A TOOL-CHAIN FOR FUNCTIONAL SAFETY AND RELIABILITY IMPROVEMENT IN AUTMOTIVE SYSTEMS

R. Nouacer, M. Djemal, **S. Niar**, G. Mouchard, N. Rapin, J.P. Gallois, P. Fiani, F. Chastrette, T. Adriano and B. Mac-Eachen

reda.nouacer@cea.fr
smail.niar@univ-valenciennes.fr

https://equitas-project.com/site/

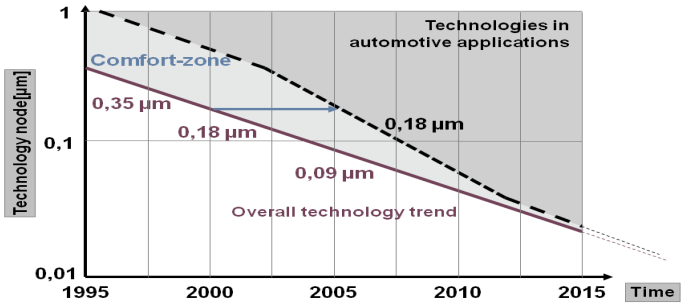
Bpifrance AAP FUI16 and the General Council of Essonne France

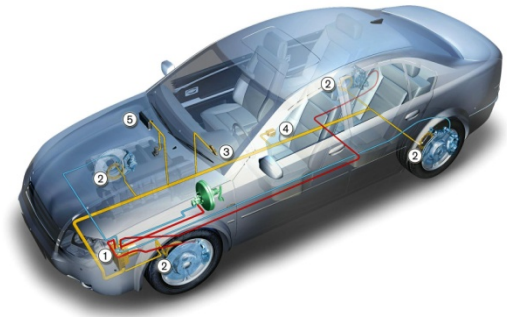
AGENDA

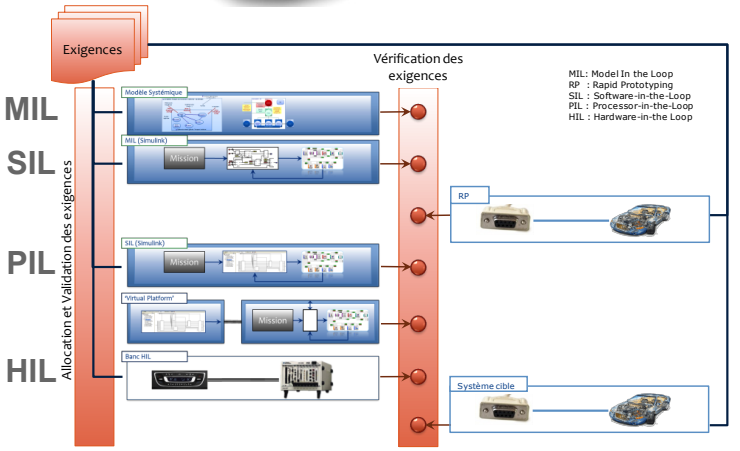
- Context and Trends
- Objectives and Results
- Methodology and tools
  - Technical challenges
  - Automatic test generation
  - Analysis and verification of compliance with the requirements
  - Virtual platforms and HW faults injection
- Current status – Tools chain V2
- Next works

CONTEXT AND TRENDS

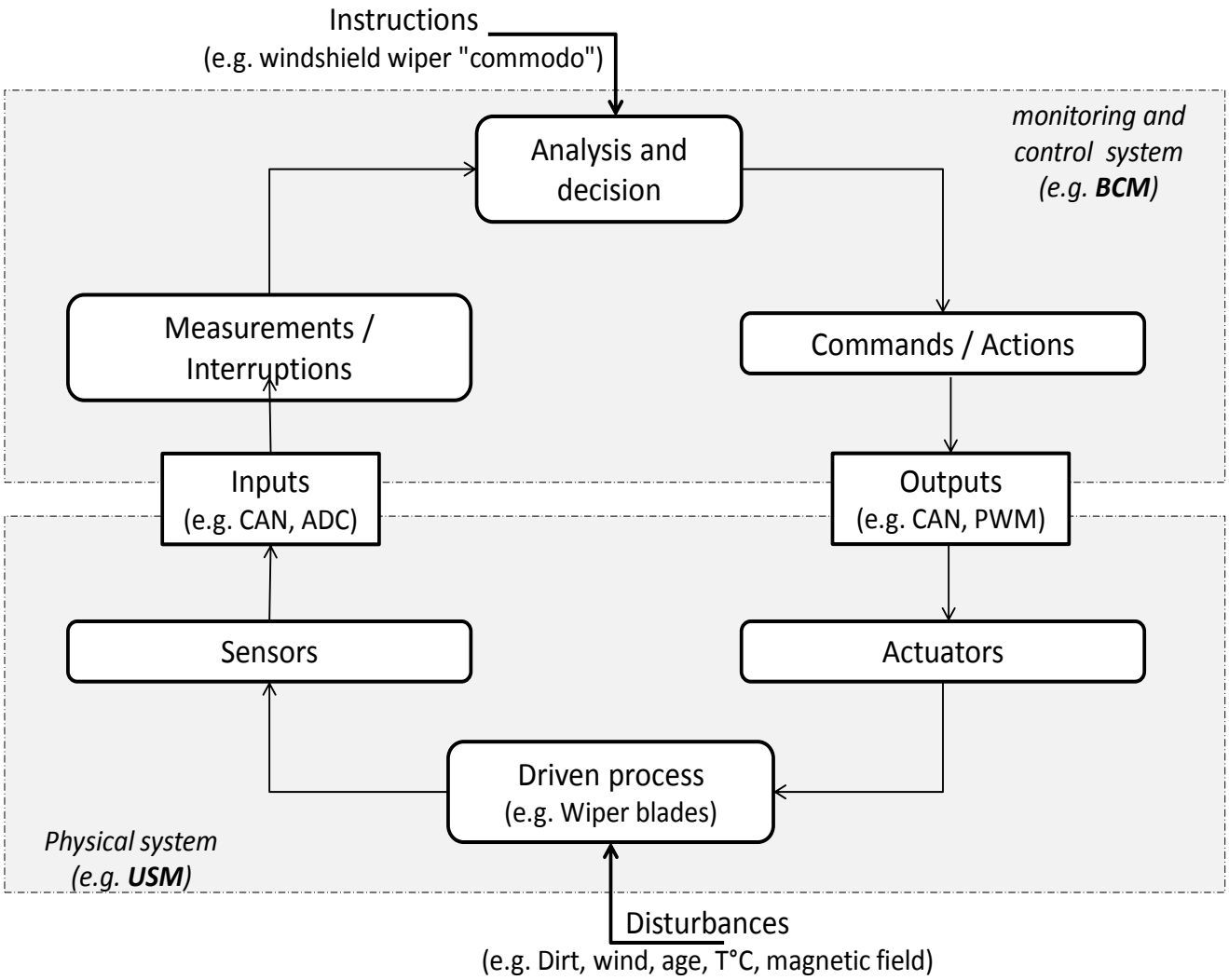
- **µElectronic Miniaturization**
  - Increased sensitivity of ECU to transient hardware faults
- **Increased number of functions**
  - 10-100 ECU (distributed system)
- **Hostile operating environment**
  - Electromagnetic fields, temperature, humidity
- **ISO26262 standard**
  - Safety constraints (product and process)
- **Embedded software V&V**
  - Complex iterative process
  - 40-50% total development cost





