Authors: D. Brizzi, M. Cotogni, L. Lubrano,
M. Panunzio, M. Pasquinelli, L. Saoud

System Verification through the Lifecycle

From the ESA MARVELS study to MBSE deployment in TAS

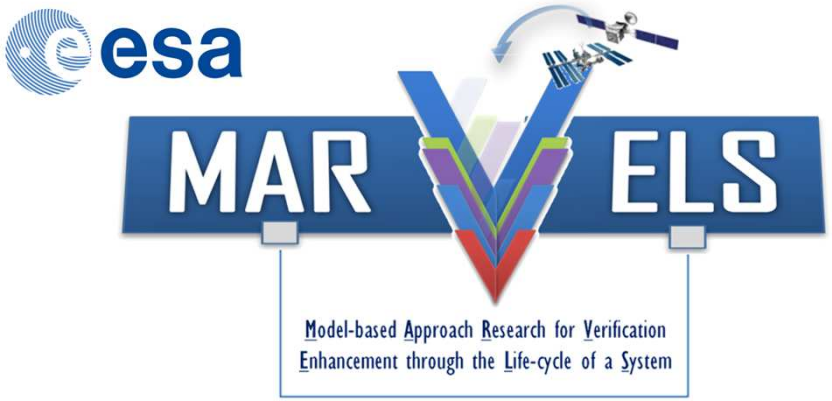
ThalesAlenia Space
a Thales / Leonardo company

Presenters: Marco Panunzio, Letizia Lubrano

Table of contents

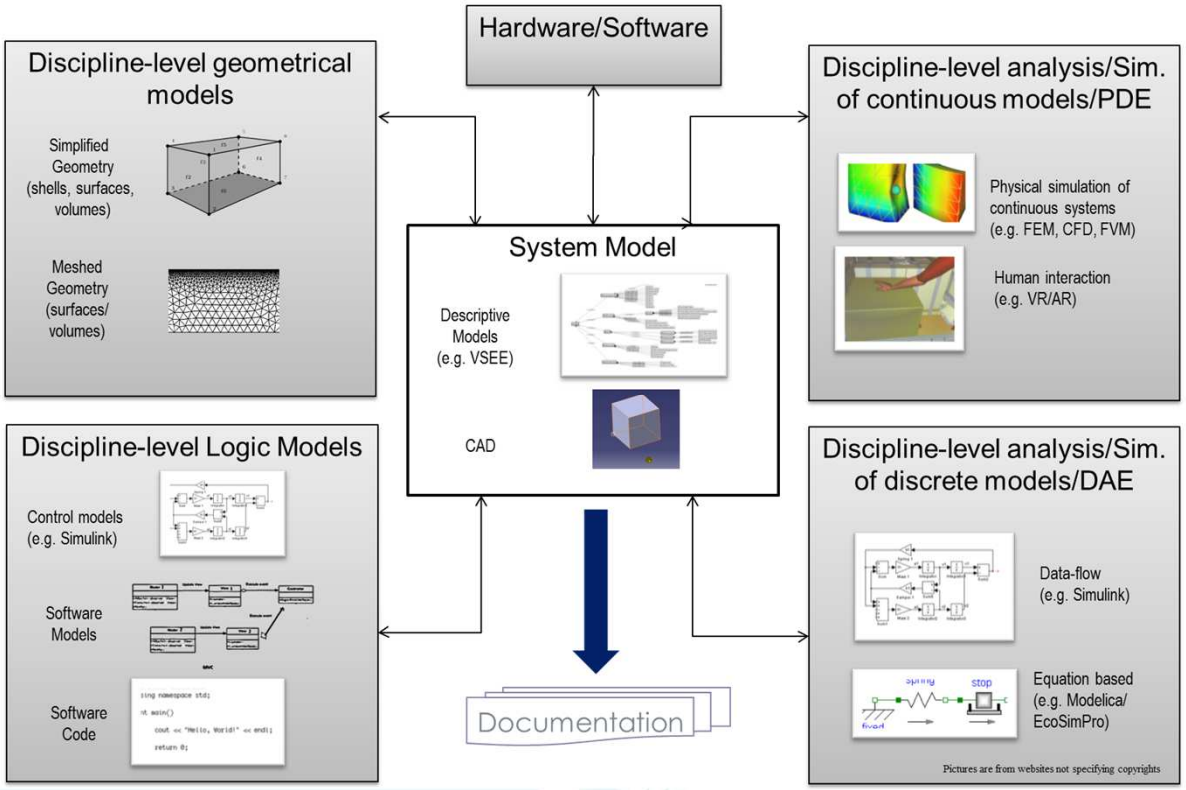
ESA TRP study – System Verification through the lifecycle

- Thales Alenia Space led consortium:
  - **M**odel-based **A**pproach **R**esearch for the **V**erification **E**nhancement across the **L**ifecycle of a space **S**ystem)
  - Intecs, POLITO and VTT as partners
  - ended in 2014
- Objectives:
  - to **define adequate model-based methods** to improve the overall verification process of space systems
  - to **define, prototype and integrate supporting tools** for System Verification along the entire project life-cycle



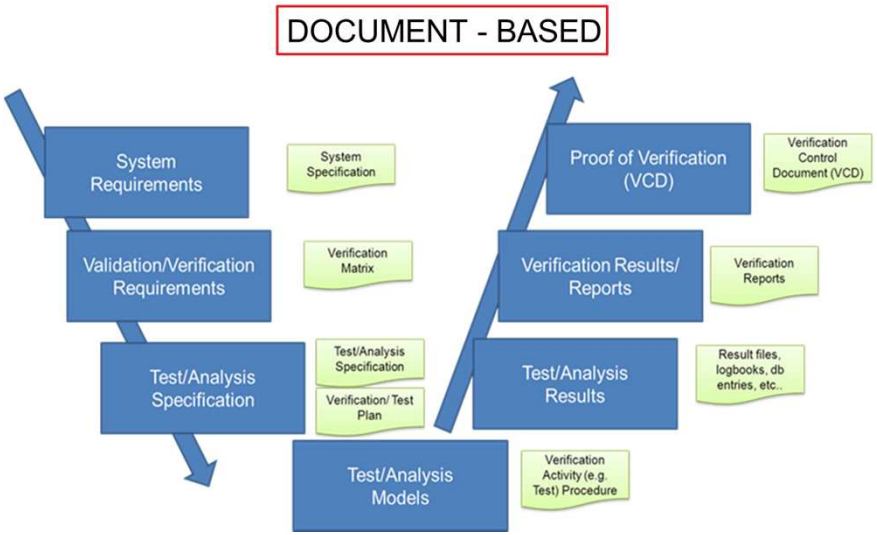
Major outcomes from the MARVELS study - Models

