ENABLE-S3
European Initiative to Enable Validation for Highly Automated Safe and Secure Systems

http://www.enable-s3.eu/

Sergio Sáez, Instituto Tecnológico de Informática, Spain

Workshop on Challenges and new Approaches for Dependable and Cyber-Physical Systems Engineering
Warsaw, Poland, 14th June 2019

ITI
INSTITUTO TECNOLÓGICO DE INFORMÁTICA

This project has received funding from the ECSEL Joint Undertaking under grant agreement No 692455. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway.

Project motivation

How can we make sure that an autonomous system behaves correctly in every situation?

Project consortium

68 Partners / 16 Countries

70 M€ budget

6 Domains (Automotive, Farming, Rail, Maritime, Aerospace, Health)

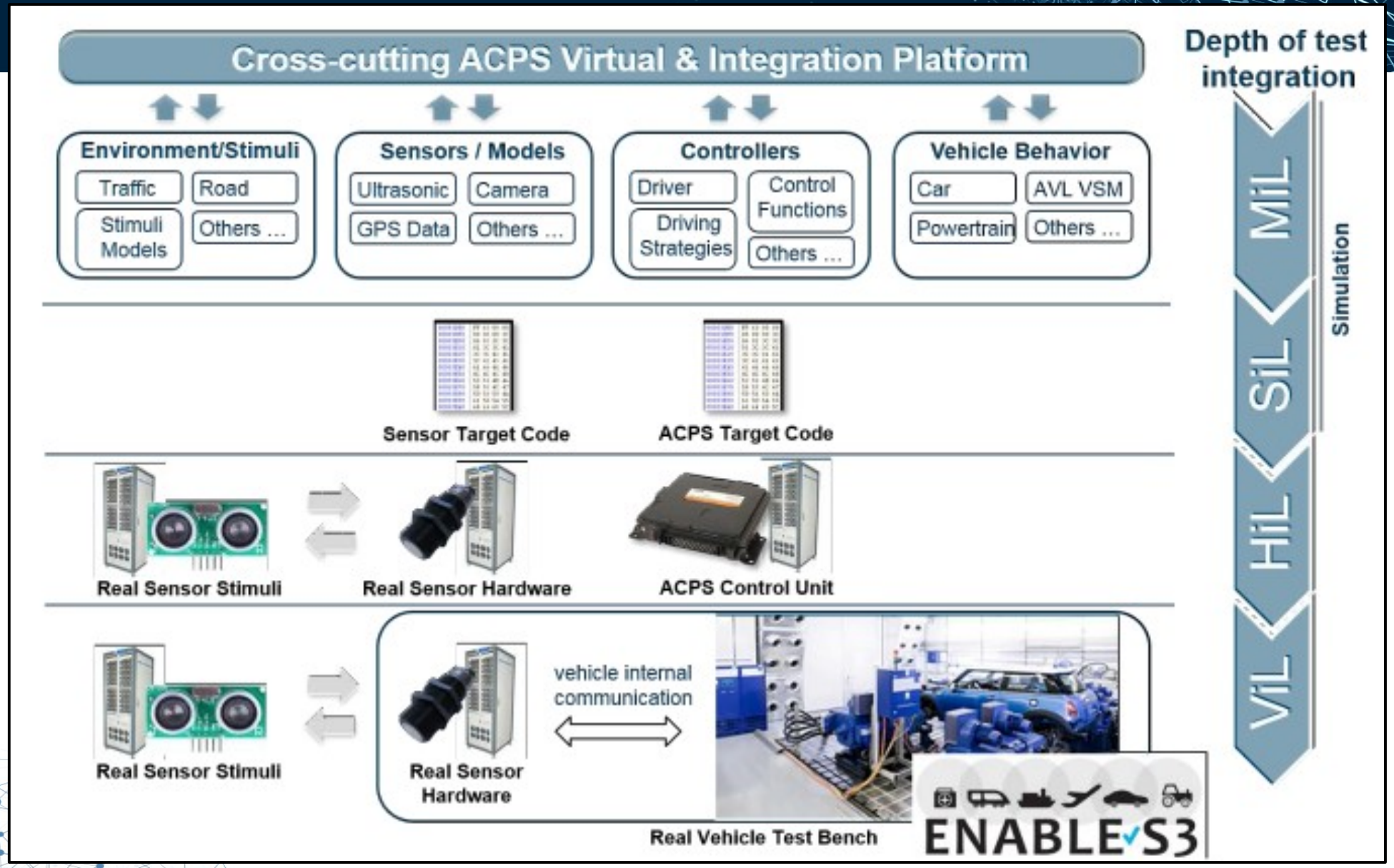
Full Value Chain for automated systems

- 7 OEMs as producer of end-customer products
- 12 Component supplier / tiers
- 5 Academia (highly automated systems)
- **20 Tool suppliers**
- **23 Academia (V&V Methodology)**

Project Goals

- Scenario-based V&V in virtual, semi-virtual and real testing environments
- The collection and/or development of environment and sensor models as well as adequate sensor stimuli for seamless Model / Software / Hardware / Powertrain / Vehicle-in-the-loop testing (MiL, SiL, HiL, PiL, ViL)
- The extraction of test scenarios from recorded operation data by using big data technology
- Risk- and coverage-oriented methods to reduce the number of required tests in highly varying environmental conditions
- Integrated safety and security analysis as well as runtime verification approaches
- Simulation-based approaches for homologation, certification and type approval of ACPS components and systems

