formal proofs on the MSU SW TS

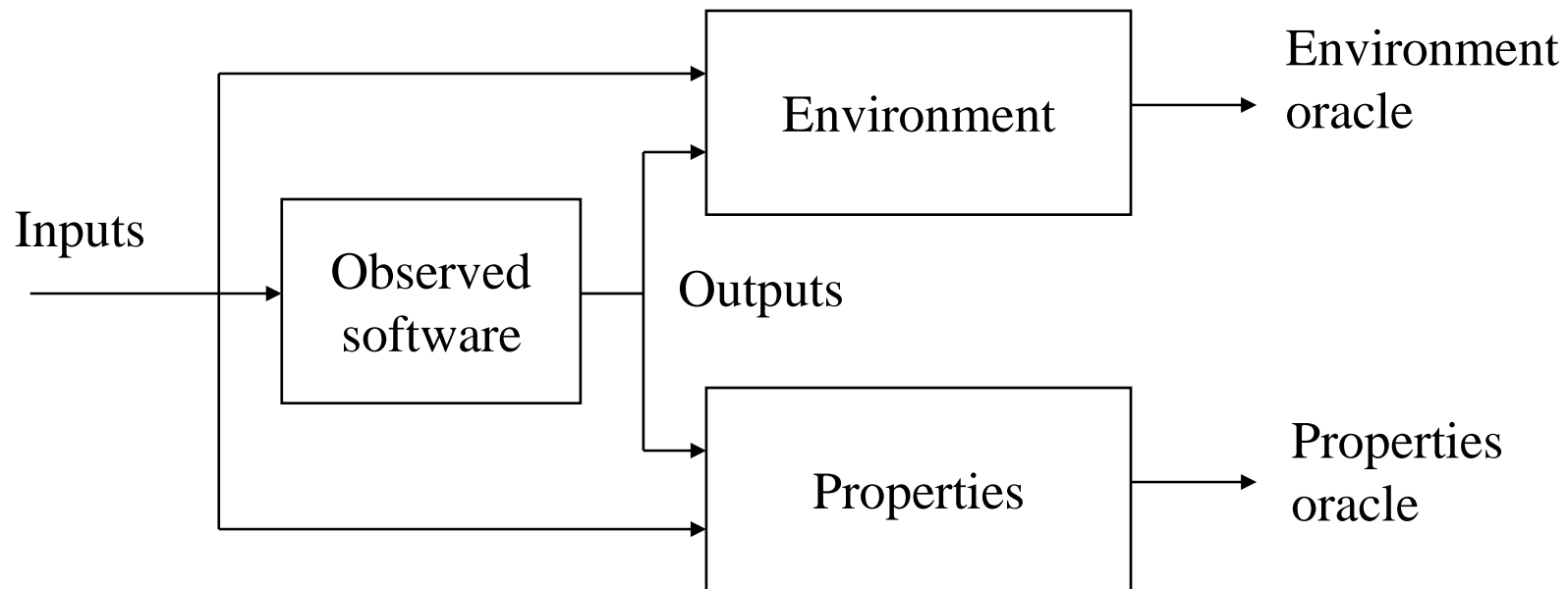


LESAR tool is developed by the **VERIMAG** laboratory

Properties description

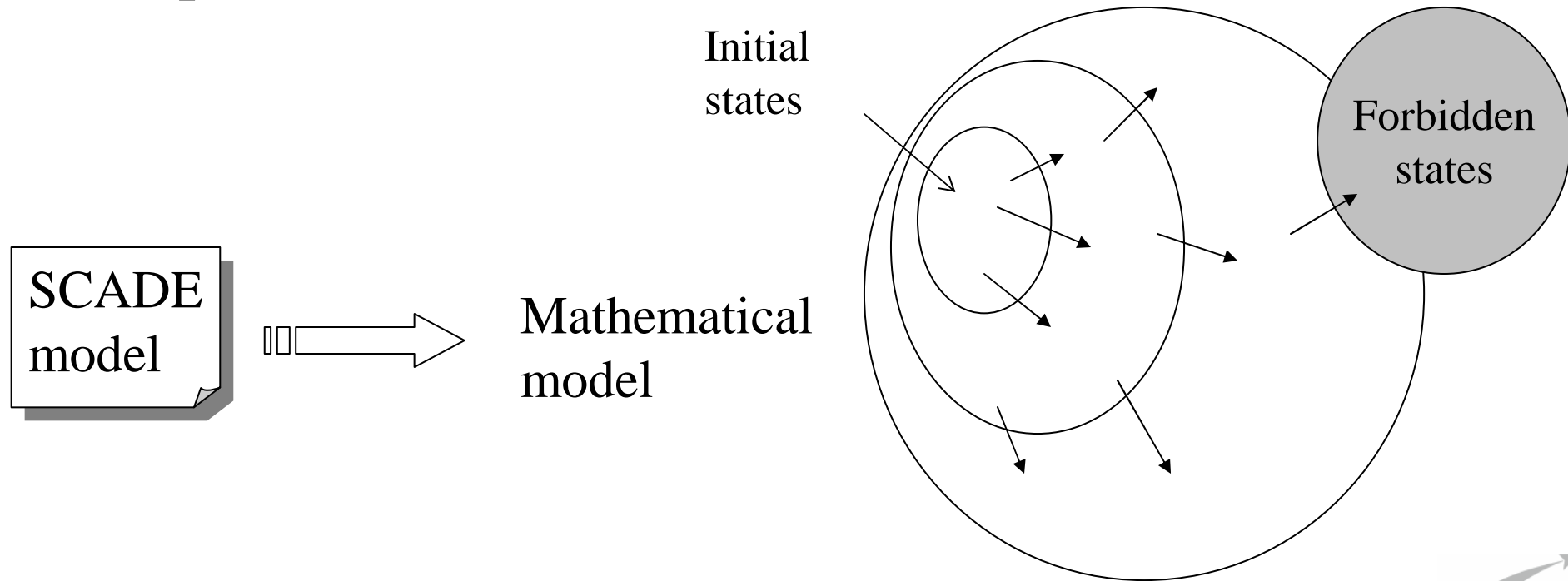
☞ Use of synchronous observer, specified