- The "system model" collects all the relevant pieces of information about the product and the process to allow:
  - Consistency between disciplines
  - Clear interfaces between customer/suppliers
  - Consistency between discipline level and system level analysis
- The "system model" can be deployed as a toolchain comprising at least:
  - Descriptive models (e.g. based on ARCADIA, SysML, VSEE)
  - CAD models (e.g. CATIA)



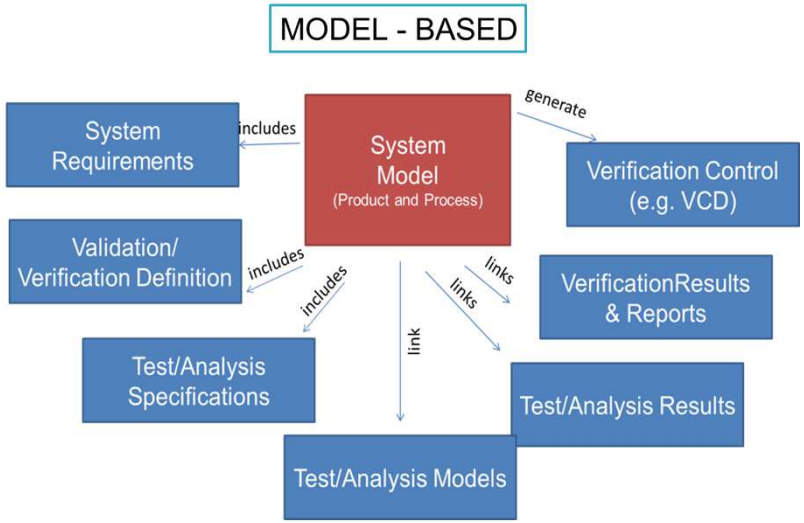
VSEE – http://www.vsd-project.org/
SysML – http://www.omgsysml.org/
CAD – Computer Aided Design
ARCADIA - https://www.polarsys.org/capella/arcadia.html

Major outcomes from the MARVELS study - Lifecycle



Same Tasks but enhanced by:

- Co-engineering (teamwork on the model)
- Concurrent Engineering (between Architects, IVVQ specialist and AIT practitioners)
- Link between design, calculation models and tests



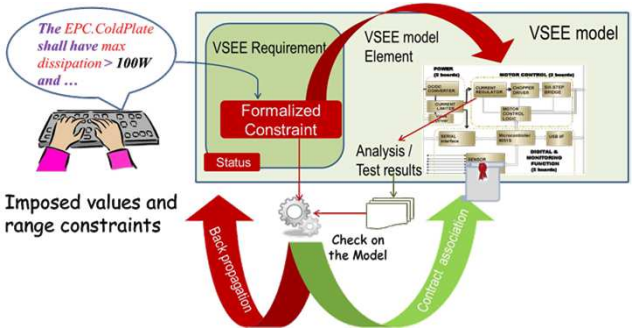
More consistency, more product-oriented work, less paperwork

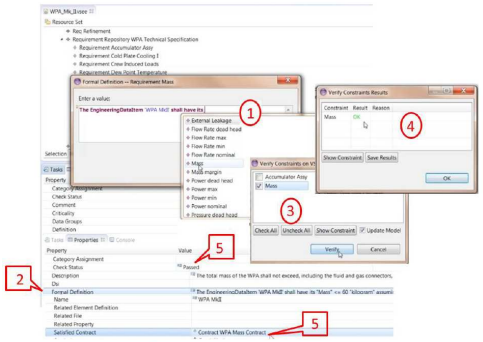
IVVQ – Integration, Validation, Verification and Qualification
AIT – Assembly, Integration and Test
VCD – Verification Control Document

ThalesAlenia Space
a Thales / Leonardo company

Major outcomes from the MARVELS study

- **Requirements vs. Models**
  - Textual nature of requirements vs. formalism of MBSE
    - with a MBSE environment it is possible to **be assisted to write correct requirements**, and store them **as models** which can be interpreted by a machine
    - "Formal" requirements can be used to perform **checks on the model and on the analysis/test results**
    - Requirements are connected to formal "**assumptions**", showing the limits of applicability
    - Once the requirements is verified, the requirement + related assumptions becomes a "guarantee", to be **checked for verification program in case of re-use**
  - INTECS developed and demonstrated a prototype to demonstrate the feasibility of the approach

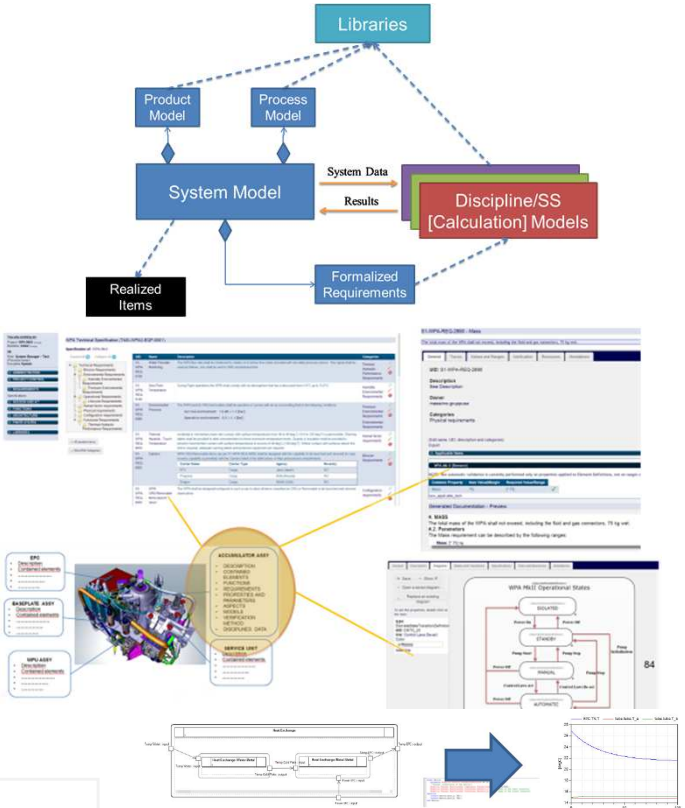




ThalesAlenia Space
a Thales / Leonardo company

Major outcomes from the MARVELS study

- **Process model, product models and collaboration**
  - Design, Verification Activities and related models
    - Definition of **links** between of discipline/system analysis and test models, the related activities and the link with the verification control techniques
    - Definition of a **collaboration strategy** taking into account the sharing of MBSE object libraries and the **improvement of review process** thanks to MBSE approach (supported by Industry-Agency Workshop)
    - Use of a **generated VCD as a dashboard** to share the verification status and enhance collaboration
  - TAS-I/POLITO performed a validation of the concept using a Modelica based simulator and a web-based distributed modelling environment connecting requirements, design and verification activities
- **Re-use of models and of past projects data**
    - **Critical review of the VSEE data model w.r.t. re-use** (introduction of libraries concept)
    - Methodology to compare and use past projects data (past models or anomaly databases as ESA MATED)