Project Goals



ENABLE-S3

Use Case Work Packages

DOMAINS & USE CASES

RAIL

UC 9
Automated RailwayCommand and Control Systems

AUTOMOTIVE

UC 1
Highway Pilot

UC 2
Intersection Crossing using Autonomous Vehicles

UC 3
Context-Aware In-Car Reasoning System

UC 4
Traffic Jam Pilot with V2X

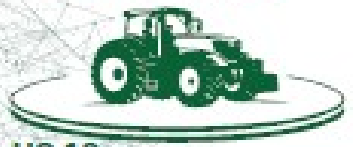
UC 6
Valet Parking

AEROSPACE

UC 7
Touch and Go Assistant

UC 8
Reconfigurable Video Processor for Space

FARMING



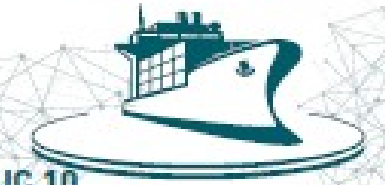
UC 13
Autonomous Control Platform

HEALTH

UC 11
Autonomous Robotic Movements

UC 12
X-ray Imaging Automation

MARITIME

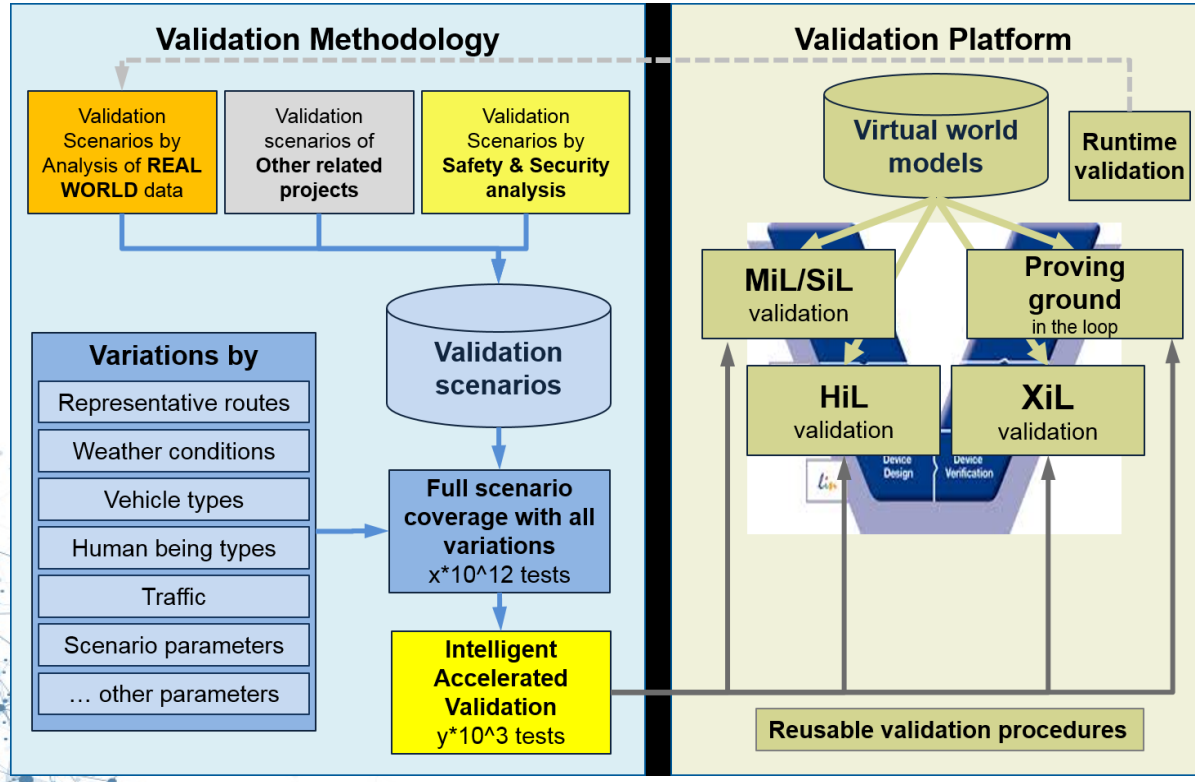


UC 10
Shore Based Bridge/Navigation Centre including Secure Data Exchange

ENABLE-S3 is following an use-case driven approach. This means that the requirements for the project are coming from industrial use cases within the 6 industrial domains and that each technical solution is required by a specific use case.