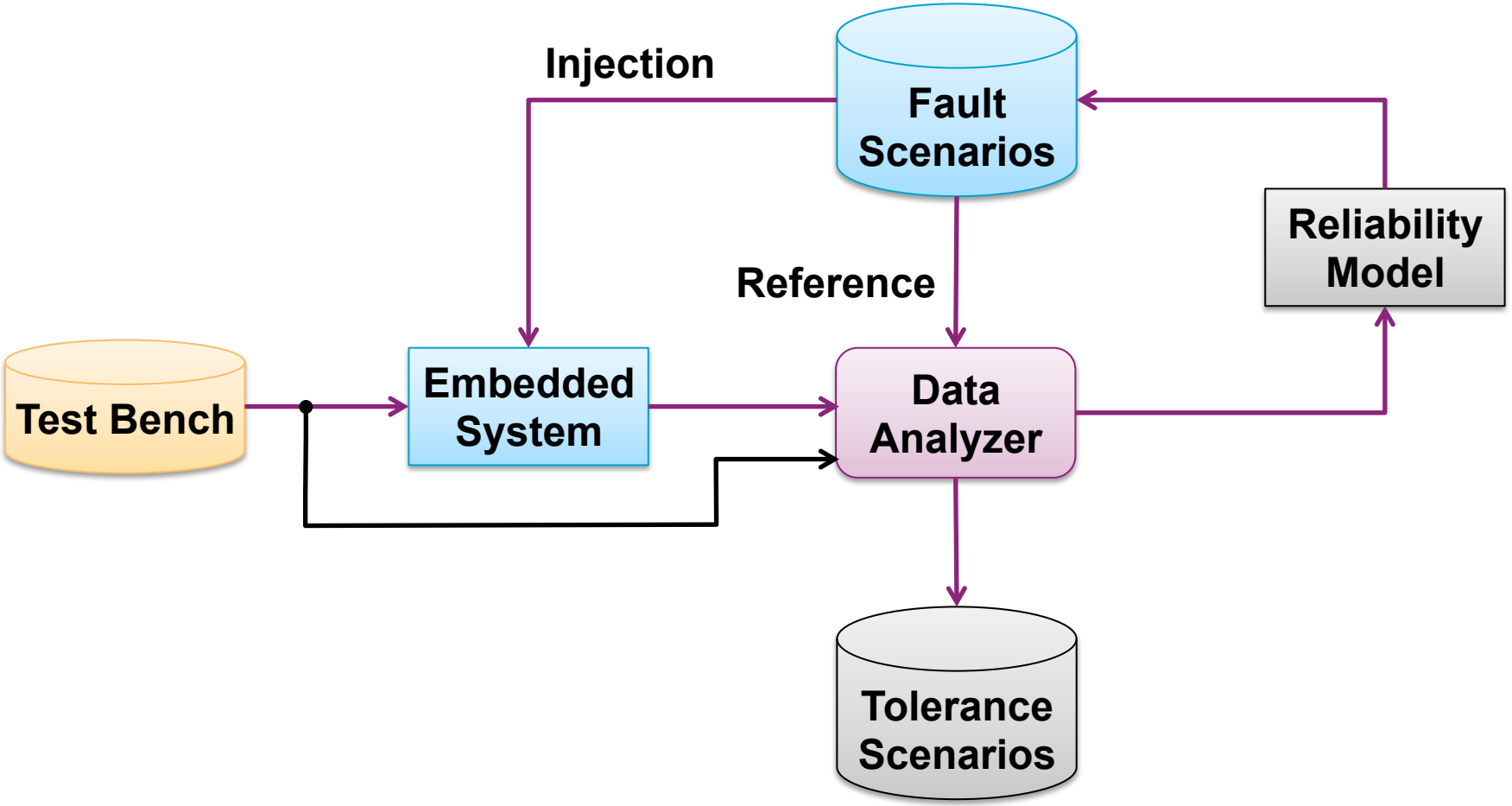


BLOC DIAGRAM OF CONTROL LOOP



EQVITAS

FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

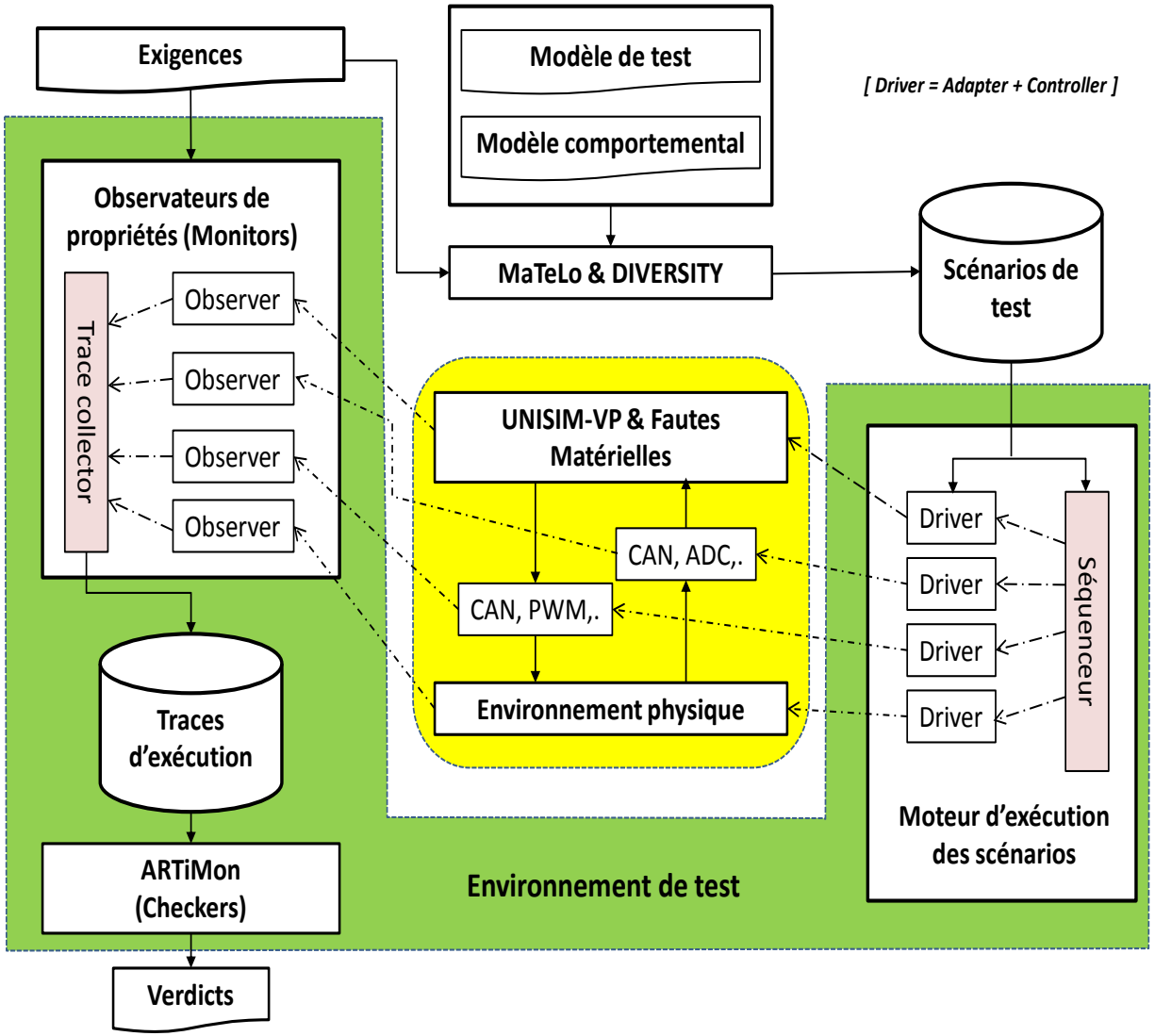


EQVITAS

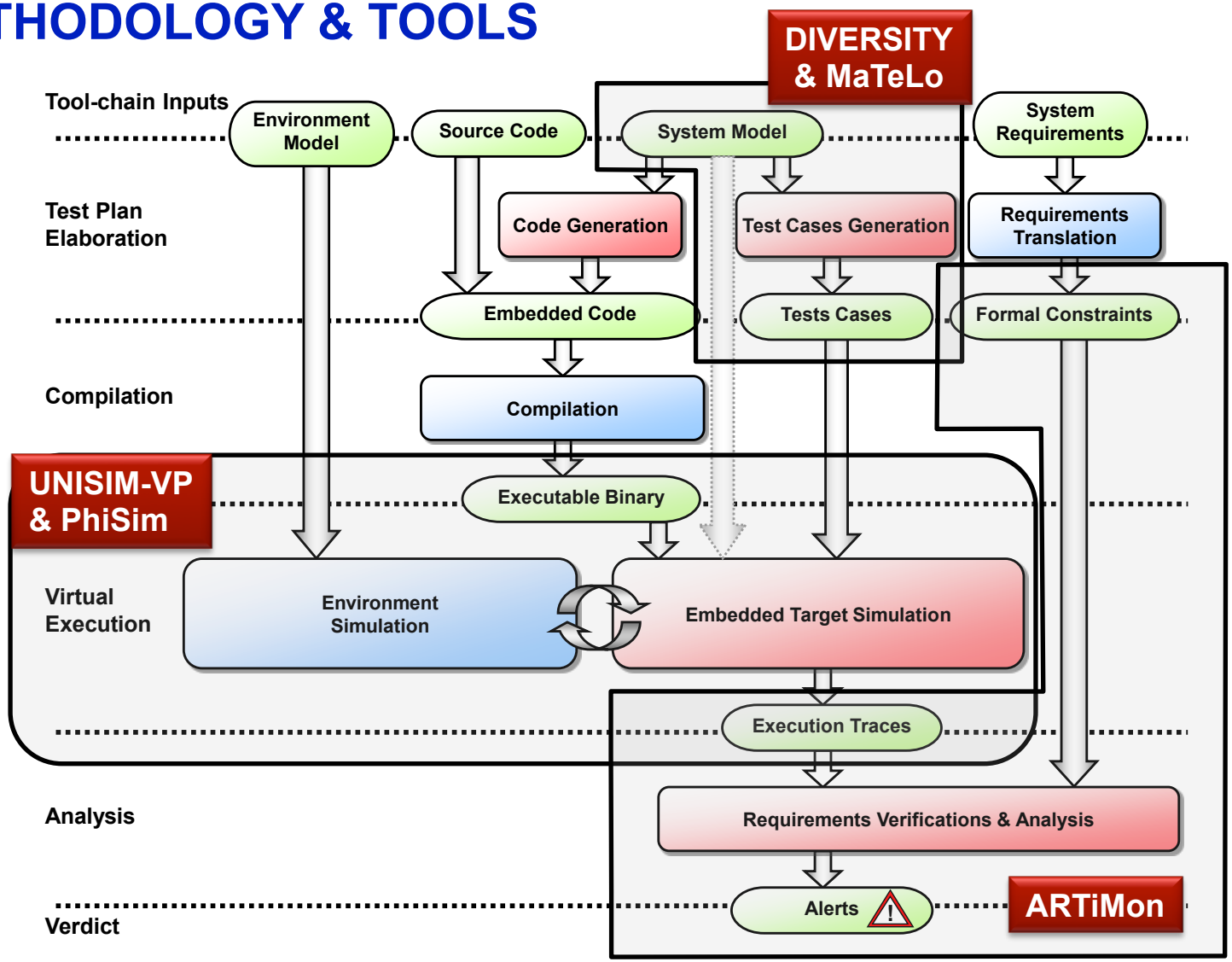
OBJECTIVES AND RESULTS

- **Automate the verification and validation process of whole embedded software stacks**
  - By developing a continuous tool-chain
  - In the context of automotive electronic systems
- **Improve the relevance of the test campaigns**
  - By detecting the redundant tests using equivalence classes
- **Provide assistance to the hardware failure effect analysis (FMEA)**
  - By introducing a hardware faults model during simulation.
- **Extract a comprehensive V&V methodology using virtual platforms**
  - By assessing the EQUITAS tool chain on real automotive use cases
- **Assess the tool-chain under the ISO 26262 requirements.**

VIRTUAL TESTING ENVIRONMENT



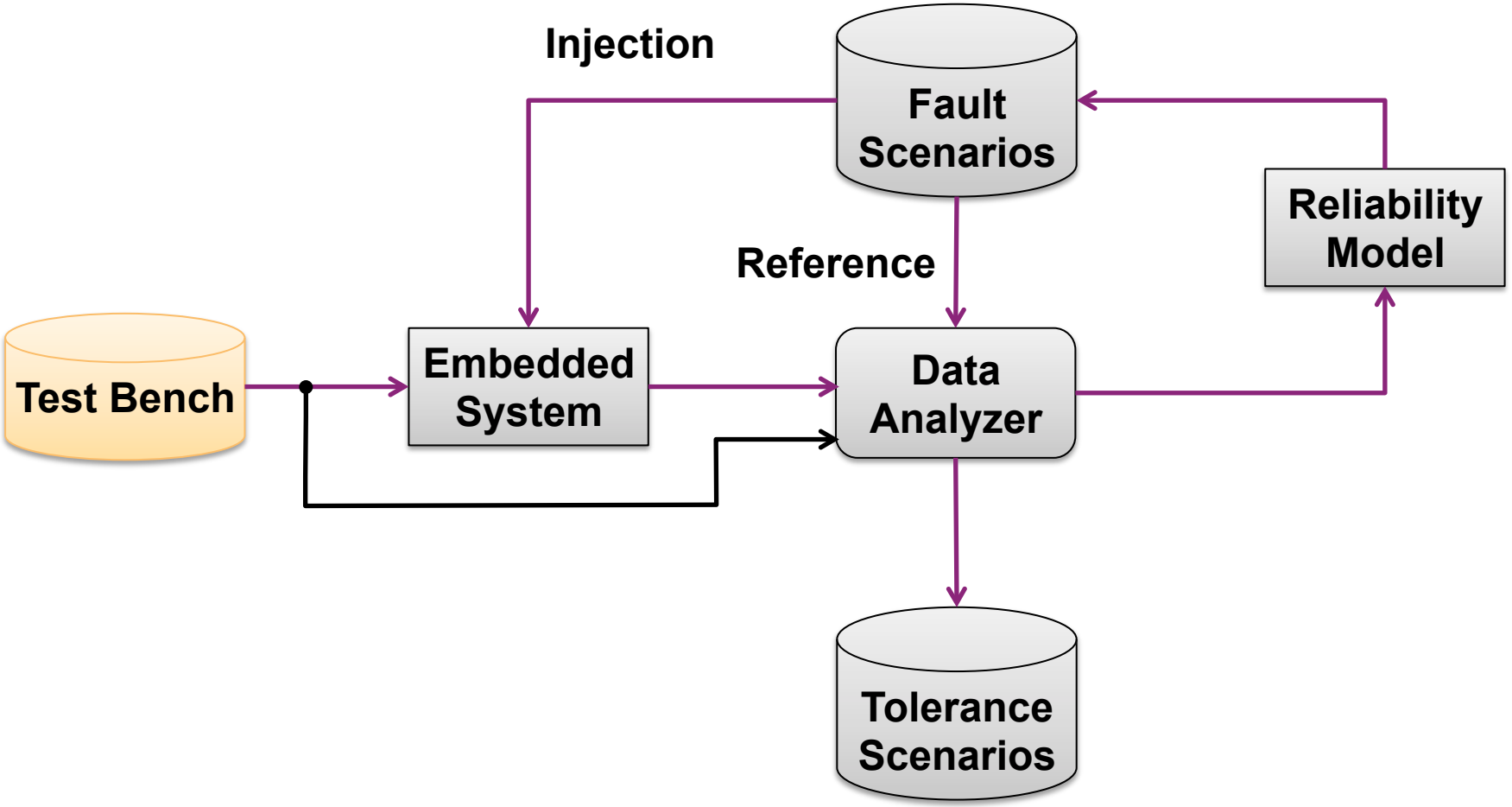
METHODOLOGY & TOOLS



TECHNICAL CHALLENGES

- **The use of symbolic execution principle to analyze and reduce test cases obtained by a stochastic approach**
  - MaTeLo: stochastic test generation technique
    - ⇒ Generate the most likely tests
    - ⇒ Many redundant/duplicate tests
    - ⇒ Developped by ALL4TEC (http://www.all4tec.net/MaTeLo/homematelo.html)
  - DIVERSITY: symbolic execution
    - ⇒ Model validation by analyzing its symbolic execution tree
    - ⇒ Property verification
    - ⇒ Automatic test generation based mainly on the paths coverage
    - ⇒ Developed by CEA LIST (http://projects.eclipse.org/proposals/diversity)
- **The extension of the simulation environment UNISIM-VP**
  - Modeling and injection of characterised hardware faults
  - Interface to test cases generation tools (MaTeLo & DIVERSITY)
  - Interface to compliance (monitoring) analysis tool (ARTiMon)

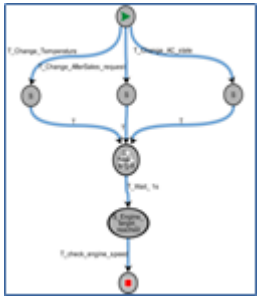
FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS



