System Verification through the Lifecycle

(MARVELS team)

Final presentation

ESA ESTEC, June 2nd, 2015

Speakers:
Mauro Pasquinelli (TAS-I)
Silvia Mazzini (Intecs)

ESA/ESTEC Contract 4000109030/13/NL/LvH

OPEN

ThalesAlenia Space
A Thales / Finmeccanica Company

Contents

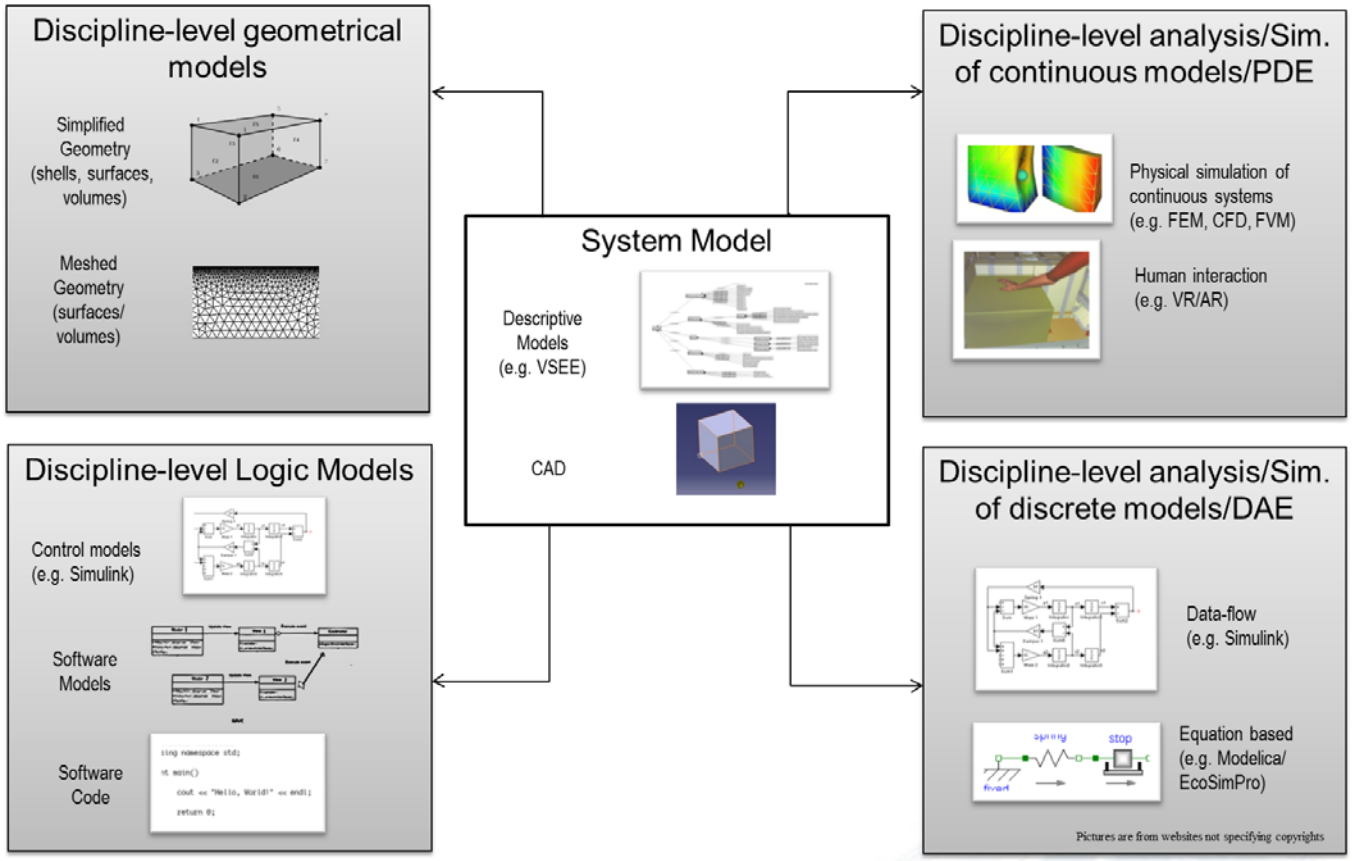
- Context: MARVELS
- Methodology
- Requirements
- Verification Methods
- Verification Management and Teamwork
- Methodology Validation approach
- Conclusions