POITO – http://www.polito.it
MATED – https://mated.esa.int/mated
SS – subsystems
Modelica - https://www.modelica.org/

From MARVELS study ideas to TAS practices

- The MARVELS study provided a **medium-long term perspective** of an optimal model-based process with related recommendations
- Among the various initiatives in Thales Alenia Space to innovate and improve constantly our products and processes, we present two of them as example of **current implementations of the main MARVELS recommendations**:
  - Improvement of the requirements based approach
    - Focus on concurrent engineering between design, verification and AIT teams, and to improve customer/supplier relationship
    - Improvement of the VCD compilation through suitable toolchain
  - Introduction of the model-based approach in all TAS projects
    - Methodology: focus on the system model and how it can support the Avionics design, IVVQ and the interaction with related models
    - Deployment status

TAS – Thales Alenia Space
IVVQ – Integration, Validation, Verification and Qualification

Improvement of the Verification activities during test campaigns

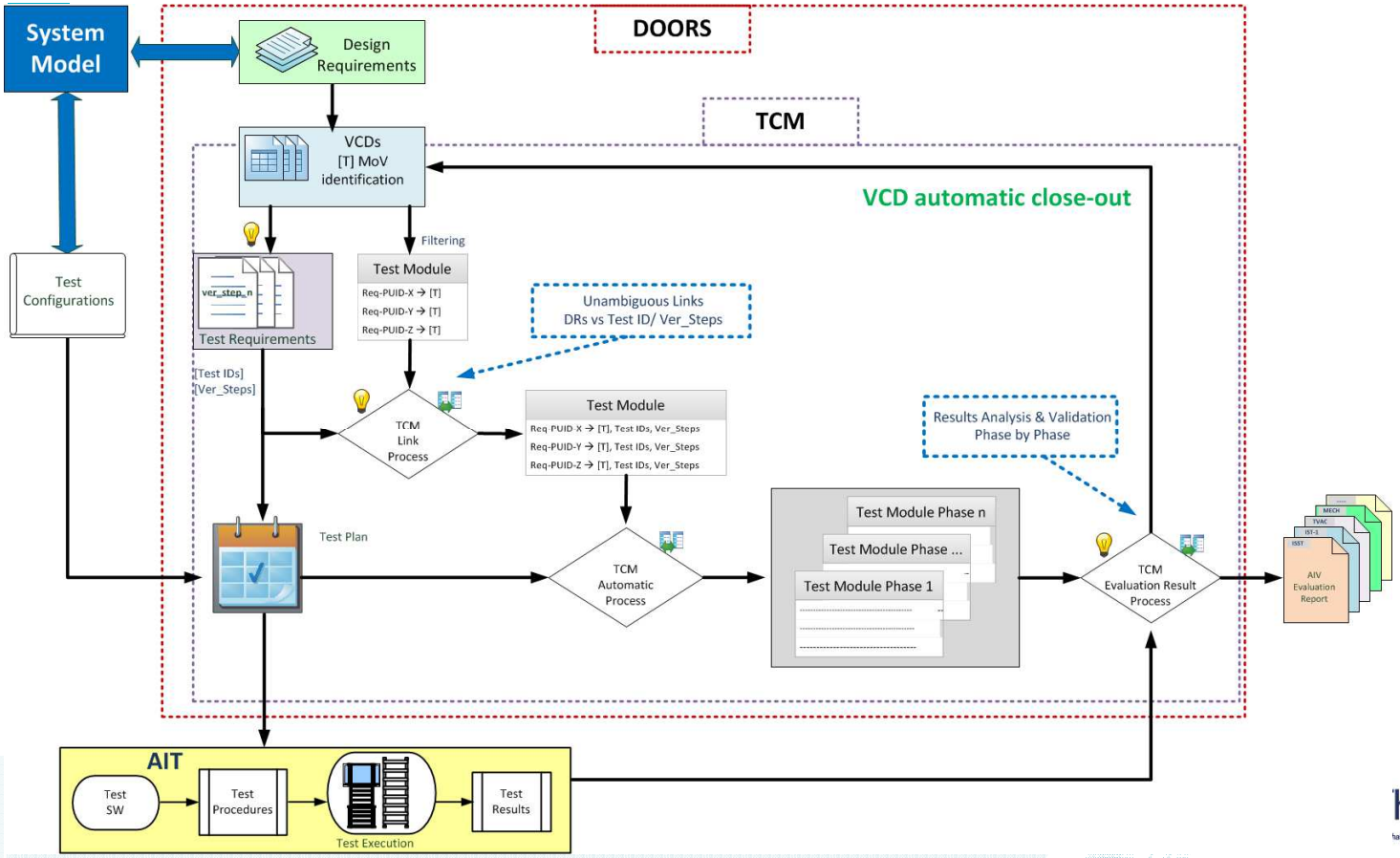
- TCM Preamble:
  - The model-based-methods shall be supported by suitable tools able to strictly trace the **verification** by test even in a complex environment as the **Satellite level test campaign**.
  - The **model-based-methods** will allow to clearly identify in early program phase the verification methods to apply to each design requirement and so determine the set of the design requirements to be verified by **Test** through the **VCD**.
  - Verification approach shall be as much as possible **transversal** to the different **level** of the product from element to system in order to capitalize the results and in **common** to the different **disciplines** allowing to **knowledge sharing** and speed up the process.
  - **DOORS** is the main tool adopted by industry to manage the design requirements.
  - The world is **paper-less** oriented.

Test Campaign Manager (**TCM**) framework was born based on above…

Improvement of the Verification activities during test campaigns

- **TCM Objectives:**
  - to support the Verification by Test by **increasing the traceability** between the design requirements and dedicated steps of a (complex) test campaign leading a **reliable** requirement closure;
  - to **exploit a unique Data Base** where the design requirements (DRs) and verification control data(VCDs) are available;
  - to speed up the **test campaign preparation** and related **reviews** (TRR, PTR, TRB);
  - to support the **standardization** of the verification approach between levels and disciplines
- **TCM content**:
  - it is an IVVQ framework, a set of **DOORS** tools, being DOORS the Data Base of DRs and VCDs;
  - it allows to easily write **test requirement** specifications (TRs) as DOORS module, and identify special objects called "**verification steps**" designed to provide evidence of DRs verification achievement during the tests;
  - it enables **test campaign planning and control**;
  - It allows to **evaluate** and assess the test **results** and **automatically close the VCD**

Improvement of the Verification activities during test campaigns



halesAlenia Space

Improvement of the Verification activities during test campaigns

S1C **AVS** VCD: VCD: [T]@ S/C level

S1C AVS Test Requirement
Test Execution Section
with verification steps

'Avionic Subsystem Requirements' current 2.5 in /SENTINEL-1C/1-Requirements/Level-III Subsystems (Formal module) - DOORS