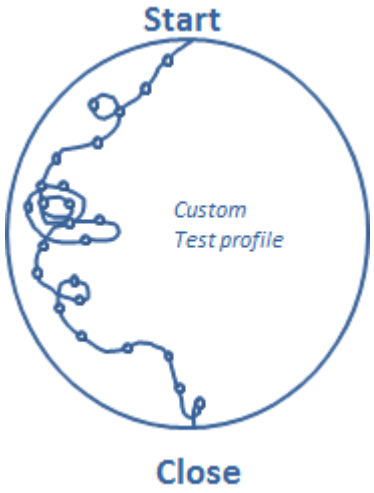
EQVITAS

MATELO OVERVIEW

1 Graphical Design

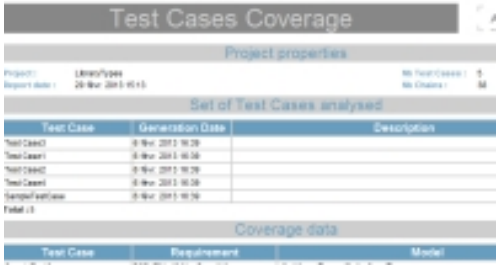


2 Test Case Generation



3 Test Script Generation

4 Coverage Report



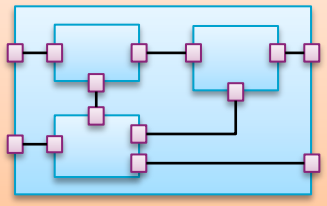
http://www.all4tec.net/MaTeLo/homematelo.html

EQVITAS

DIVERSITY - METHODOLOGY

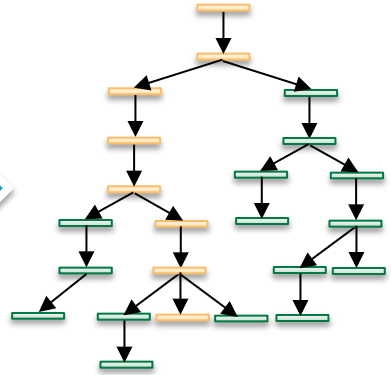
Modeling Environment

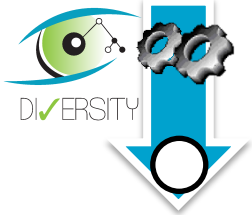
Specification



Specification Requirements

Behavior tree



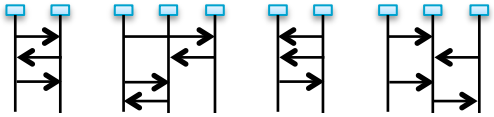


Functional model « Black box »

Specification model Simulation

Conformance testing

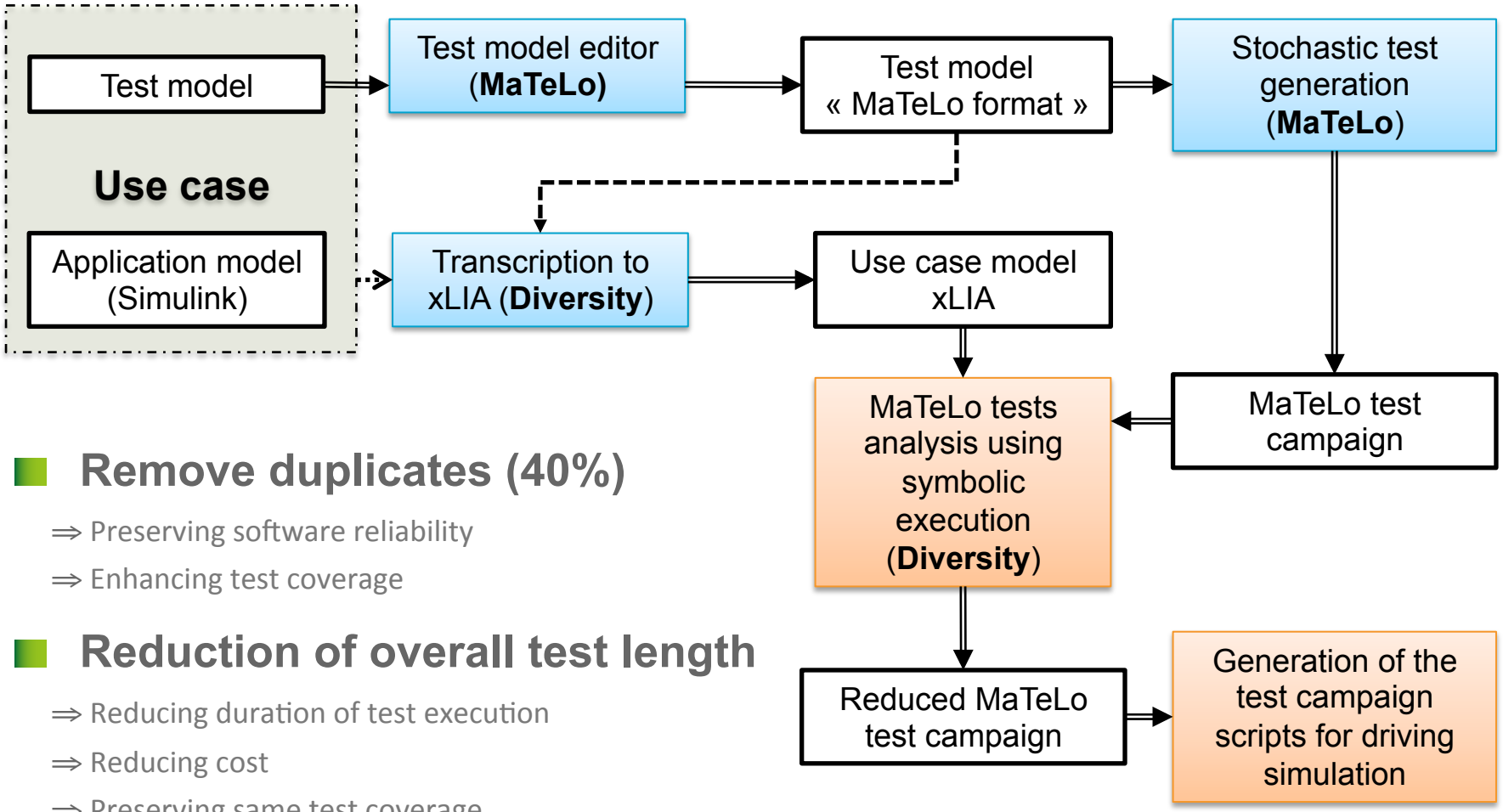
Specification correctness



Test cases « numeric scenarios »

