MARAE: Component-based proven-by-construction robust control software for space autonomy

Jean-Paul Blanquart, Saddek Bensalem, Félix Ingrand, David Powell

ASTRIUM Satellites, Verimag, LAAS-CNRS

ADCSS-2011 – MBAVV

Noordwijk, October 26th, 2011

Motivations

- Advanced autonomous systems
  - Complexity, variability, low predictability
  - Criticality
    - Validation
    - Property enforcement at run-time
- Combination of approaches
  - Layered architecture
  - Modular programming
  - Model-based approaches
  - Component-based approaches
  - Guaranteed properties (by construction)
  - Formal validation
  - Robustness testing

MARAE

Robust Architecture and Method for Autonomy in Space

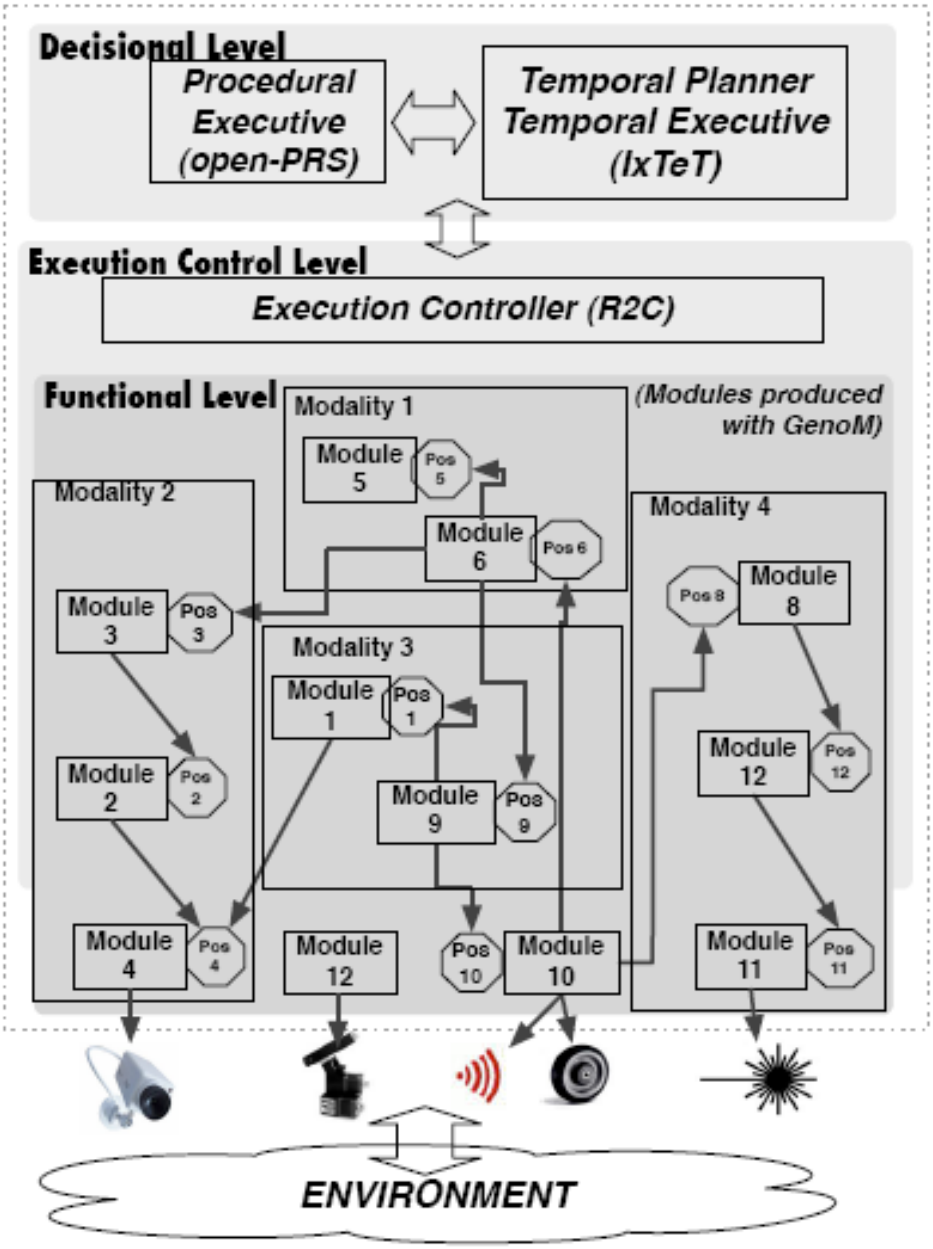
- French Collaborative project
  - FRAE
  - 3 years (Jan.2008-Jan.2011)