ENABLE-S3

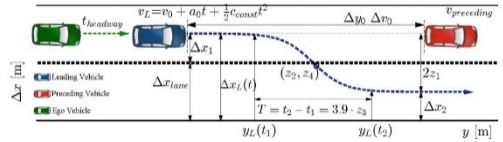
Overview Essential Results



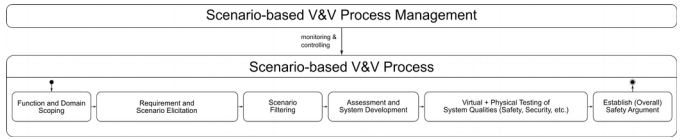
Cross-domain R&D

Best practice sharing

Scenarios and Scenario Classes



Scenario-based V&V methodology

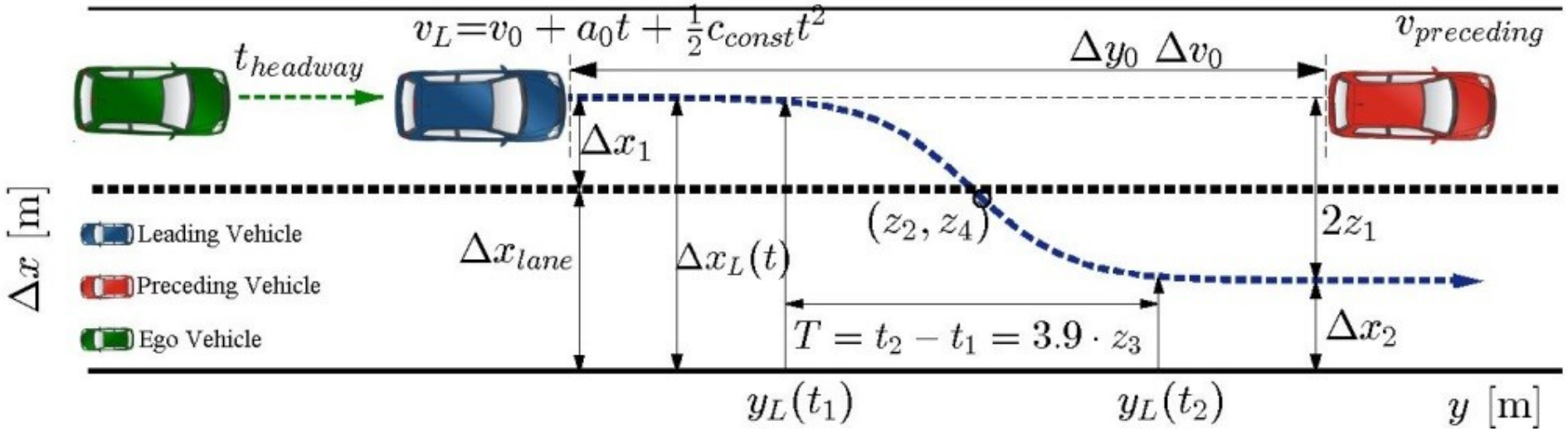


Generic reference architecture

Reusable technology bricks

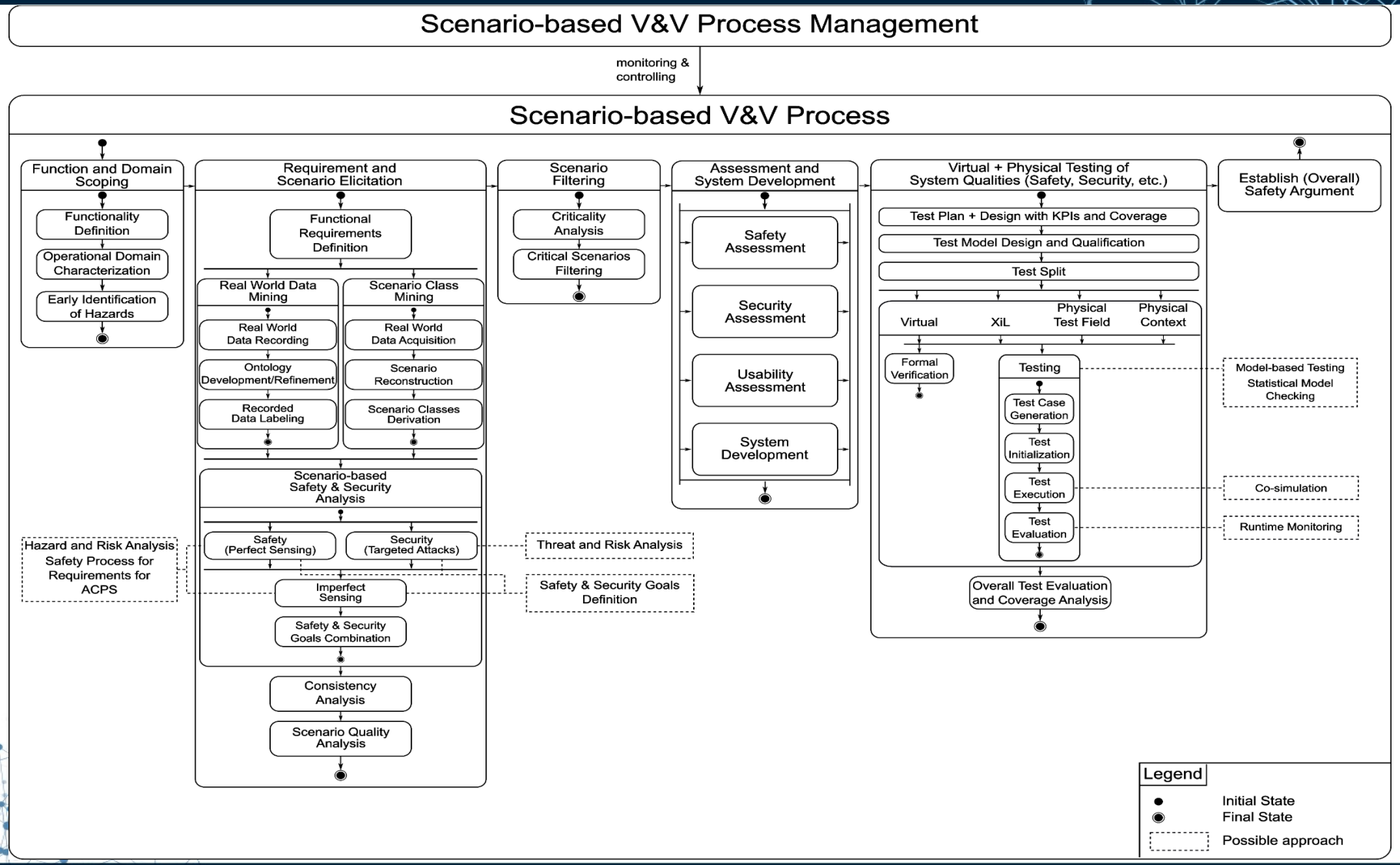
ENABLE-S3

Scenarios and Scenario Classes

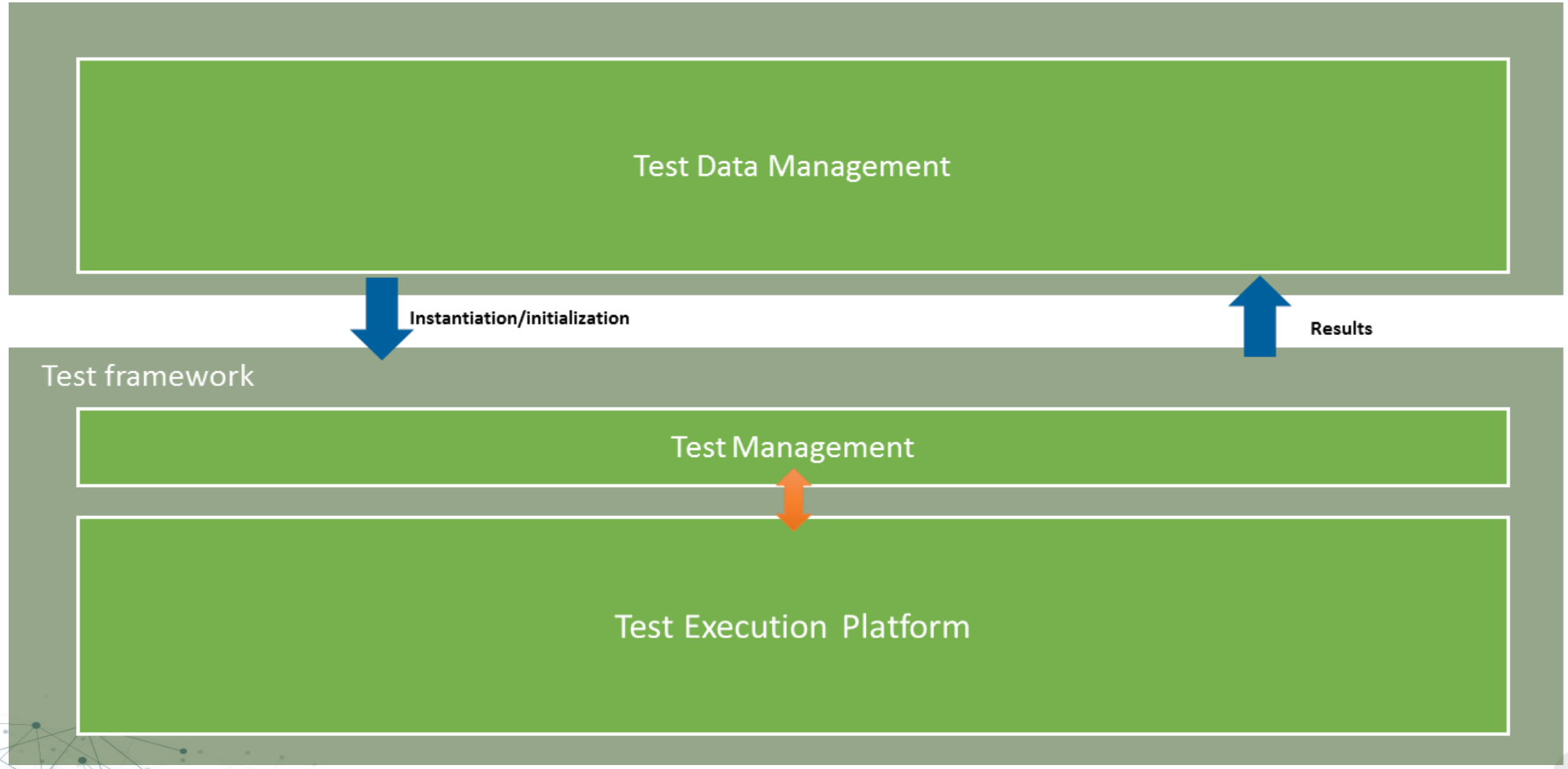


Scenario: all parameters instantiated – e.g specific velocities and distances
Scenario class: parameter ranges – e.g. velocity and distance ranges