EQVITAS

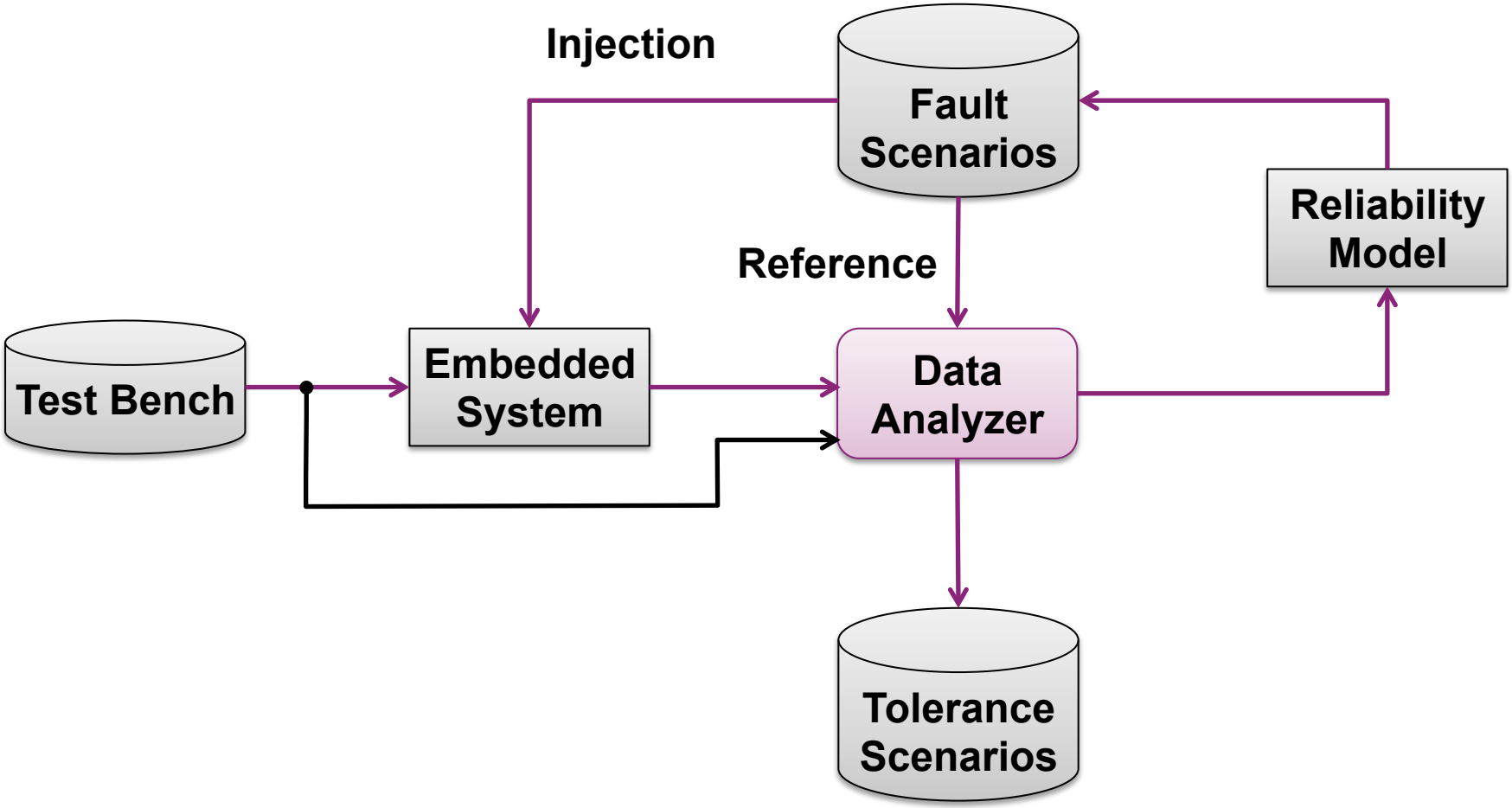
COUPLING DIVERSITY AND MATELO



- **Remove duplicates (40%)**
  - ⇒ Preserving software reliability
  - ⇒ Enhancing test coverage
- **Reduction of overall test length**
  - ⇒ Reducing duration of test execution
  - ⇒ Reducing cost
  - ⇒ Preserving same test coverage

EQVITAS

FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

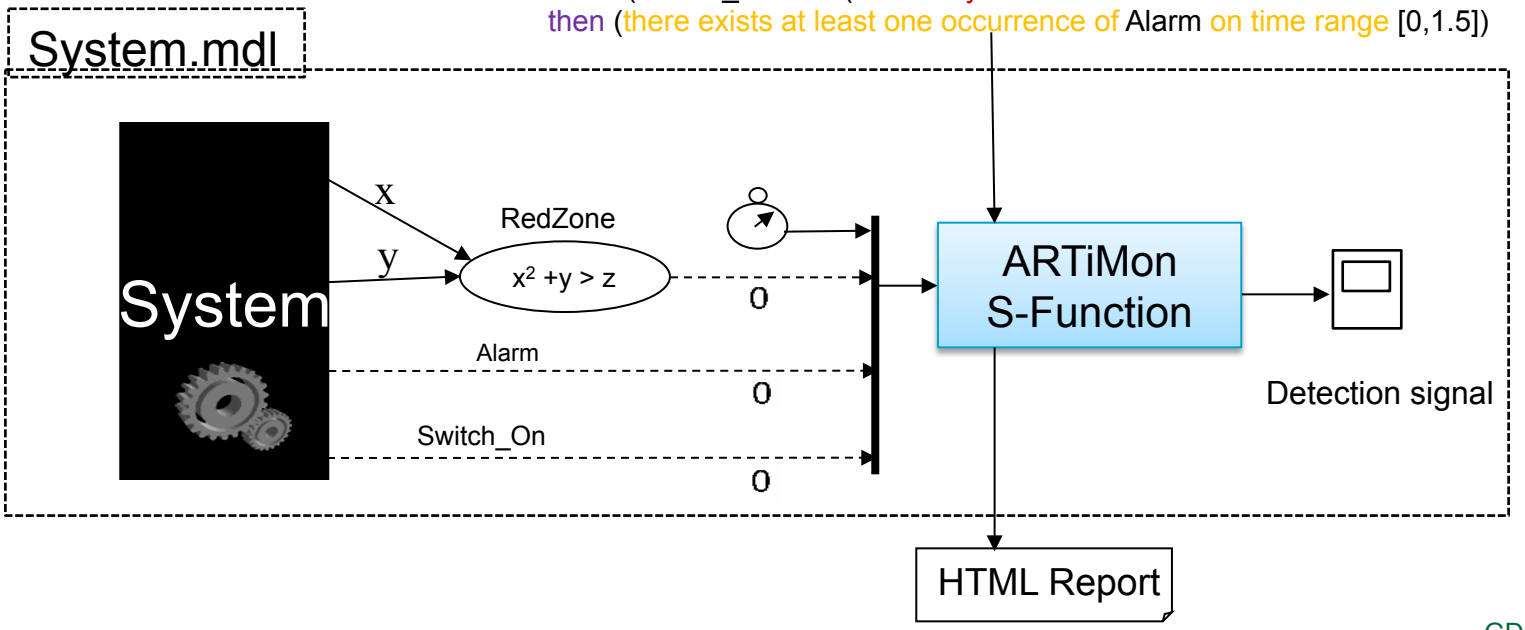


EQVITAS

ARTIMON: ADVANCED REAL TIME INFORMATION MONITORING

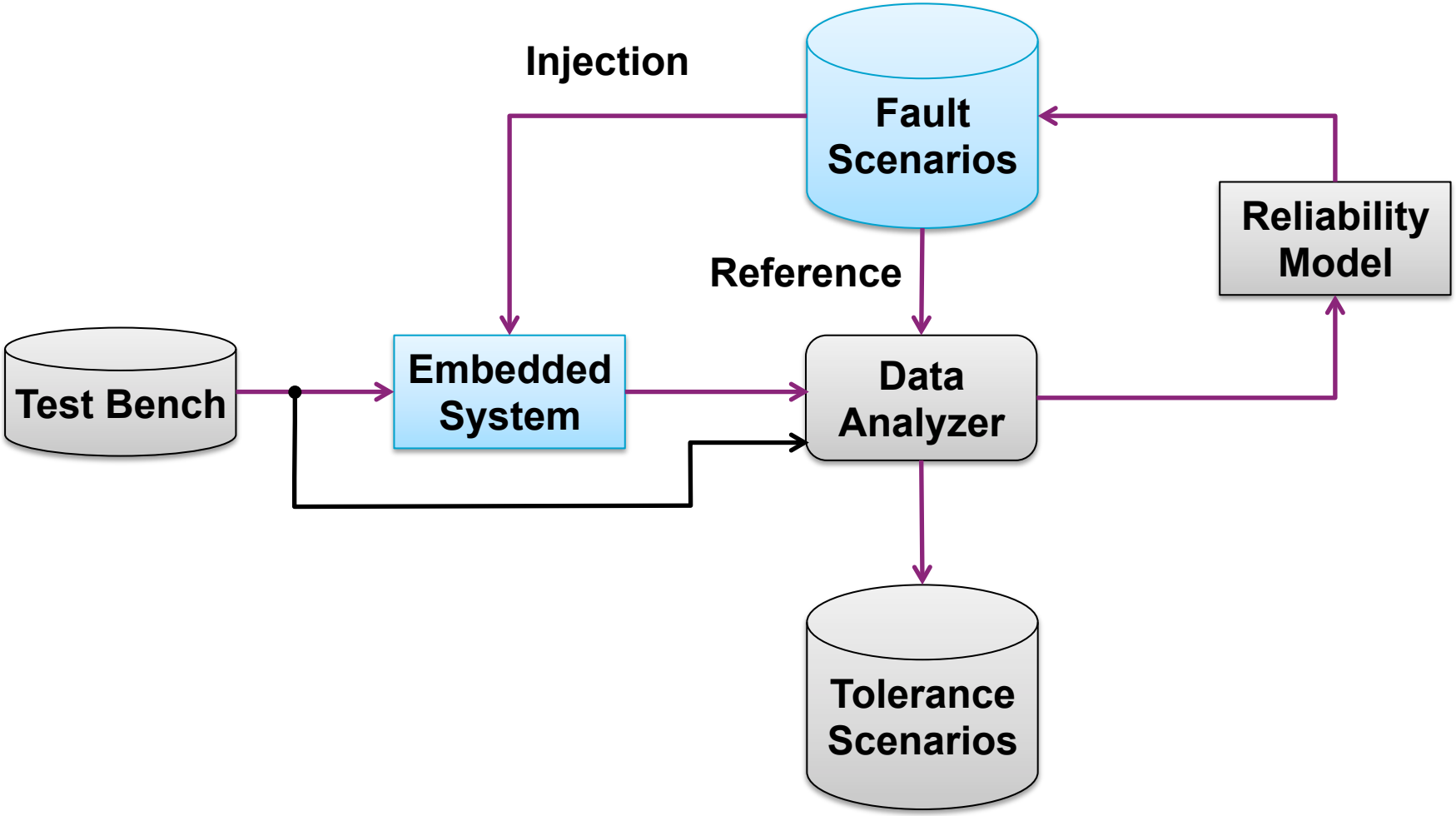
- **Provides a temporized logic based language**
  - To express requirements about system real-time behavior
- **Transforms a set of requirements into operational detectors**
  - For the simulation/execution environment