- Academic partners
  - LAAS-CNRS
    - Robotics (RIS) (Project Coordinator)
    - Dependability (TSF)
  - VERIMAG

- Industrial partner
  - Astrium Satellites

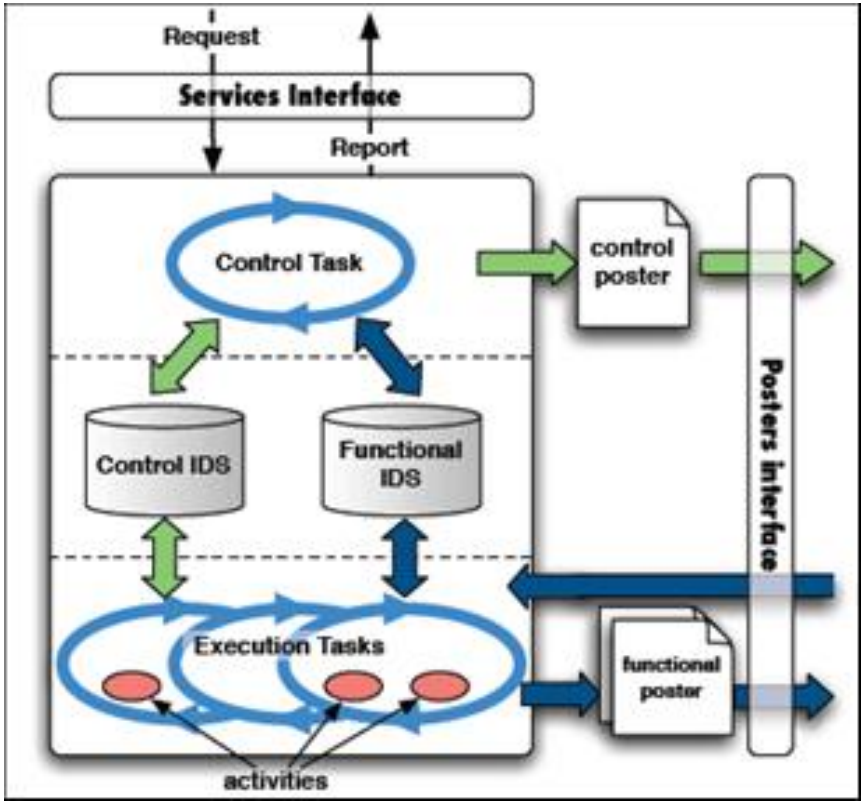
Background

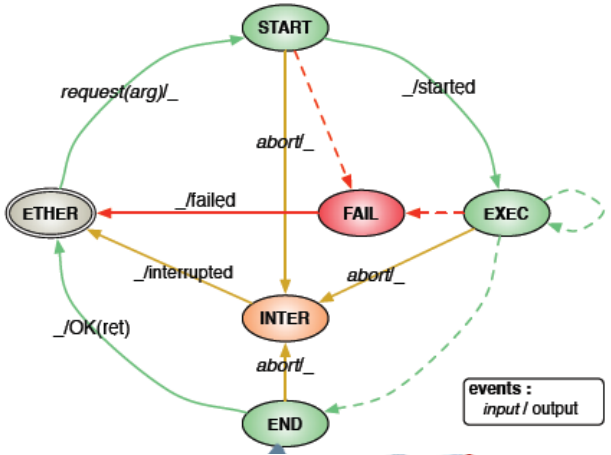
- Layered architecture
  - Hierarchy of roles, decision making capability, temporal granularity
- Functional level
  - Key for safety and appropriate trade-off w.r.t. availability