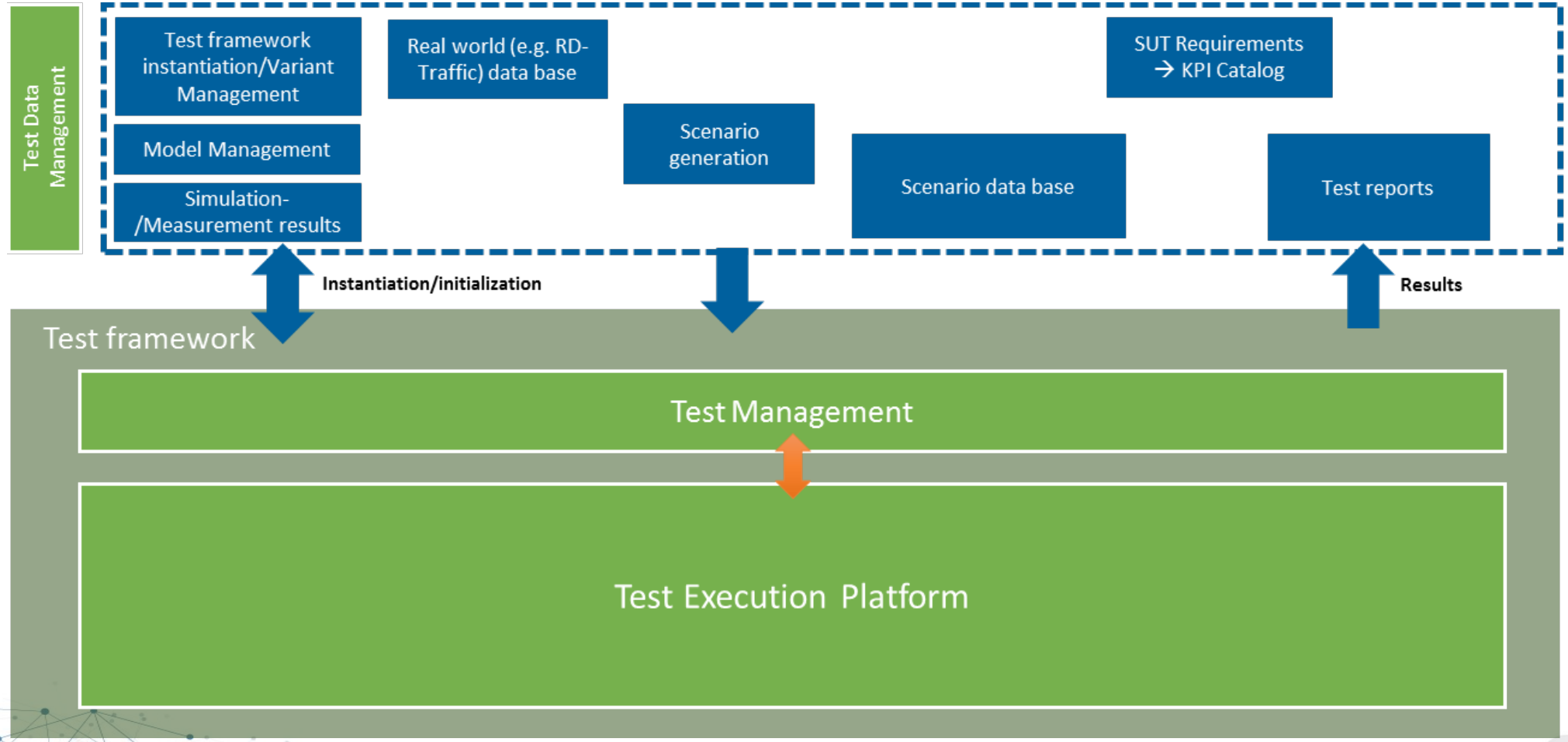
Scenario-based V&V Methodology



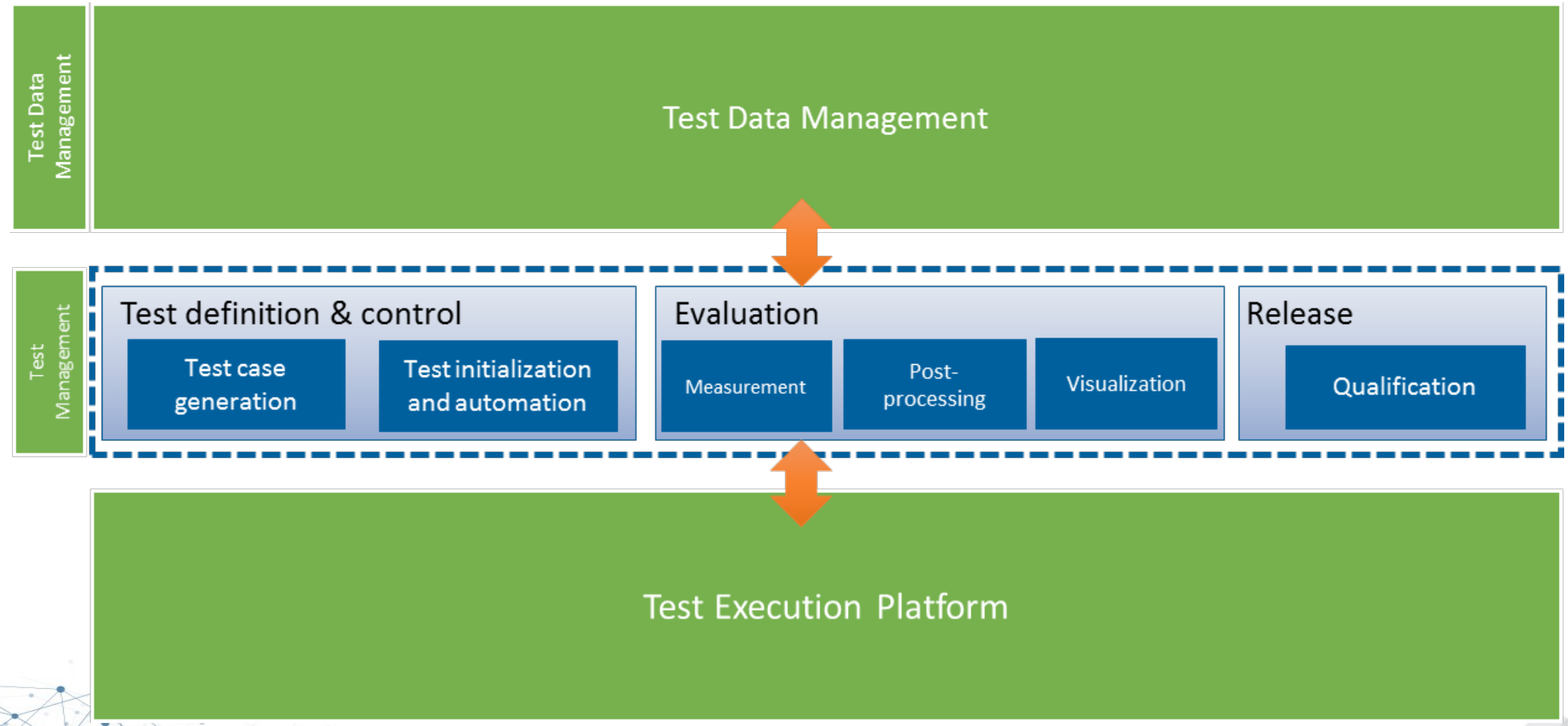
Generic Test Architecture



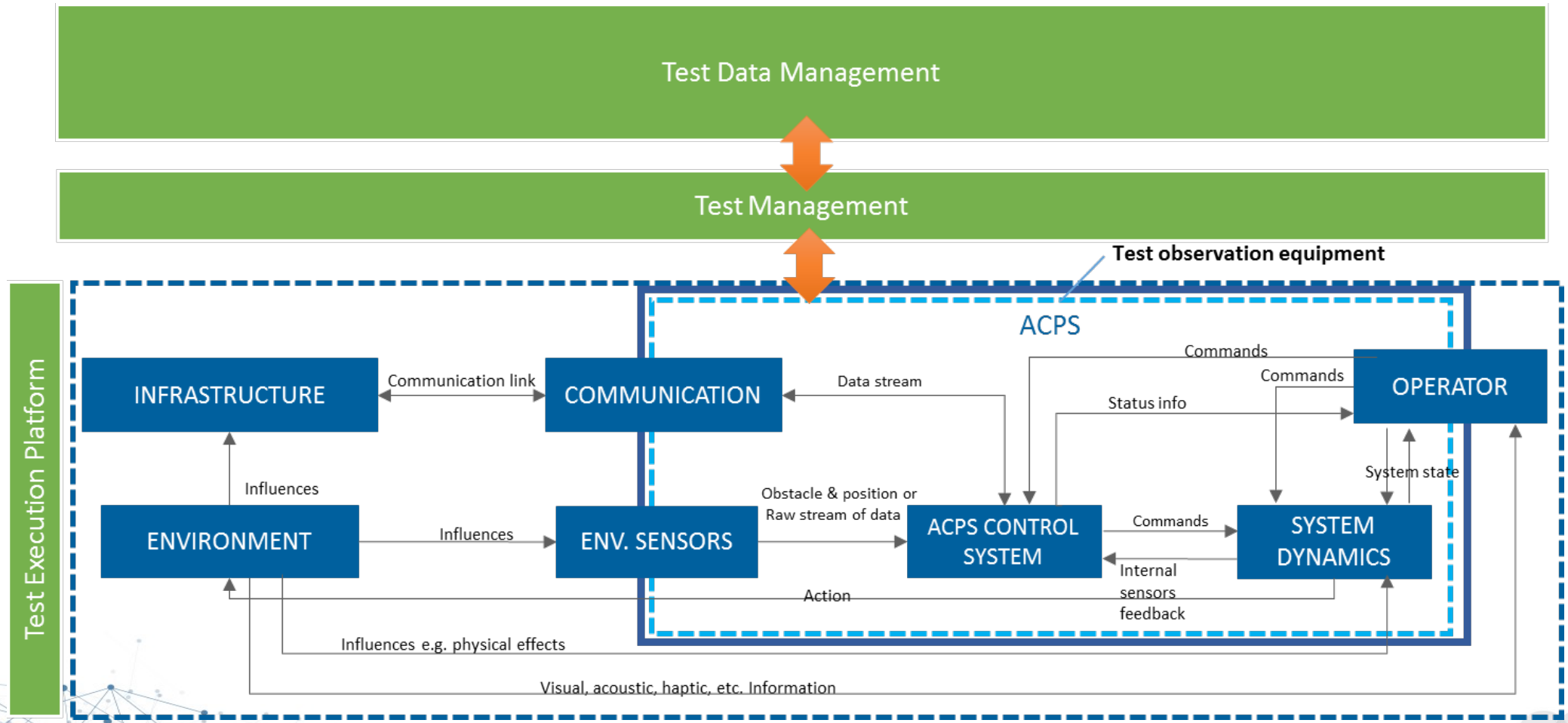
Generic Test Architecture



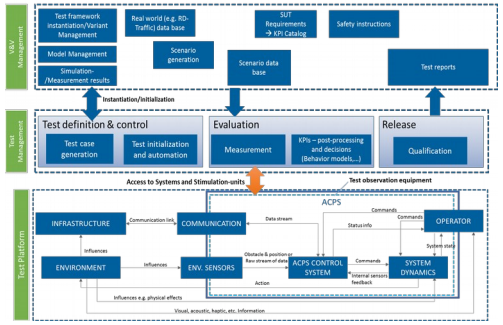
Generic Test Architecture



Generic Test Architecture

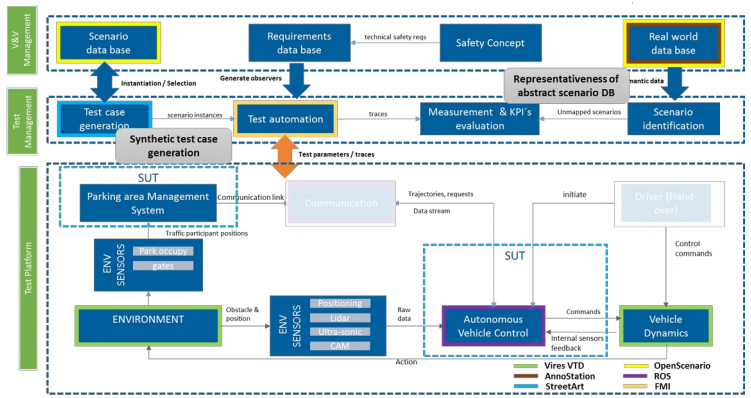


Technology bricks & GA



Reference test architecture for scenario based virtual/real validation of highly automated systems

Set of reusable technology bricks



Use Case specific Validation tool chains

ENABLE-S3

Technology bricks: Tools

Main areas

- Automated test design
- Simulation based testing
- Automated validation and verification

Adaptations for use cases

- Domain specific enhancements
- Cross-domain tools

Support re-usability

- Common interfaces
- Integration into V&V environments

Technology bricks: Tools

- Finalization of tools, tool integration to use cases, and evaluations in use cases
  - 57 tools
  - 17 tools used in two use cases
  - 4 tools used in three use cases
  - 9 tools used in several domains
- Four categories of tools
  - Open source
  - Commercial
  - Proprietary
  - Research
- Related objectives:
  - Obj_01 Reduce at least 50% of test execution effort compared to conventional testing.
  - Obj_04 Reduction of re-qualification efforts by at least 30% compared to effort prior to the project.

Technology results

- Know-How and Technology developed
  - generic test architecture
  - generic methodology for scenario-based V&V of ACPS
  - 50+ tools and tool-extensions