PUID	Requirement Text	Assignment	SoC	Stage	SC	SS	SA	EQ	UN	Verification Document(s)	VD(s) Title	VD Section	VM Status	VCB	V Status
[S1-AVS-REQ-040020]	**Title: Satellite Mode Transition** The satellite mode transitions shall be performed both autonomously and on ground command.	#ASW	C	ACC	R T					S1CD-PL-TAI-SC14-0002 S1CD-RS-TAI-SC01-0016	Spacecraft Test Plan Avionics Integrated Subsystem Test Requirement	9.11	C O	S1CD-MN-TAI-PM03-0371	OPEN
[S1-AVS-REQ-040080]	**Title: Separation detection** The AVS shall apply a majority voting logic to the triple HW separation signals in order to confirm the separation from launcher. The detected and confirmed separation shall be provided as a telemetry status bit.	#ASW	C	ACC	R T					S1CD-PL-TAI-SC14-0002 S1CD-RS-TAI-SC01-0016	Spacecraft Test Plan Avionics Integrated Subsystem Test Requirement	9.13	C O	S1CD-MN-TAI-PM03-0371	OPEN
[S1-AVS-REQ-050205]	**Title: Configurable Steering attitude** Ground shall be allowed to configure steering attitude angles.	#ASW	C	ACC	R T					S1CD-PL-TAI-SC14-0002 S1CD-RS-TAI-SC01-0040	Spacecraft Test Plan Integrated Spacecraft Test Requirement (IST) Mission Time Line		C O	S1CD-MN-TAI-PM03-0371	OPEN
[S1-AVS-REQ-080010]	**Title: SA Position Setting** AVS shall mange the SA Position Setting. The ASW shall drive the	#ASW	C	ACC	R T					S1CD-PL-TAI-SC14-0002 S1CD-RS-TAI-SC01-0015	Spacecraft Test Plan Power Integrated Subsystem Test Requirement	9.5	C O	S1CD-MN-TAI-PM03-0371	OPEN

'Avionics Integrated Subsystem Test Requirement - AVS ISST' current 1.4 in /SENTINEL-1C/2-Verification/Test Requirement (Formal module) - DOORS

Object Text | Change Record

9.3.7 Test Execution

With the S/C Configured as per Test Configurations and all the Wheel in "OFF" status:

#AVS_03_#VER_STEP_10

For Each Wheel:
- Switch on RW, thourgh TC (137,131)
- Check RWs ON/OFF Status
- Acquire RW Bearing Temperature and Motor current TM (3,25)
- Calculate RW Power Consumption from current and voltage, TM (3,25)

##

In order to store in the CKPM buffer the RW speed for the test:

Reset CKPM buffer using TC (137,27)
For each Wheel load into CKPM buffer, thourgh TC(137,21), the run-up parameters of the Wheel
Enable RWA Preprocessing Flag using TC(137,21)
Update CKPM buffer TC (137,27)

In order to store in the CKSG Buffer the Enable flag and activate the Wheel run-up:

Reset CKSG buffer TC (137,27)
For Each Wheel Set flags to Enable the Speed Test, TC (137,24)
Update CKSG buffer TC (137,27)

Wait run-up completed, 60 seconds

#AVS_03_#VER_STEP_20

Acquire for 15 minutes the following TM (3,25) parameters at the for each RW:
- RW speed Measured and Filtered
- RW Motor current
- RW Bearing Temperature
- Calculate RW Power Consumption from current and voltage, TM (3,25)