ARTiMon 4 Simulink:



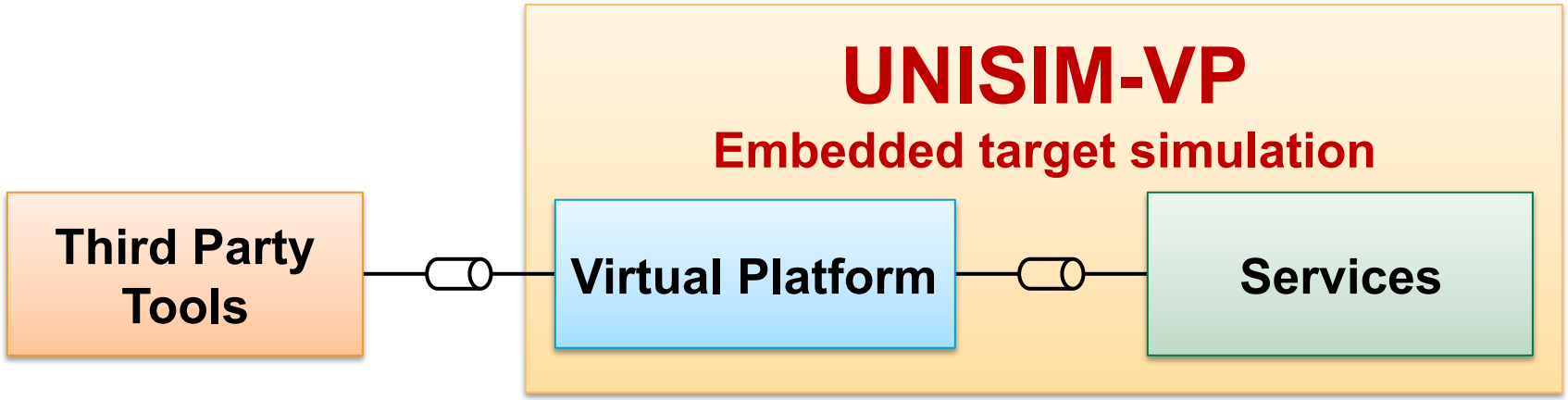
EQVITAS

FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS



EQVITAS

COMPONENT-BASED VIRTUALIZATION ENVIRONMENT



- Co-simulation
- Test-bench database
- Existing tool-chains

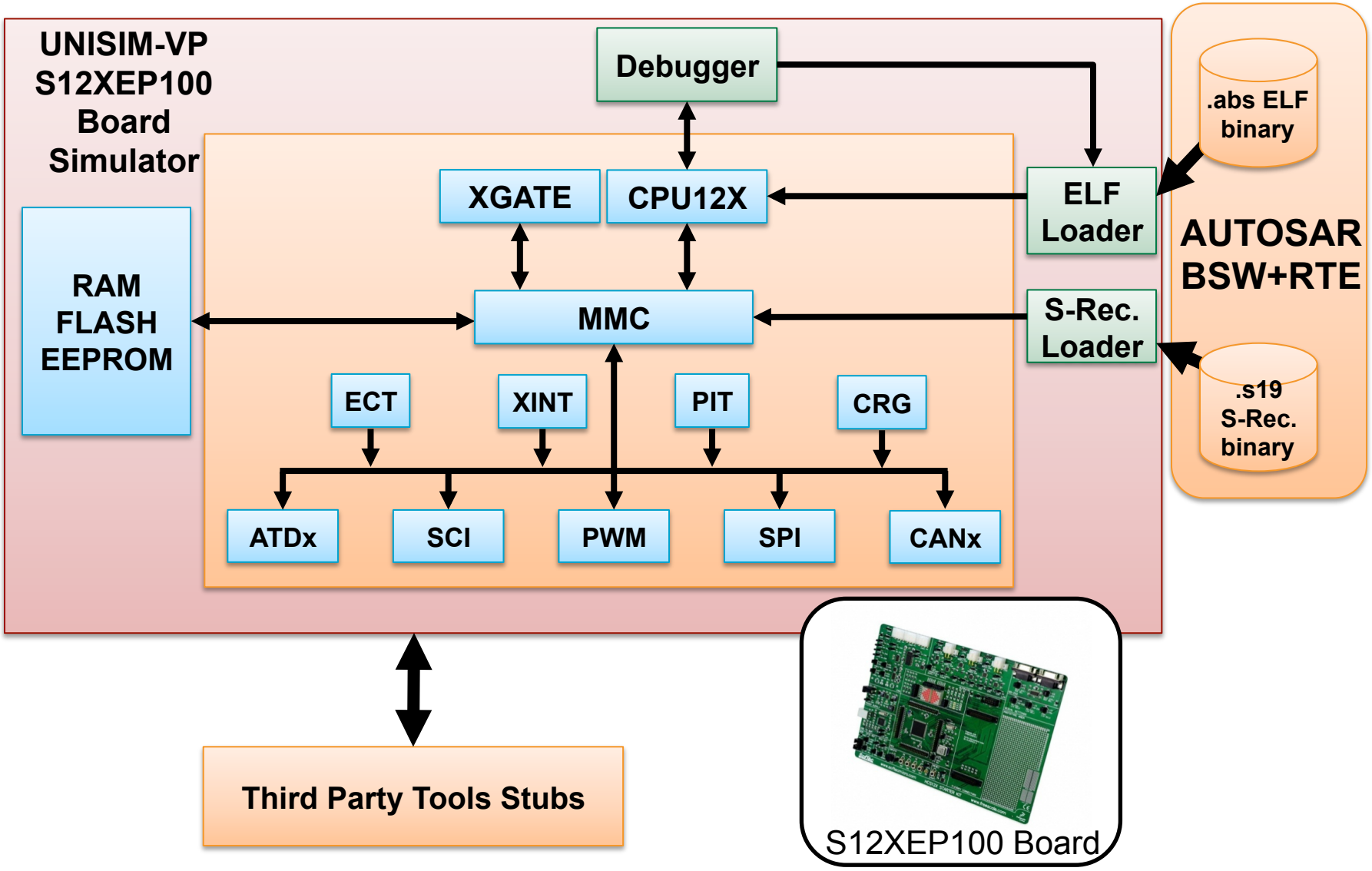
- System on Chip
- Boards
- SystemC/TLM

- Debugger
- Test
- Monitor
- Trace analysis
- Profiling
- HW fault injection

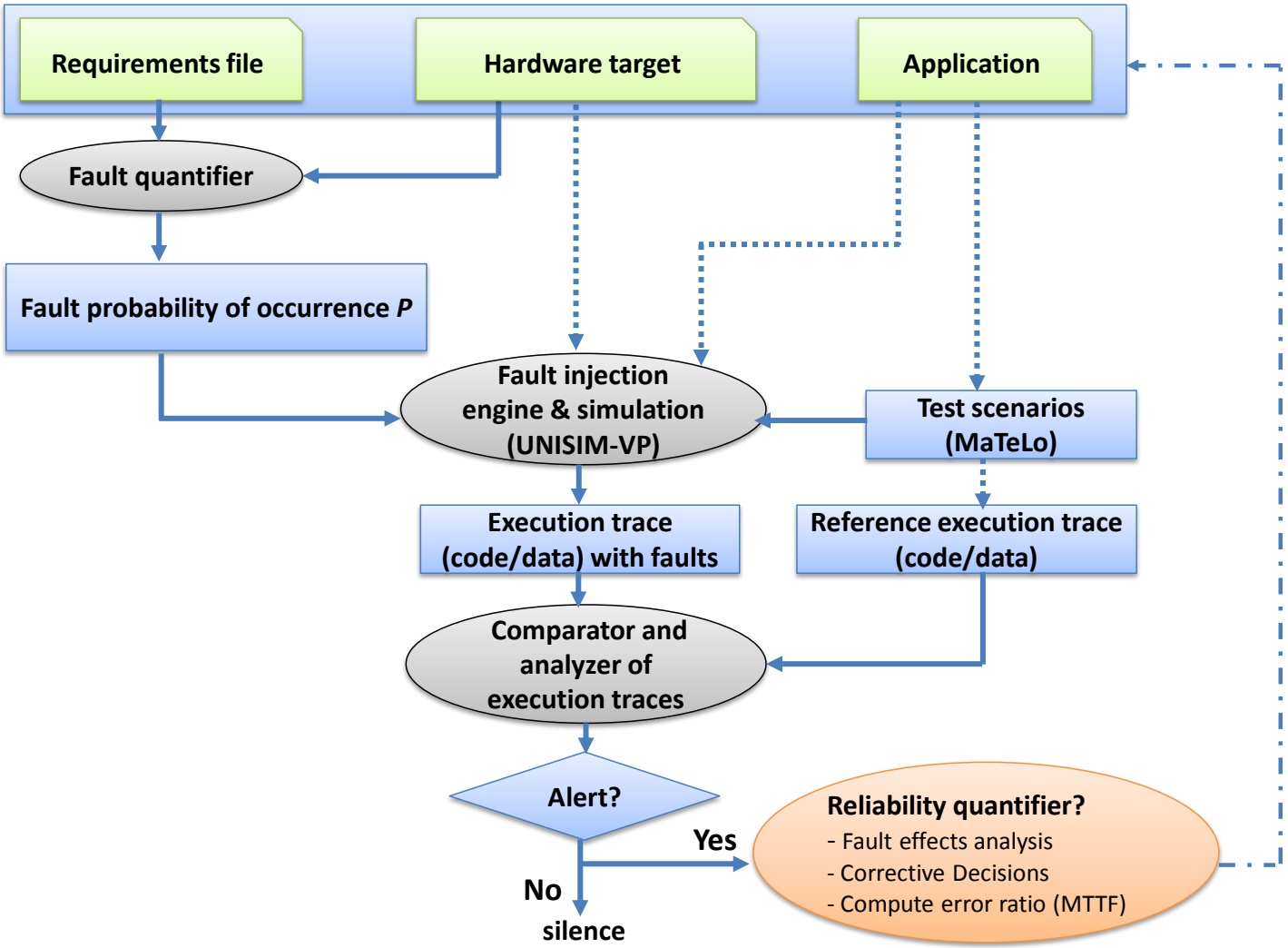
https://unisim-vp.org/site/index.html

EQVITAS

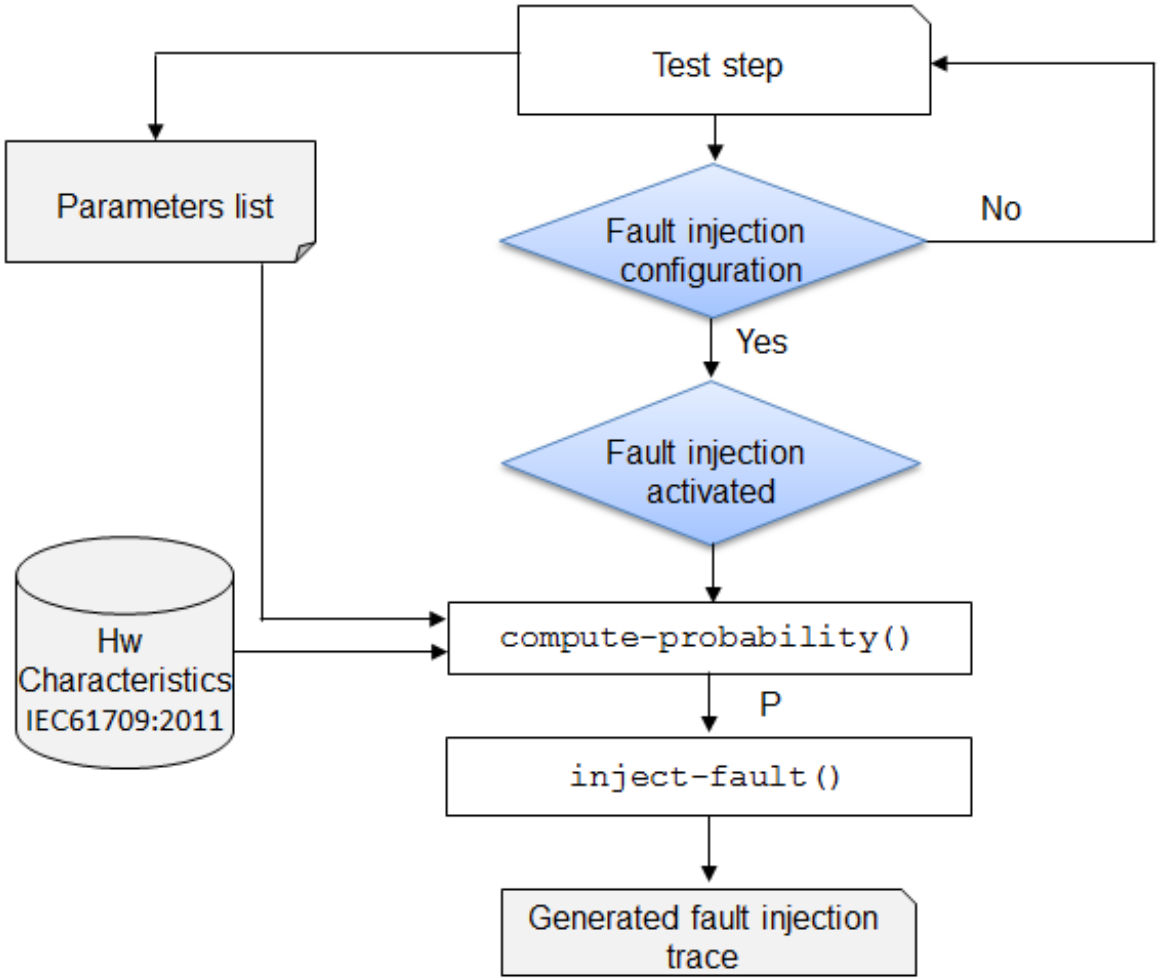
STAR12X – AUTOMOTIVE APPLICATION



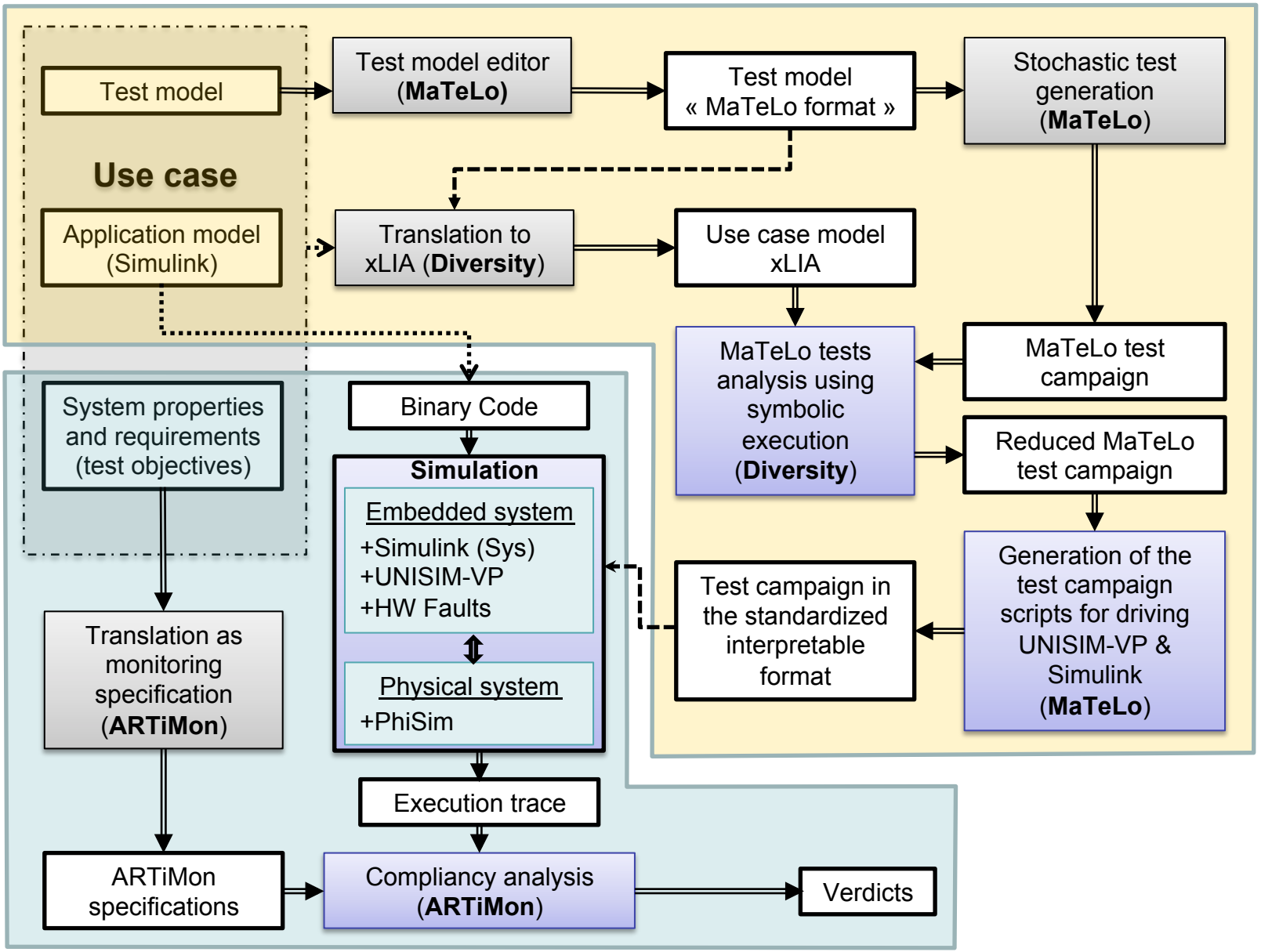
TEST CASE ENHANCED WITH HARDWARE FAULT INJECTION



FAULT INJECTION STRATEGY

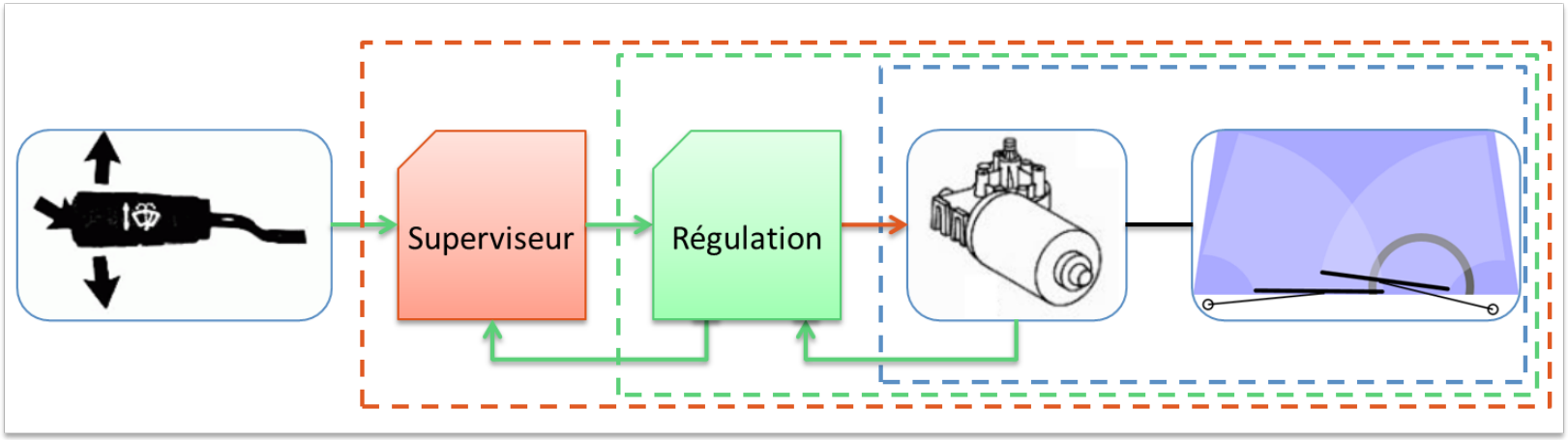


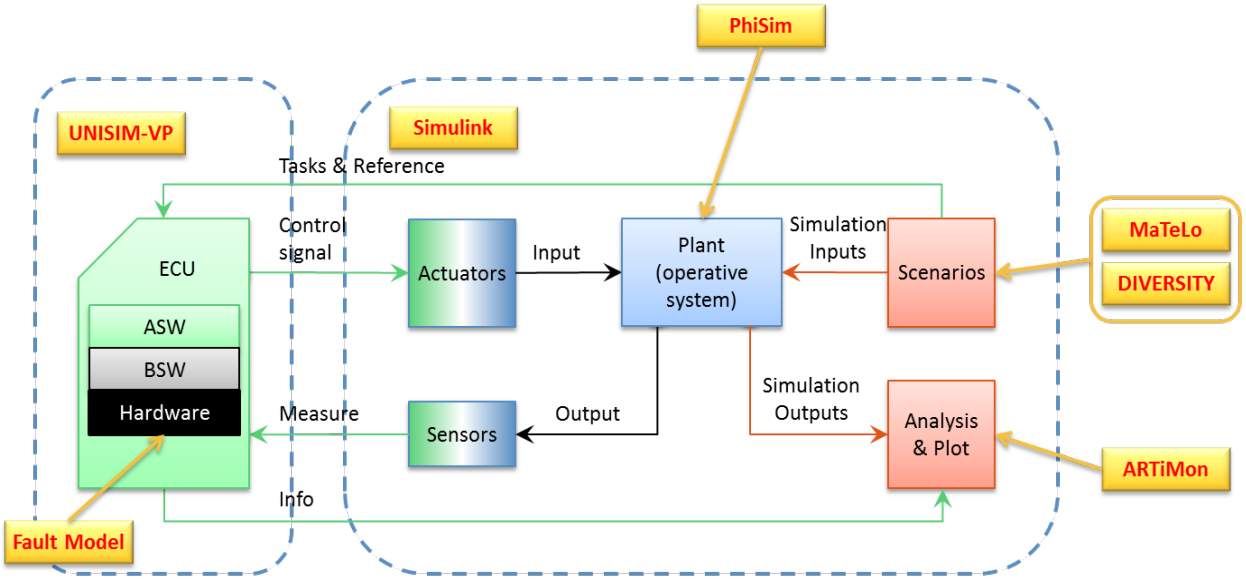