  - new scenario data-sets including analysis
  - virtual sensor models
  - methods for sensor stimulation
  - improved co-simulation techniques (real-time, distributed)
- Contributions to standards
  - OpenSCENARIO, OpenDRIVE, OpenCRG
  - SoTIF
  - FMI, DCP
  - OSI
- Commercial exploitation

ENABLE-S3

DOMAIN
AEROSPACE

ENABLE-S3

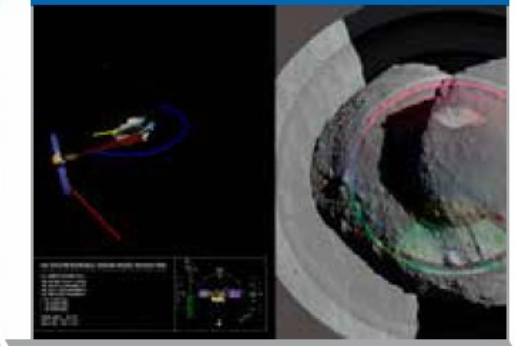
- UC8 – Reconfigurable Video Processor

New Space Challenges

Step 1: Today vs. traditional approaches

New solutions are being explored for the space environment, such as Reconfigurable FPGAs used in industrial applications.

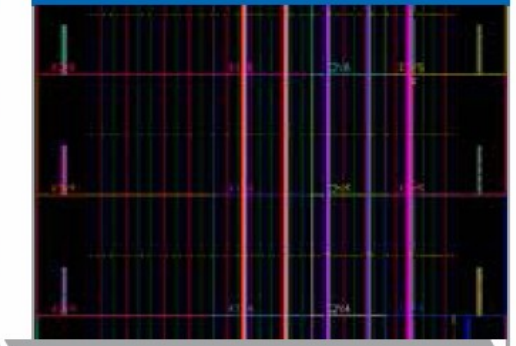
SuT & Scenarios



Step 2: Test of SuT architectures

Earth Observation and Vision-based Navigation are two traditional applications, implemented in the UC8 running common platform. Earth Observation, incl the compression of a hyperspectral image, is 1st shown in a fault free, then in a faulty environment.

FPGA in the Loop



Step 3: Fault injection tool

Rad-Hard are used traditionally to avoid radiation faults due to space environment. Reconfigurable FPGAS are not Rad-Hard, so the self-healing mechanism provided by Artico3 is used to cope with radiation simulated by a fault Injection tool.

Scheduling Simulation

Step 4: SuT model-based simulation

The satellite platform and the applications were modelled with the tool suite. Model-based simulation allows the engineer to identify unfeasible scenarios that do not comply with timing constraints due to the fault recovery processes.