/SENTINEL-1C/2-Verification/Test Requirement/SC Test Module

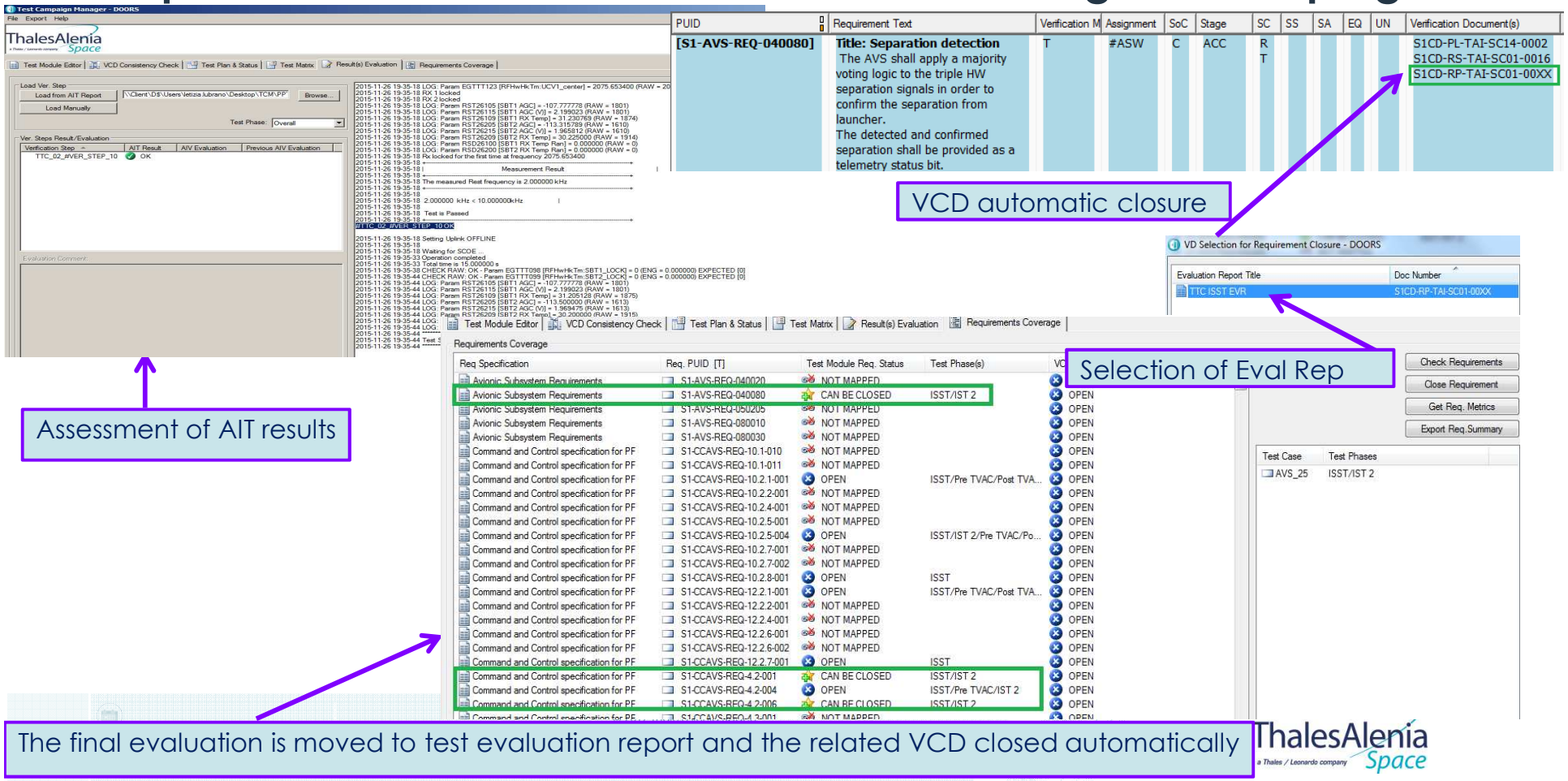
##

SENTINEL-1C/2-Verification/Test Requirement (Formal module) - DOORS

PUID	Object Text	Applicability	TEST ID(s)	Verification STEP(s)
			AVS_07	AVS_10_#VER_STEP_30 AVS_10_#VER_STEP_100 AVS_10_#VER_STEP_110 AVS_07_#VER_STEP_10 AVS_07_#VER_STEP_80
S1-CCAVS-REQ-4.3-006	It shall be possible to individually command all AVS equipment directly from the ground.		AVS_03 AVS_04 AVS_06 AVS_07	AVS_03_#VER_STEP_20 AVS_04_#VER_STEP_20 AVS_04_#VER_STEP_30 AVS_04_#VER_STEP_40 AVS_06_#VER_STEP_50 AVS_07_#VER_STEP_20 AVS_07_#VER_STEP_30 AVS_07_#VER_STEP_40 AVS_07_#VER_STEP_50 AVS_07_#VER_STEP_60 AVS_07_#VER_STEP_70
S1-CCAVS-REQ-5.2-001	A telemetry packet for successful command acceptance shall be generated by the receiving application for every telecommand properly received and containing valid data, if the acceptance acknowledgement flag is set in the telecommand		AVS_03 AVS_04	AVS_03_#VER_STEP_10 AVS_03_#VER_STEP_30 AVS_04_#VER_STEP_10

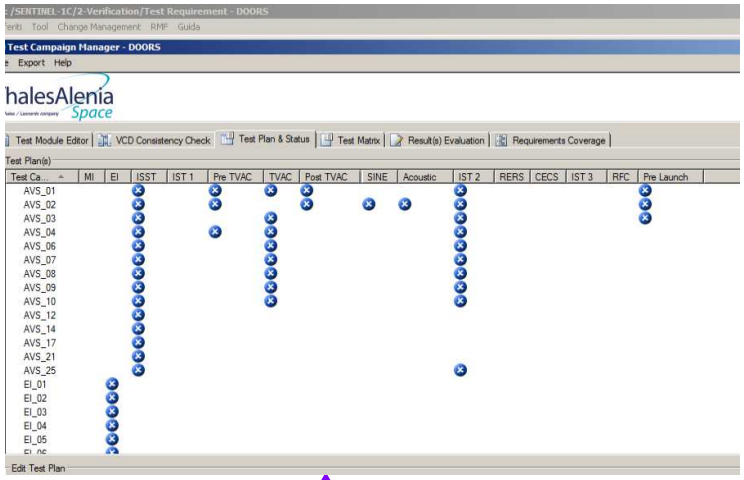
Test Module: AVS DRs linked to Test ID and verification steps