Background GenoM

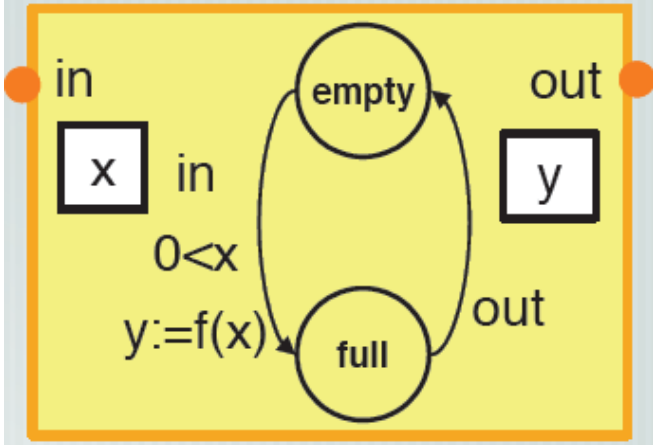
- GenoM
  - Generic architecture of modules
    - Services
    - Posters
    - Activities
    - Control task
  - Automatic generation
  - + functional code
    - “codels”

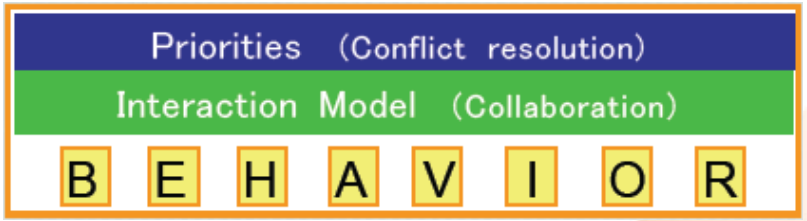


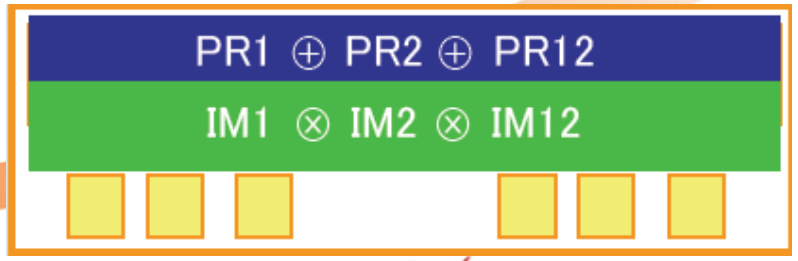


Background
BIP (Behaviour, Interactions, Priorities)

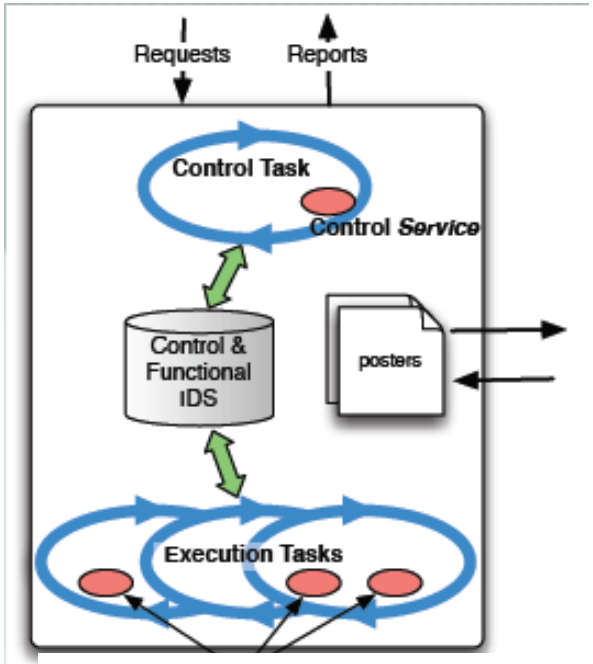
- Layered component model
  - Heterogeneous components
- Composition (incremental description
- Synthesis of controller
- Property preservation
- Validation
  - D-Finder
  - Compositional verification of invariants