- In SCADE
- In LUSTRE
- Using regular expression



Proof by model checking

- Construction of a mathematical model of the SCADE model
- Computation of the reachable states
- Comparison with the forbidden states



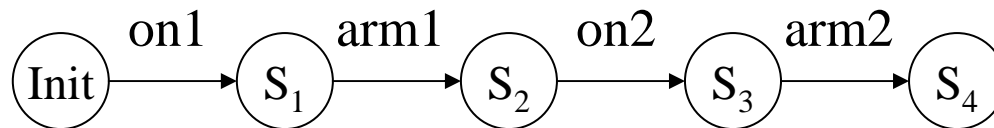
Property examples

☞ A CAM test can only be triggered by a "red button" signal

- `true_after_false(CAM_TEST_TRIG) ⇒ RED_BUTTON`
- No assertion is required from the environment to satisfy this property.

☞ When the initialisation of the two MSU chains is correct, they can not triggered both a CAM at the same time

- `!(MSU1_CAM_TRIG, MSU2_CAM_TRIG)`
- It is satisfied only when the initialisation of the 2 MSU is correct
- `cam_arm(SWITCH_ON_MSU1, ARM_MSU1, SWITCH_ON_MSU2, ARM_MSU2, RED_BUTTON)`



Conclusion on formal method use for ATV



- Description of a MSU **cyclic** and **synchronous architecture**
- Formal semantics (no ambiguity, no incoherence)
 - . Data flow / Activation condition
 - . Data obsolescence description
- MSU SW TS **easy to understand**
- Semantics verification / Formal proof



Definition of properties at **system level**

- Non adapted for **asynchronous** software
- Limited to small, cyclic, synchronous software
- Start of the MSU software **design**



*Improve the **quality** of the TS of the MSU Software*

*Not usable for a **complex** software*

Plan

☞ EADS LAUNCH VEHICLES

- Quinous som m es

☞ Méthodologie de développem ent d 'un systèm e véhicule

- Développem ent
- Validation

☞ Les m éthodes form elles de spécification

- Pourquoi
- Com m ent

☞ Retour d 'expérien ce

- L 'Autom atic Transfer Vehicle
 - Spécification du logiciel M SU

☞ Bilan et challenges

Prospectives (1)

Amélioration des techniques de spécification utilisées

☞ Des techniques de spécification

- Mixer synchrone et asynchrone
- Raffiner de l'asynchrone vers du synchrone
- ...

☞ Des techniques de preuve

- Spécification des propriétés
- Puissance des outils
- ...

Prospectives (2)

Amélioration de la méthodologie

Extension des méthodes formelles en amont et en aval

➔ Étendre l'approche formelle au **systeme véhicule**

- Utilisation par des **non** informaticiens
- **Raffinement**
- **Culture** d'entreprise

➔ Génération automatique de code

ACG (1): Existants et méthode

➡ A EADS LAUNCH VEHICLES

- Système de missiles Stratégiques
 - SCALA
 - ROBERT

➡ Problématique de la « certification »

ou de la justification au client

- Certification du générateur de code
 - Pour le type de logiciel / Pour le calculateur
- Cycle en V
 - Validation de la spécification (i.e. du modèle)

ACG (2): Technique de génération de code

Techniques de conception

- Langages de compilation
- Architectures multi-tâches / réparties
- ...

Compatibility

- Between semantics
- Between tools
- Between generated code