Improvement of the Verification activities during test campaigns

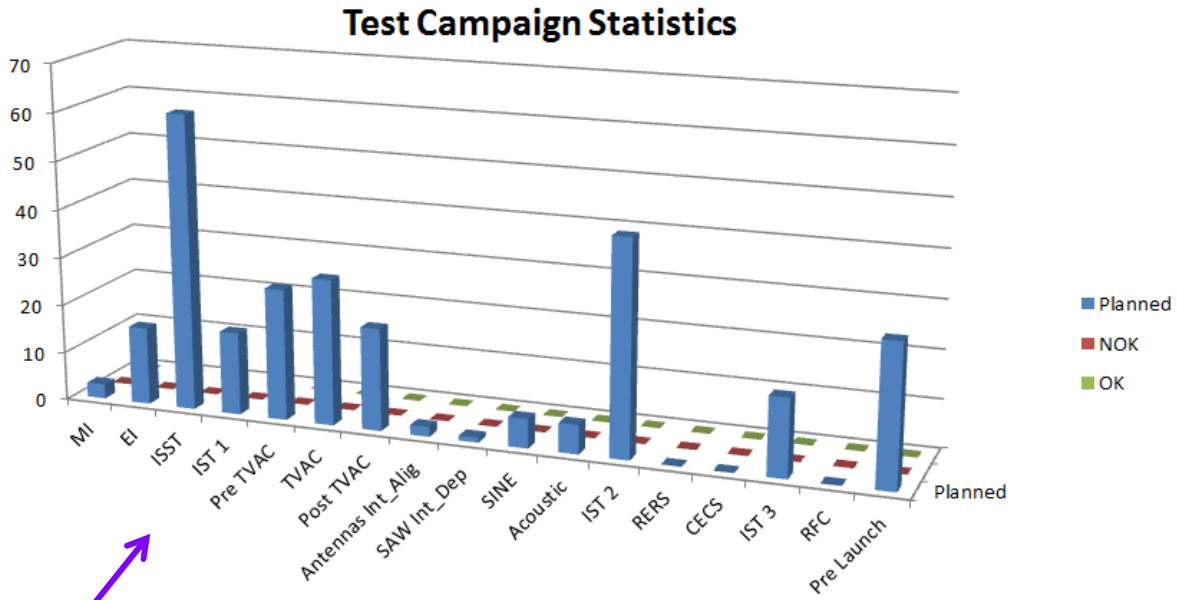


Improvement of the Verification activities during test campaigns

Test Plan and Statistics

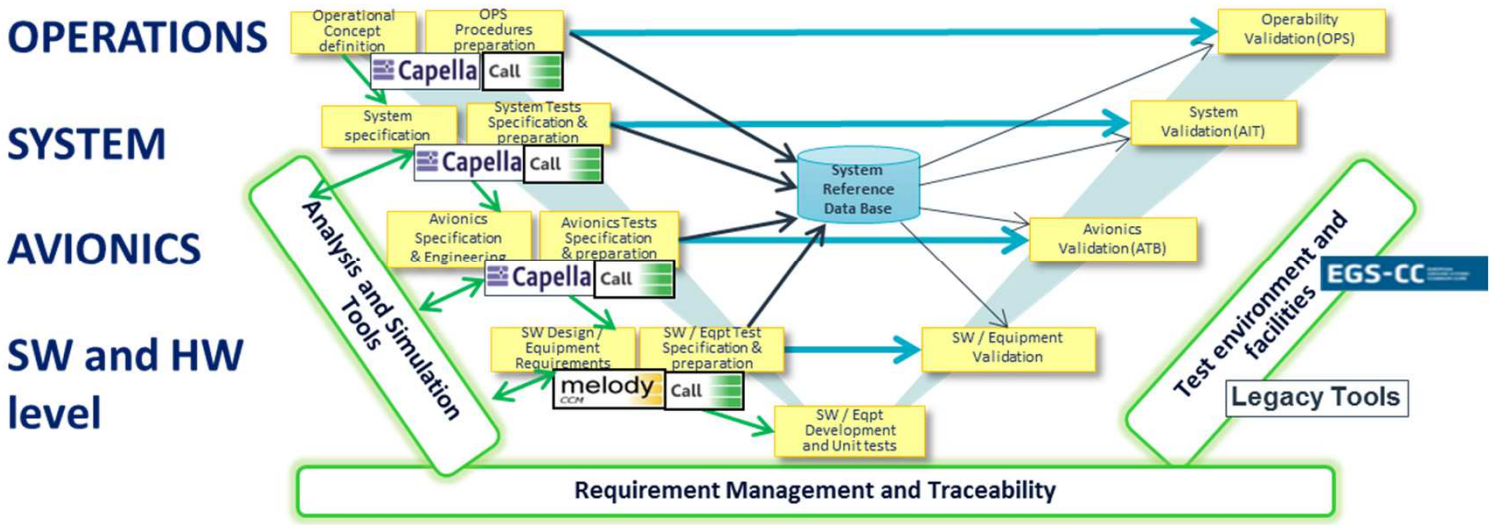


S/C Test Plan Implementation in DOORS



Test Campaign Statistics
- Test status (planned, OK, NOK)
- Design Reqs coverage

MBSE stategy in Thales Alenia Space – Our vision

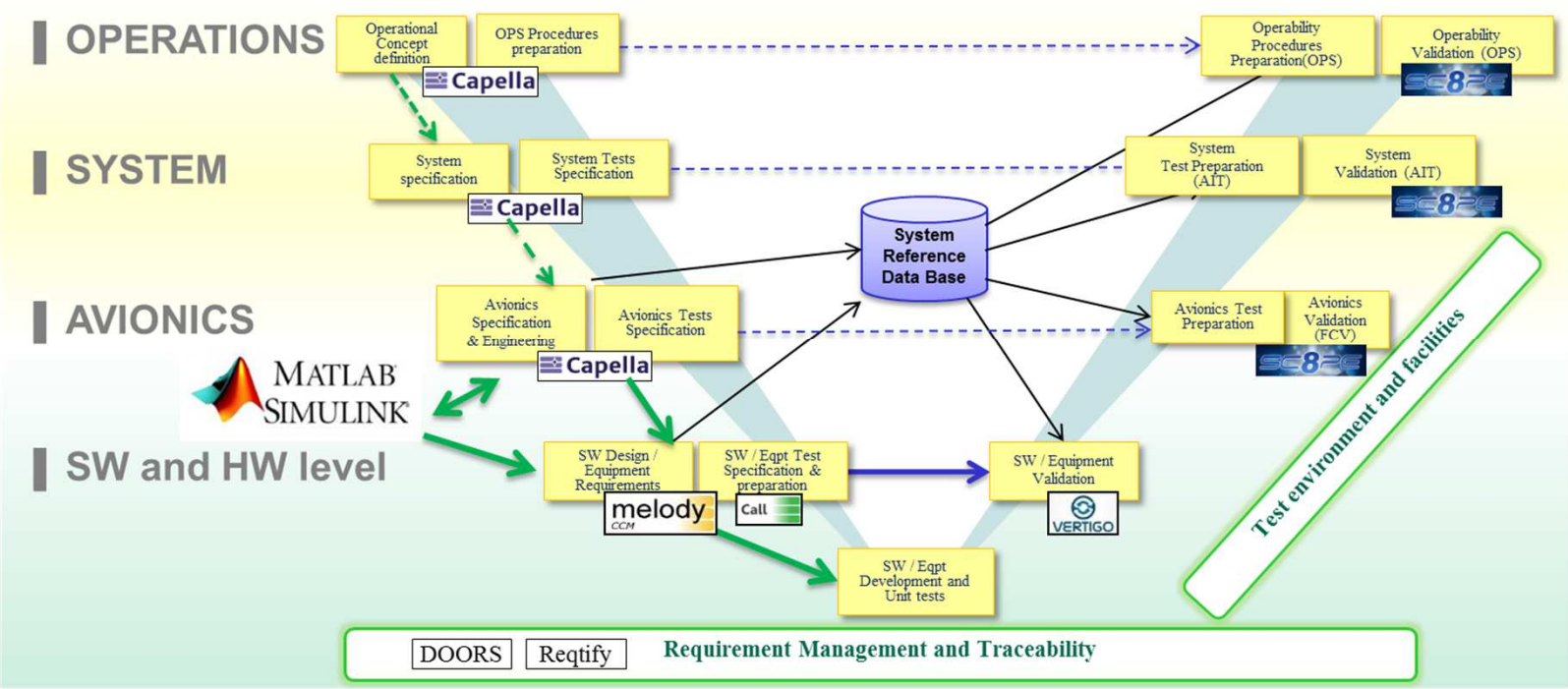


Model Based Design engineering process accross different abstraction levels.

Model based data management process accross different abstraction levels.

Model Based V&V engineering process accross different abstraction levels.

MBSE: current deployment perimeter



Tool assisted design engineering process accross different abstraction levels

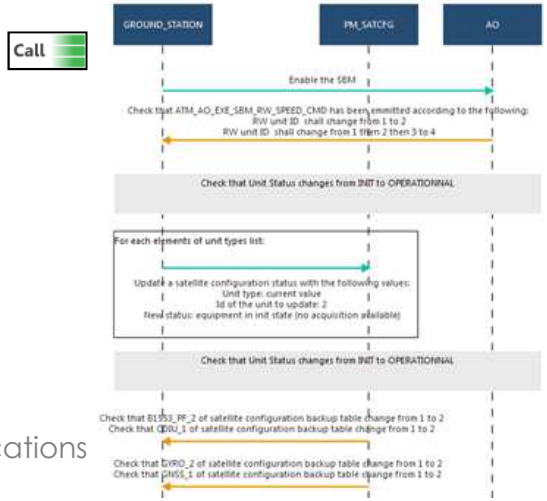
Model Based V&V engineering process accross different abstraction levels.

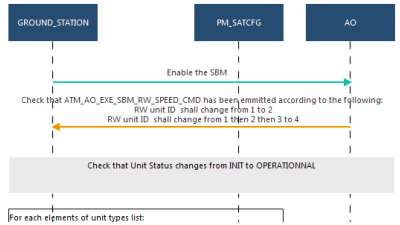
Tool assisted V&V engineering process across different abstraction levels.