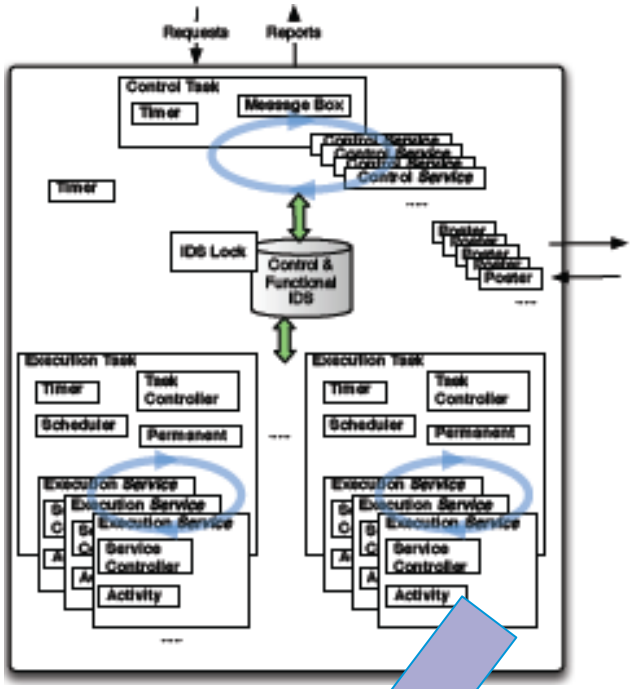


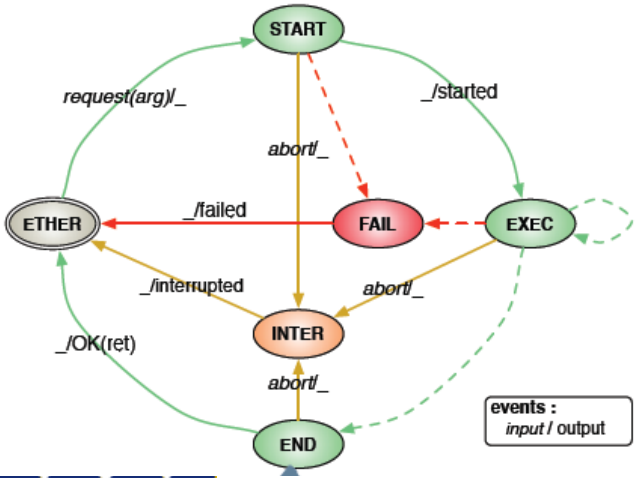


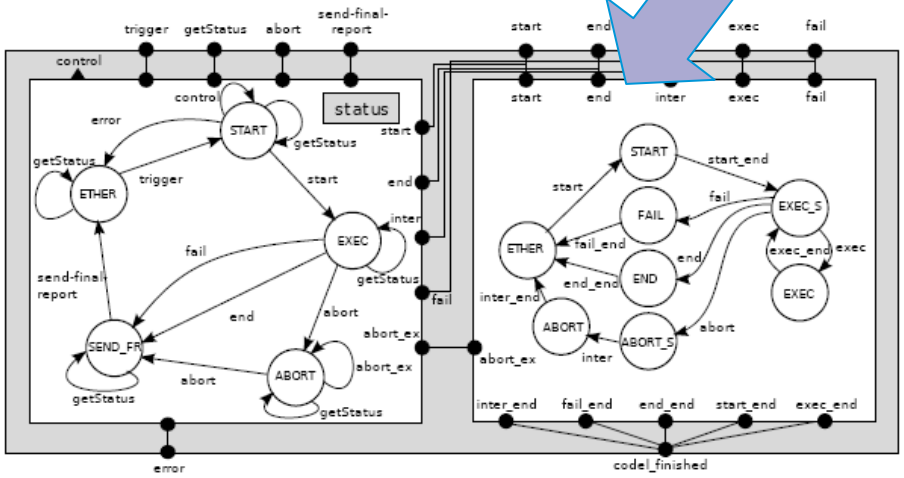


From GenoM to BIP









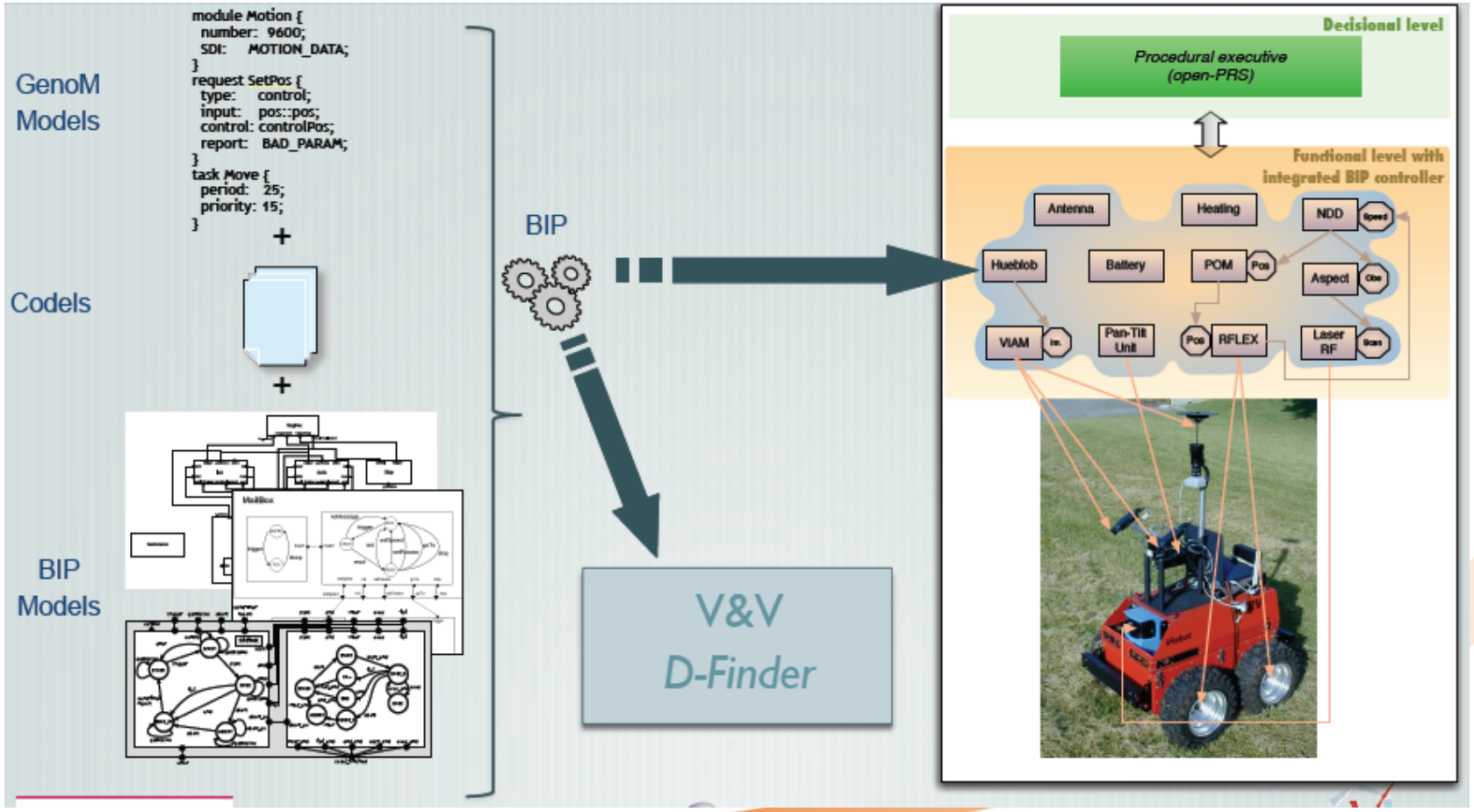
Properties

- Intra- and Inter- modules
  - Causality
    - Use an equipment after proper initialisation
  - Mutual exclusion
    - Do not use both instruments A and B
  - Pre-condition
    - Take a picture if rover does not move
  - In-condition
    - Navigation needs fresh enough environment data
  - …