TOOLS CHAIN


Test model
Test model editor (MaTeLo)
Test model « MaTeLo format »
Stochastic test generation (MaTeLo)
Use case
Application model (Simulink)
Translation to xLIA (Diversity)
Use case model xLIA
MaTeLo tests analysis using symbolic execution (Diversity)
MaTeLo test campaign
System properties and requirements (test objectives)
Binary Code
Simulation
Embedded system
+Simulink (Sys)
+UNISIM-VP
+HW Faults
Physical system
+PhiSim
Reduced MaTeLo test campaign
Generation of the test campaign scripts for driving UNISIM-VP & Simulink (MaTeLo)
Test campaign in the standardized interpretable format
Translation as monitoring specification (ARTiMon)
Execution trace
ARTiMon specifications
Compliancy analysis (ARTiMon)
Verdicts

EQVITAS

WINDSHIELD WIPER





NEXT WORKS

- **Studying the compliancy of the EQUITAS toolchain with the ISO26262 standard.**
- **Quantitative and qualitative assessment of the toolchain, by the project industrial partners.**
- **Generalization of project activities**
  - Distributed embedded systems
  - Heterogeneous (model, ASW, binary) validation and verification
- **Extension of EQUITAS toolchain**
  - RAMS analysis (Reliability, Availability, Maintainability, Safety)

A TOOL-CHAIN FOR FUNCTIONAL SAFETY AND RELIABILITY IMPROVEMENT IN AUTMOTIVE SYSTEMS

R. Nouacer, M. Djemal, S. Niar, G. Mouchard, N. Rapin, J.P. Gallois, P. Fiani, F. Chastrette, T. Adriano and B. Mac-Eachen

reda.nouacer@cea.fr

https://equitas-project.com/site/

Bpifrance AAP FUI16 and the General Council of Essonne France