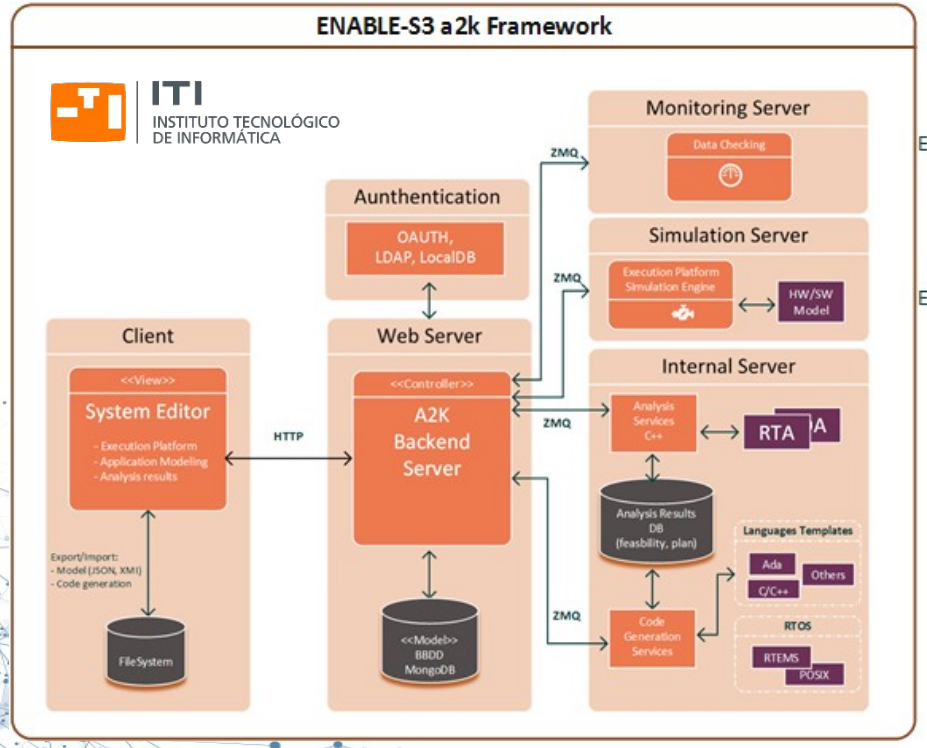
Test Campaign

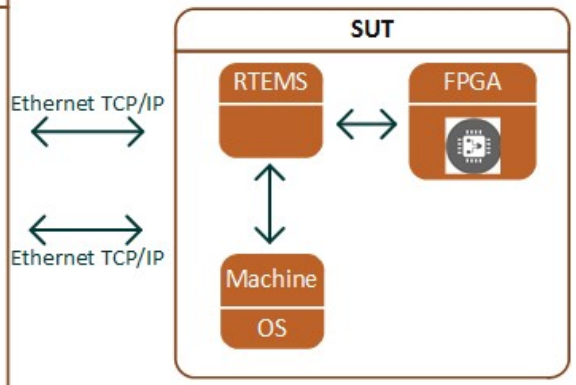
Step 5: Validation & Monitoring

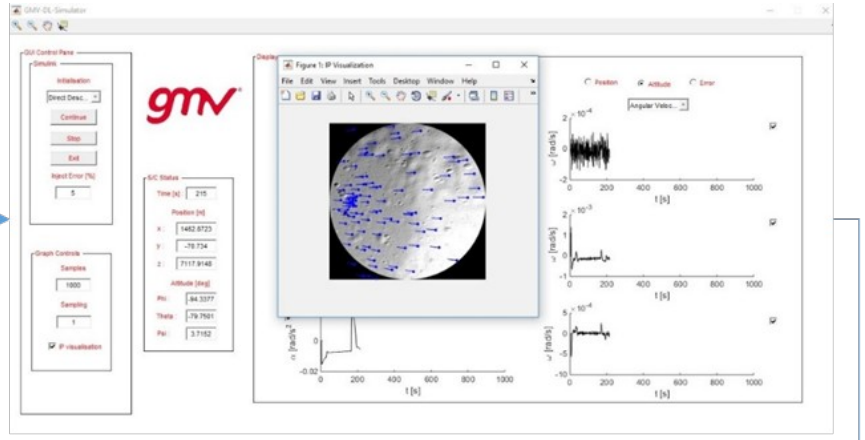
The autonomous vision-based navigation demo with reconfigurable HW capabilities is validated and verified in this step. The art2kitekt© tool suite coordinates the test system tools, while monitoring the temporal behavior of the SuT in runtime.

ENABLE-S3

- UC8 – Reconfigurable Video Processor








Xilinx Zynq UltraScale+ MPSoC ZCU102 Evaluation Kit

gmv INNOVATING SOLUTIONS

ITI
INSTITUTO TECNOLÓGICO
DE INFORMÁTICA

ThalesAlenia Space
A Thales / Finmeccanica Company

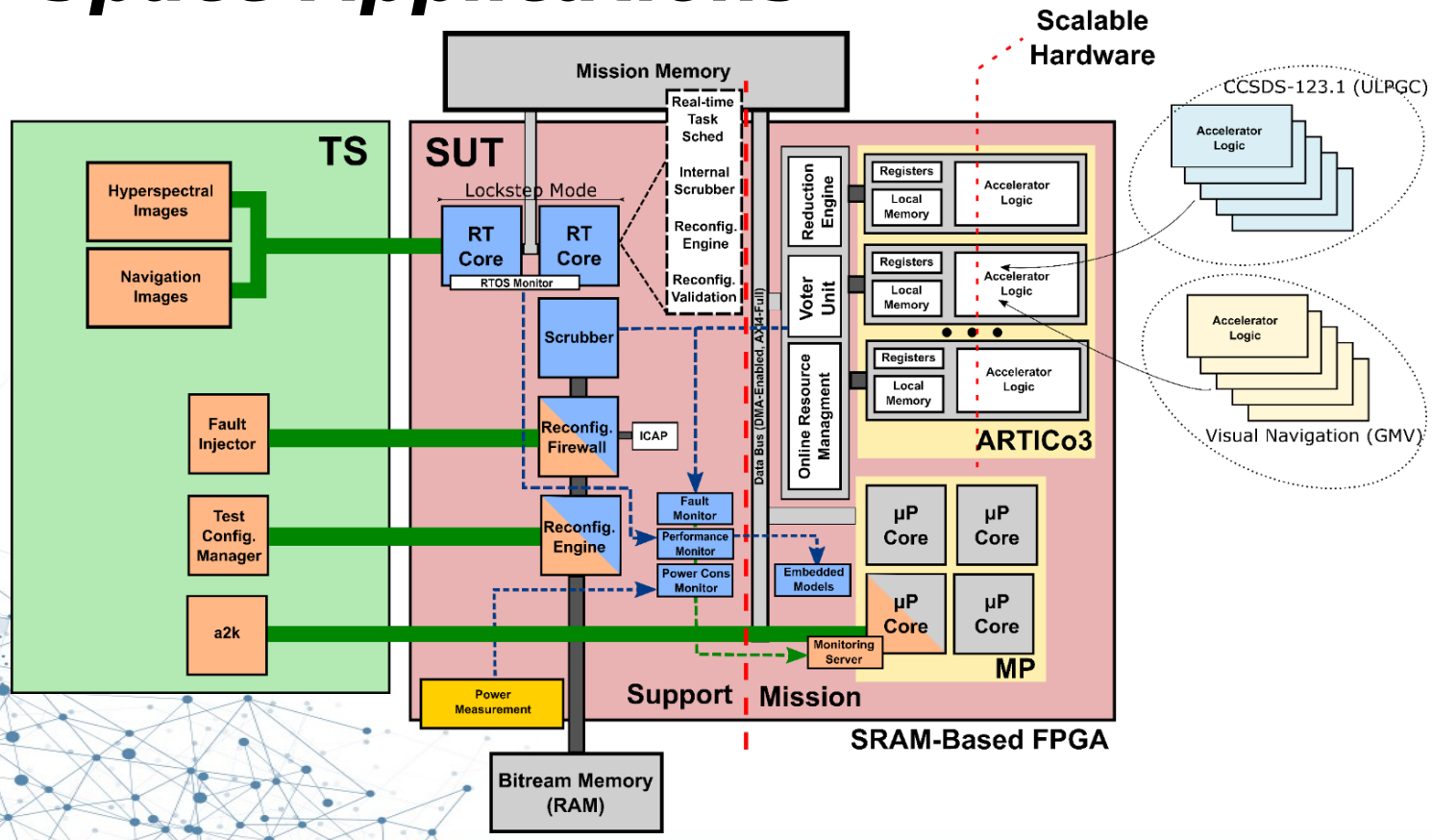
POLITÉCNICA

ULPGC

DOMAIN
AEROSPACE

ENABLE S3

Reconfigurable Platform to test Video Processors Space Applications



An **integrated platform** has been developed based on Enable S3 architecture to deeply **test 2 Reconfigurable Video Processors applications** for Space:

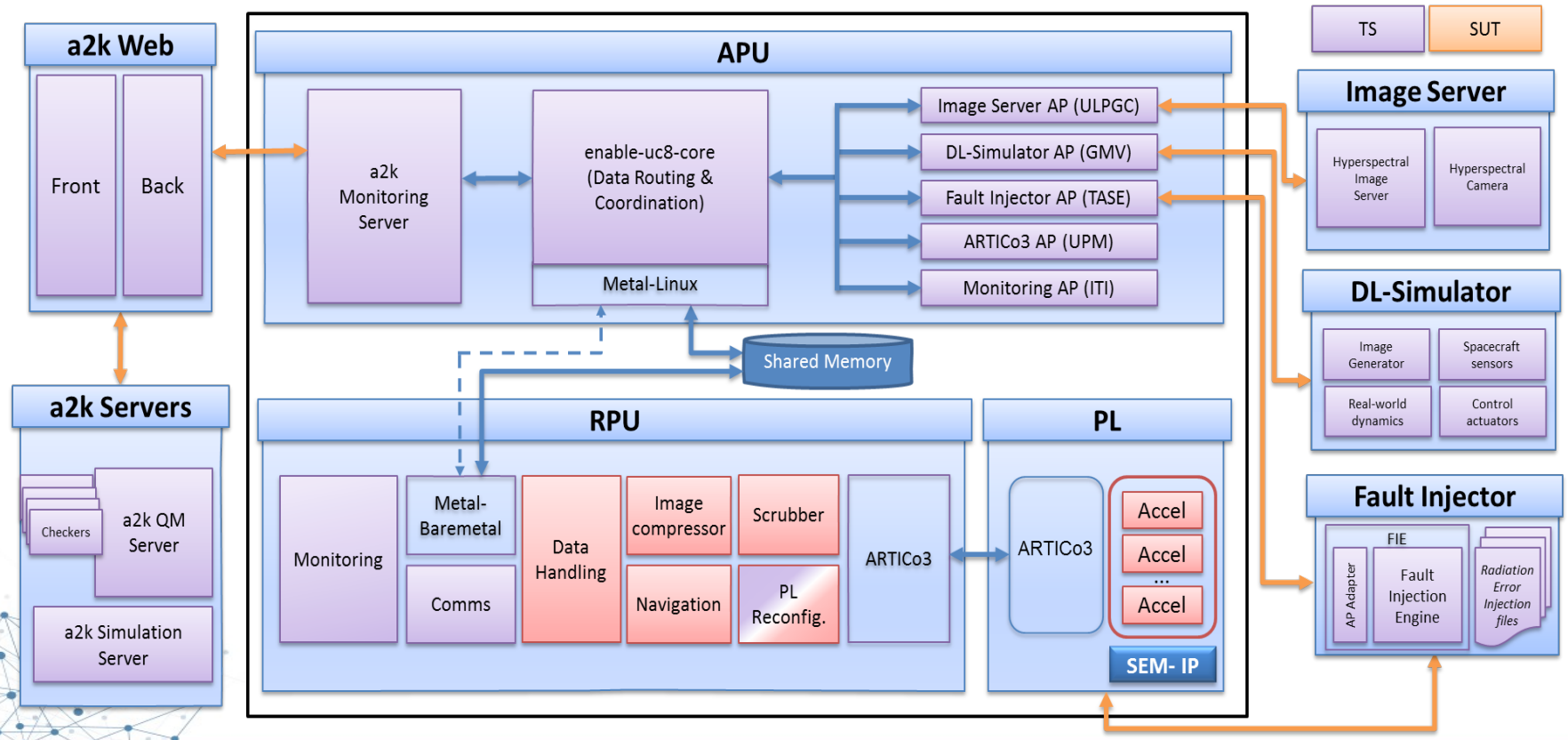
- 3 demos over the same platform to show the behavior under test of these 2 applications
- The technology bricks developed to:
  - insert real failures
  - reduce test scenarios
  - automate the test campaign

ENABLE S3

DOMAIN
AEROSPACE

ENABLE S3

Reconfigurable Platform to test Video Processors Space Applications

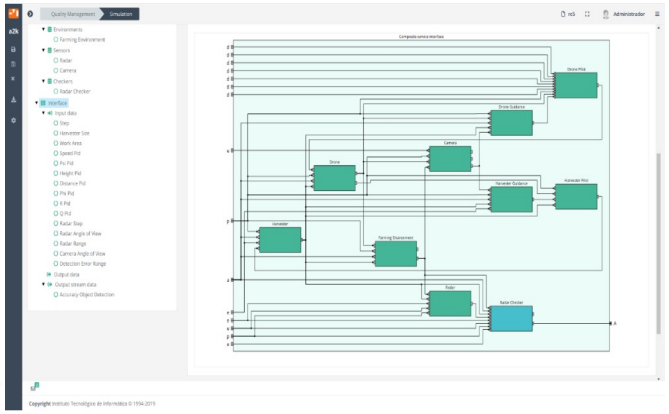


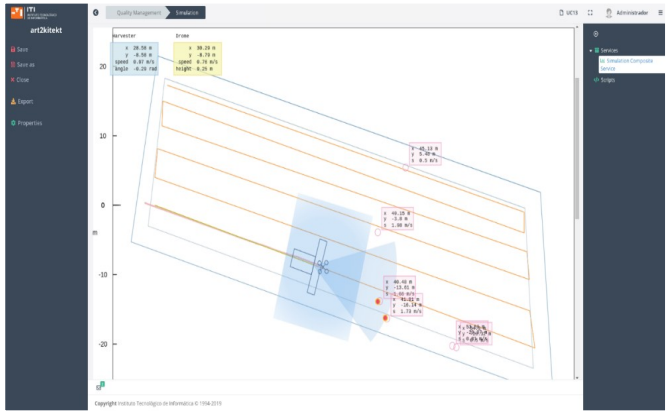
ENABLE S3

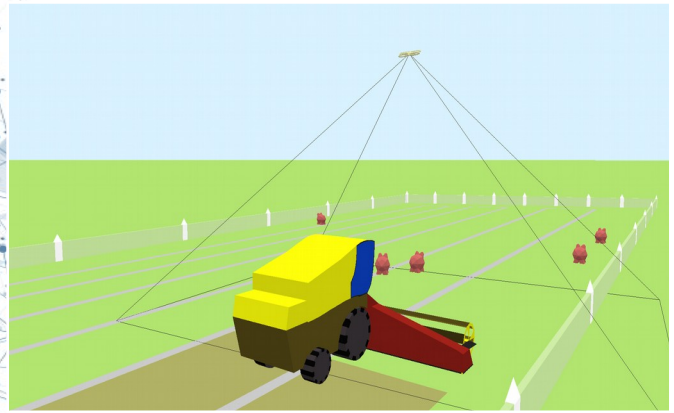
Main impacts due to UC8 Reconfigurable Video Processor:

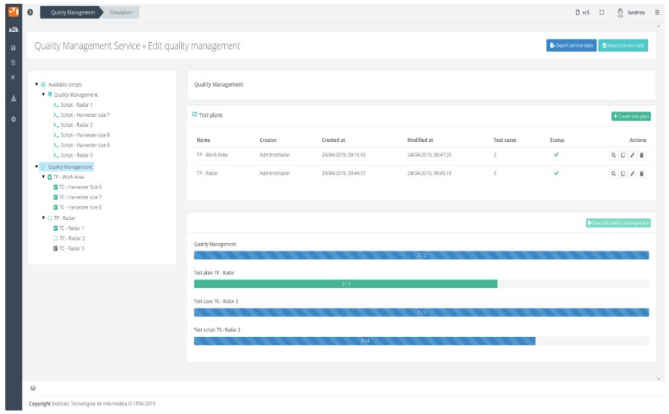
- **Enables the Use of COTS** (SRAM FPGAS in place of Rad-hardened FPGAS) thanks to self-healing and reconfiguration techniques
- **Speed-up of adaptation and its corresponding validation phase** of space Vision-Based Navigation (VBN) strategy and algorithms implementation
- Hyperspectral EO and Navigation **APPs can be tested against radiation using a fault-injection engine**, alternative to go BEAM campaigns
- Use the **same platform for develop and test new applications**
- Develop application using **QEMU (virtual simulator)** before to introduce in the real board
- **Reinforce the critical parts of the design in early stages** of the development by real and unlimited fault injection on the laboratory
- *art2kitekt*© allows the engineer to **monitor system real-time behavior** and **automatize full test campaigns**, measuring real-time performances
- **Model and simulate the applications** to perform test off-line to evaluate the match of the APPs to the mission requirements

- UC 13 – Automated Control Platform

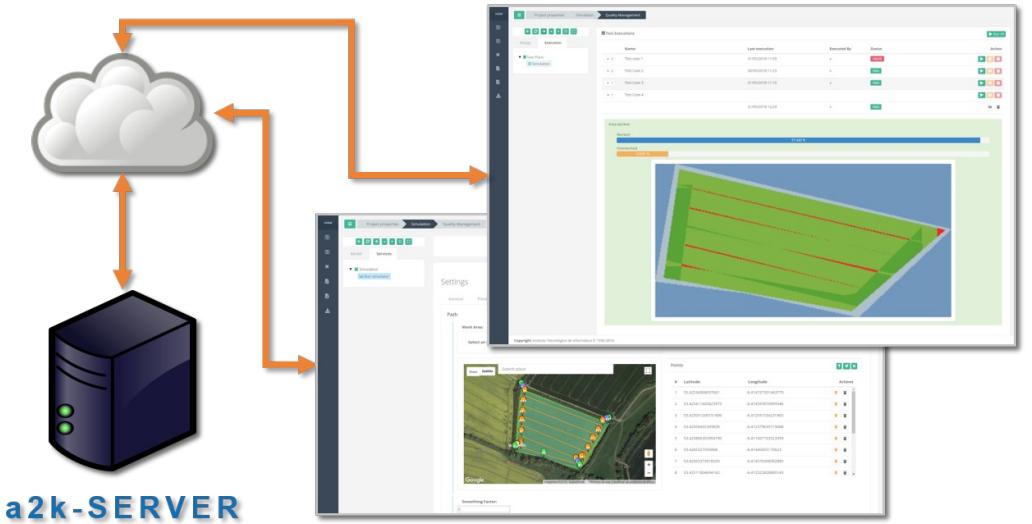






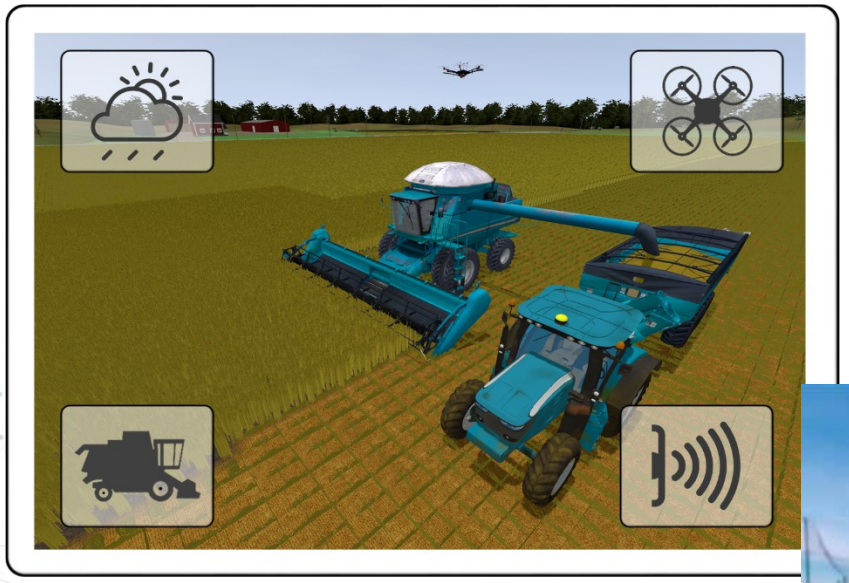


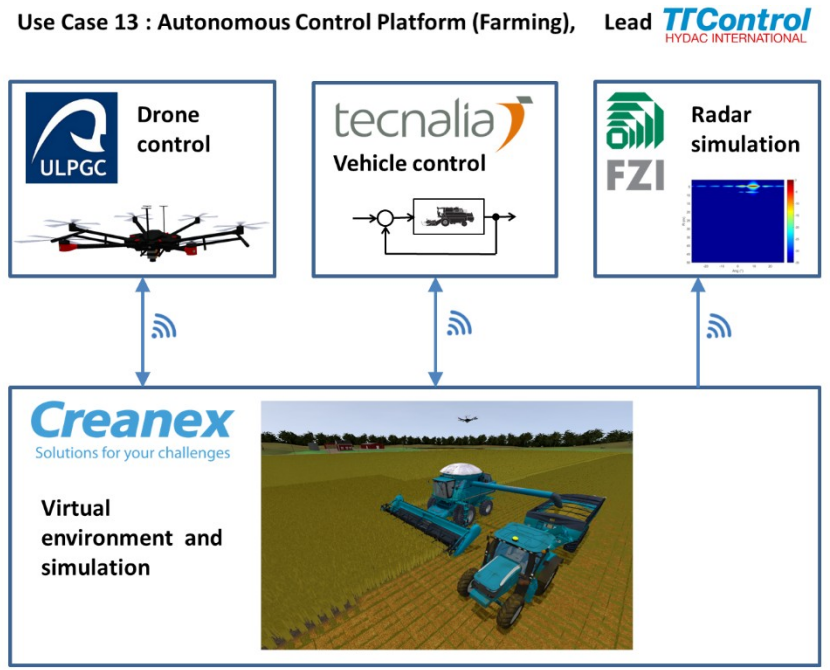
a2k-QUALITY MANAGEMENT



ITI
INSTITUTO TECNOLÓGICO
DE INFORMÁTICA

- UC 13 – Automated Control Platform





ENABLE-S3

THANK YOU

ECSEL JU

The research leading to these results has received funding from the H2020-ECSEL-2015-2-IA-two-stage for ENABLE-S3 – European Initiative to Enable Validation for Highly Automated Safe and Secure Systems Joint Undertaking under grant agreement n° 692455 and from specific national programs and / or funding authorities.