Tool assisted SDB engineering process

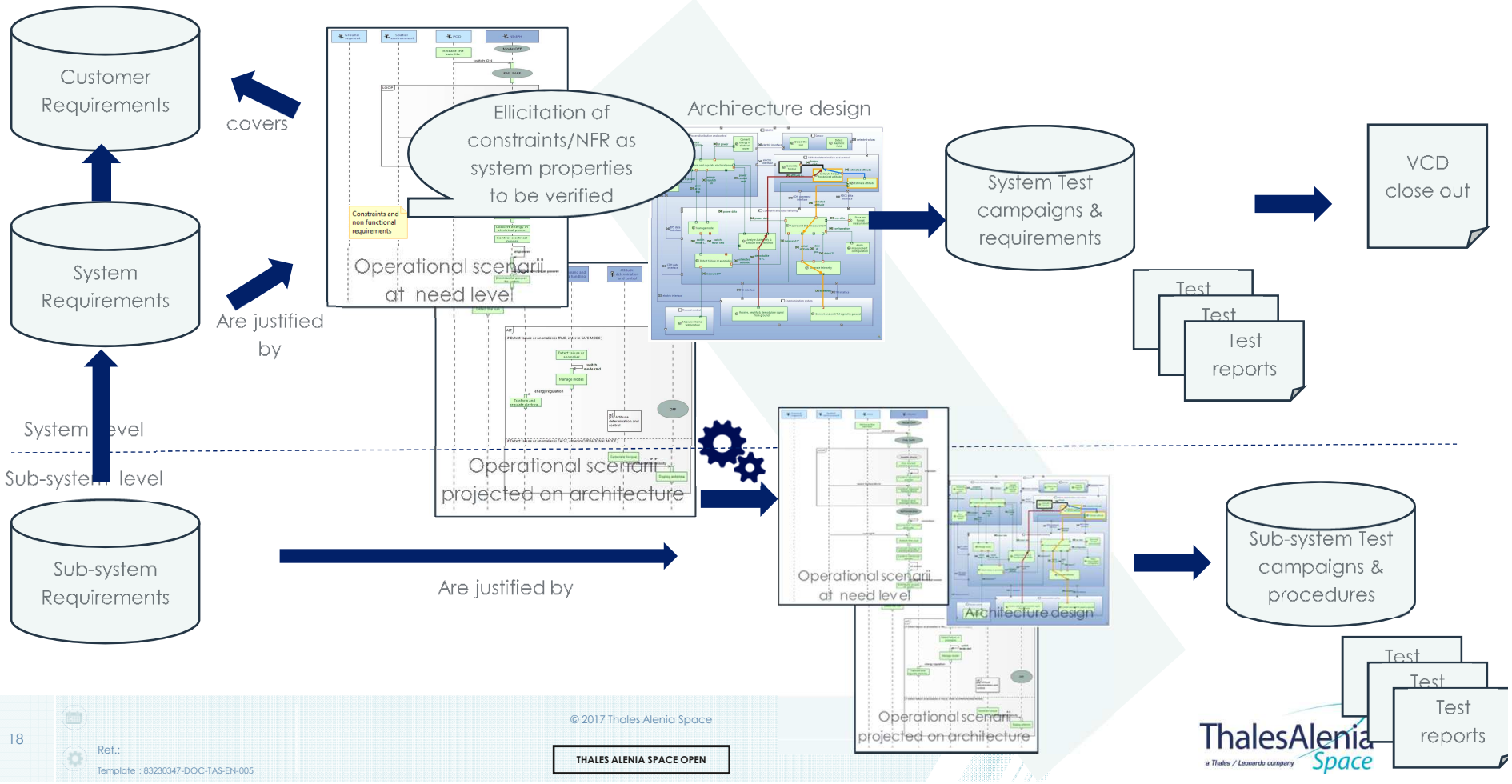
Model-based SW V&V

- Model-based V&V for OBSW => deployed operationally
  - Specification of test sequences defined at SW component-model level
    - Same abstraction level of design
    - Structured modeling of test plans and test sequences
    - Using the model-based "Call" language
      - Leveraging e.g., sequence diagrams and interaction-based specifications
  - Automated derivation of executable test scripts from the V&V model
    - In a process similar to software code generation
- Lesson learnt from Model-based SW V&V are being used to understand applicability to the right perimeter of avionics and system V&V
  - Suitability of language constructs
  - Matching the abstraction level, entities and V&V objectives at those levels
  - Successful application of MBSE for design / code generation at avionics / SW in TAS stems from a bottom up approach
    - We are following the same recipe for Model-based V&V





Current model-based deployment focus: Capella



Current MBSE deployment focus with Capella

Enterprise Architecting (operational capabilities and need, orientations, etc.)

Multi-physics: 3D, power models, thermal models, etc.

Algo, Real-time Analysis, NF, Etc.