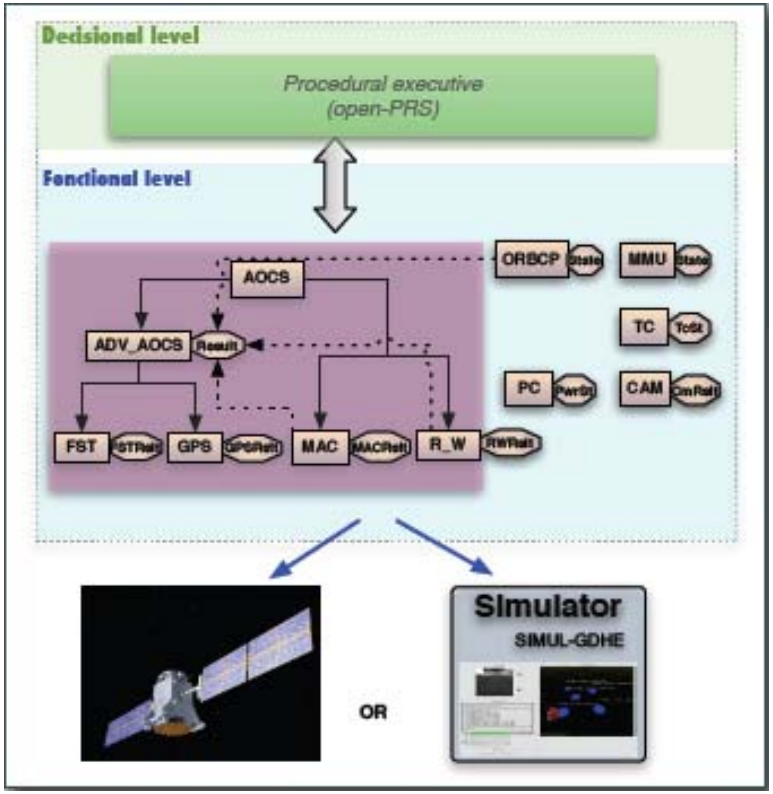
Robustness testing

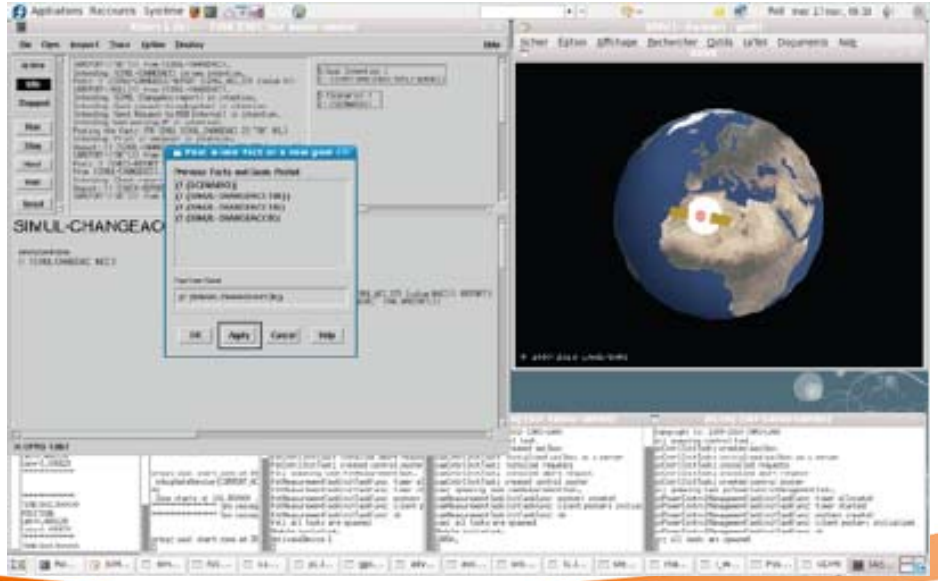
- Invalid inputs
  - Invalid in time
    - Requests at wrong time
    - Improper order
- Elicit robustness timing properties and action (reject, queue…)
- Execute plans with mutations
  - Record execution traces
- Analyse traces

Demonstrator 1
Rover



Demonstrator 2
Satellite (simulator)





Perspectives

- GOAC (Goal Oriented Autonomous Controller), ESTEC, GMV, ISTC/CNR, VERIMAG, LAAS
- Real-time BIP, distributed BIP
- Specifications, properties
  - Higher language
  - Tool support
- Robustness testing
  - More automatic support to trace analysis
  - Analysis, reduction of false observations
  - Definition of properties