ARCADIA

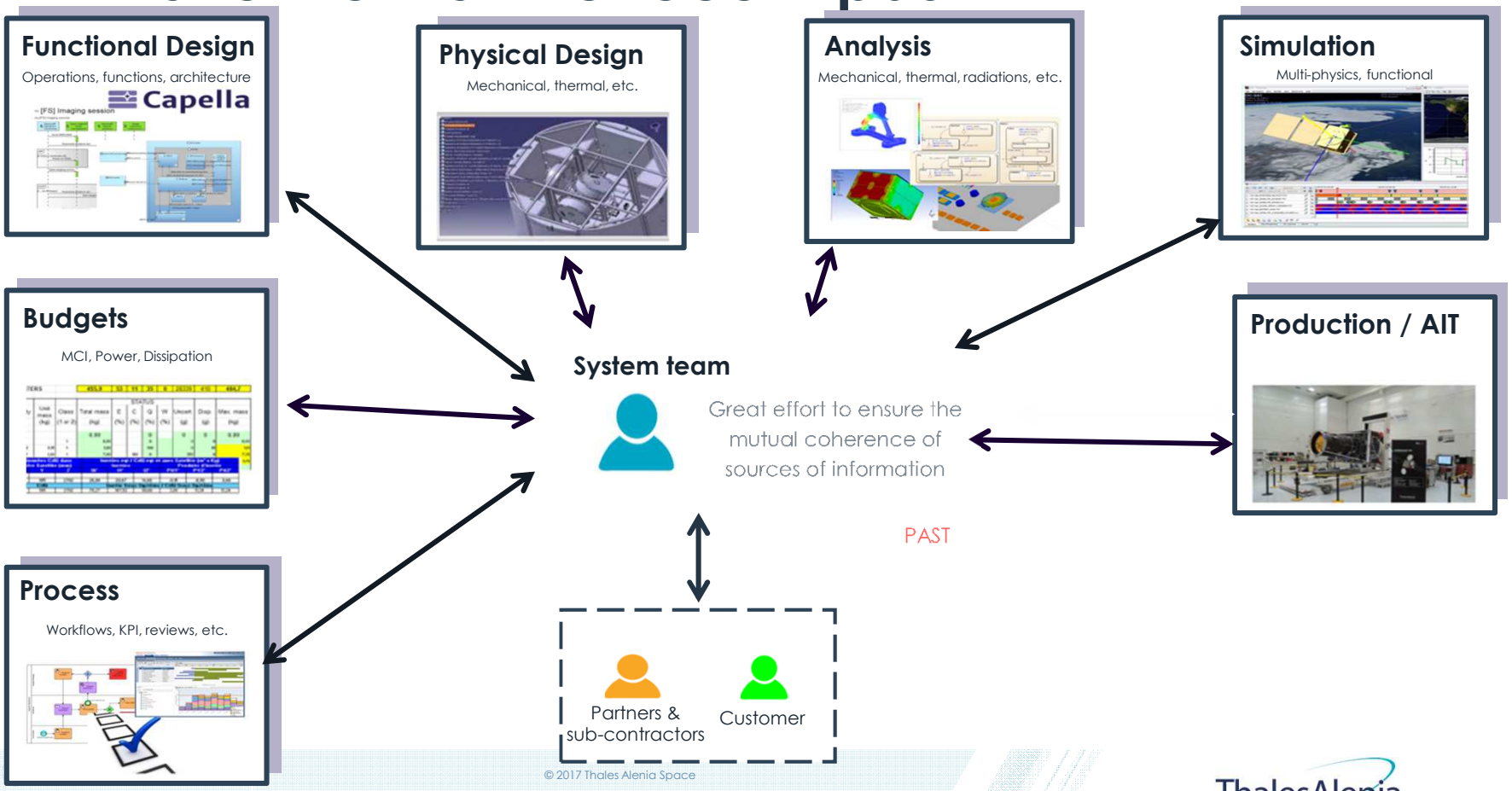
Capella

V&V

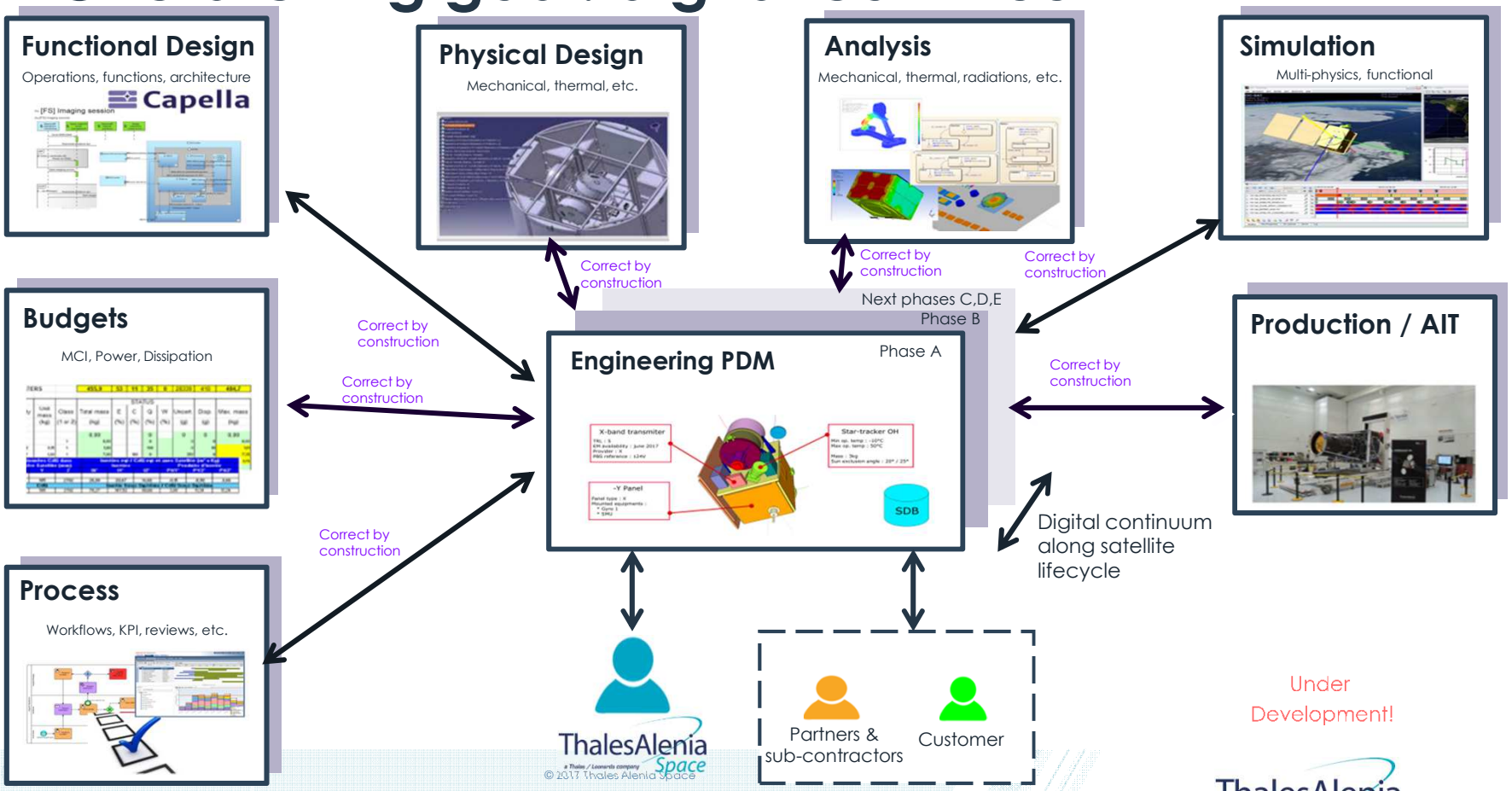
Detailed design, development

ThalesAlenia Space
a Thales / Leonardo company

An overview of the recent past



Overarching goal: digital continuum



Under Development!

ThalesAlenia Space

Conclusions

- The MARVELS study analyzed the potential directions for effective improvement of IVVQ using a model-based approach
- Major change of MBSE application in TAS from earlier years: transition from localised experimental applications at SW, avionics, and system, to consistent vision and operational application
- Powered by the Thales tools and methods and through internal developments, TAS is implementing and continuously improving the application of a complete model-based engineering environment in all its activities, including IVVQ and integrating tools belonging to different disciplines
  - Improvement on the way to
    - elicit requirements and system properties to be verified
    - demonstrate the system compliancy
  - Producing valuable inputs to support IVV strategy definition (functional chains, scenario)
  - Deployment of Model-Based V&V at SW level, with upper levels to be targeted next
- Current deployment results are encouraging and will be leveraged to increase further the perimeter, e.g.,
  - Link with Model-based Simulation, Co-Simulation and Model-based V&V for earlier validation
  - Digital continuum