MARVELS

- ESA TRP study
  - MARVELS = Model-based Approach Research for the Verification Enhancement across the Lifecycle of a space System)
- 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
- References are the outcomes of the Virtual Spacecraft Design (VSD) study and the associated ECSS-E-TM-10-23
  - http://vsd.esa.int

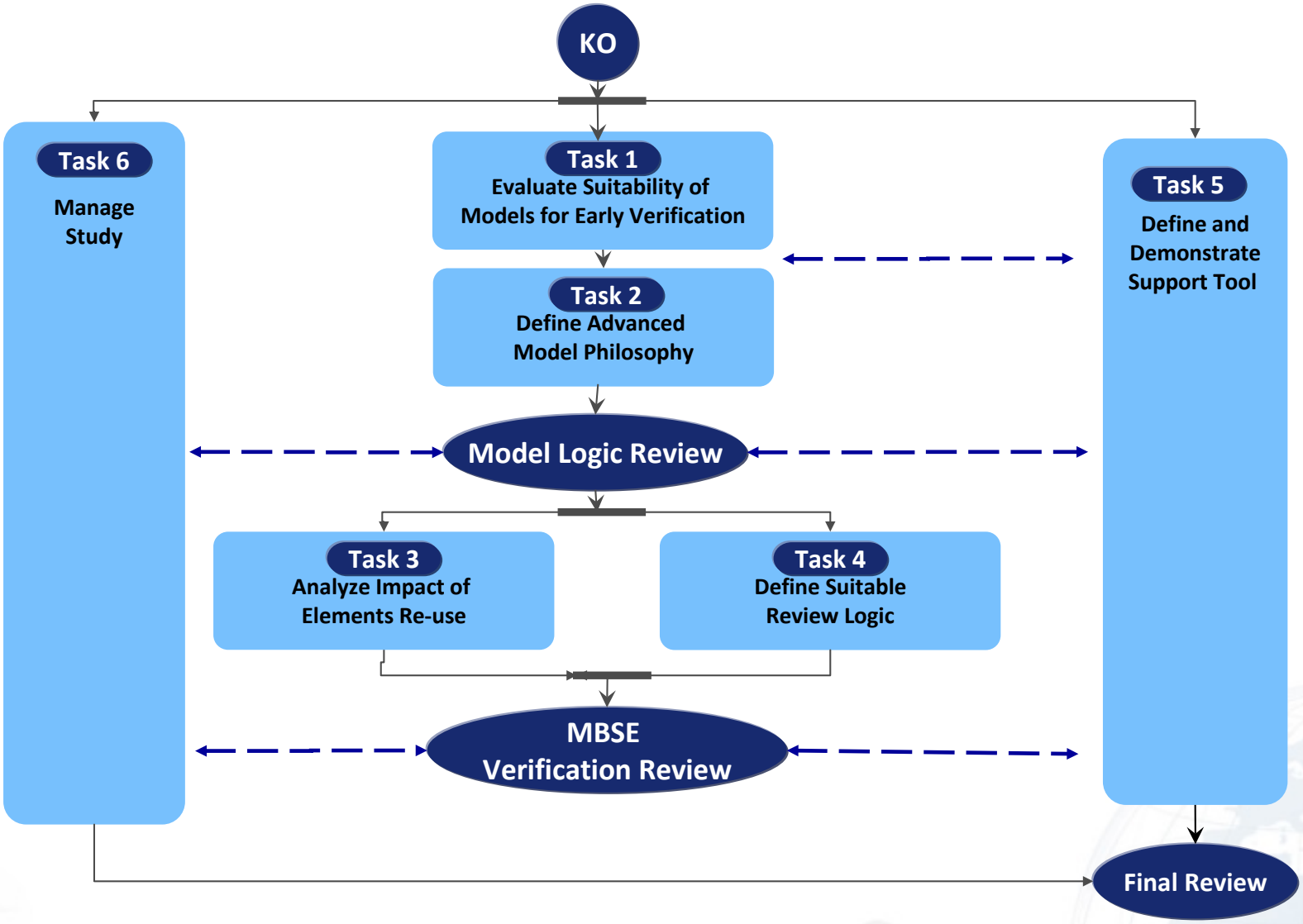
Overview of Model-Based Approaches along the lifecycle

- What is a model?
  - Formal Representations
  - Machine and Human processable
- System model
  - Descriptive
  - Physical (CAD)
- Discipline model
  - Geometrical
  - Physical
  - Logic
  - Calculation



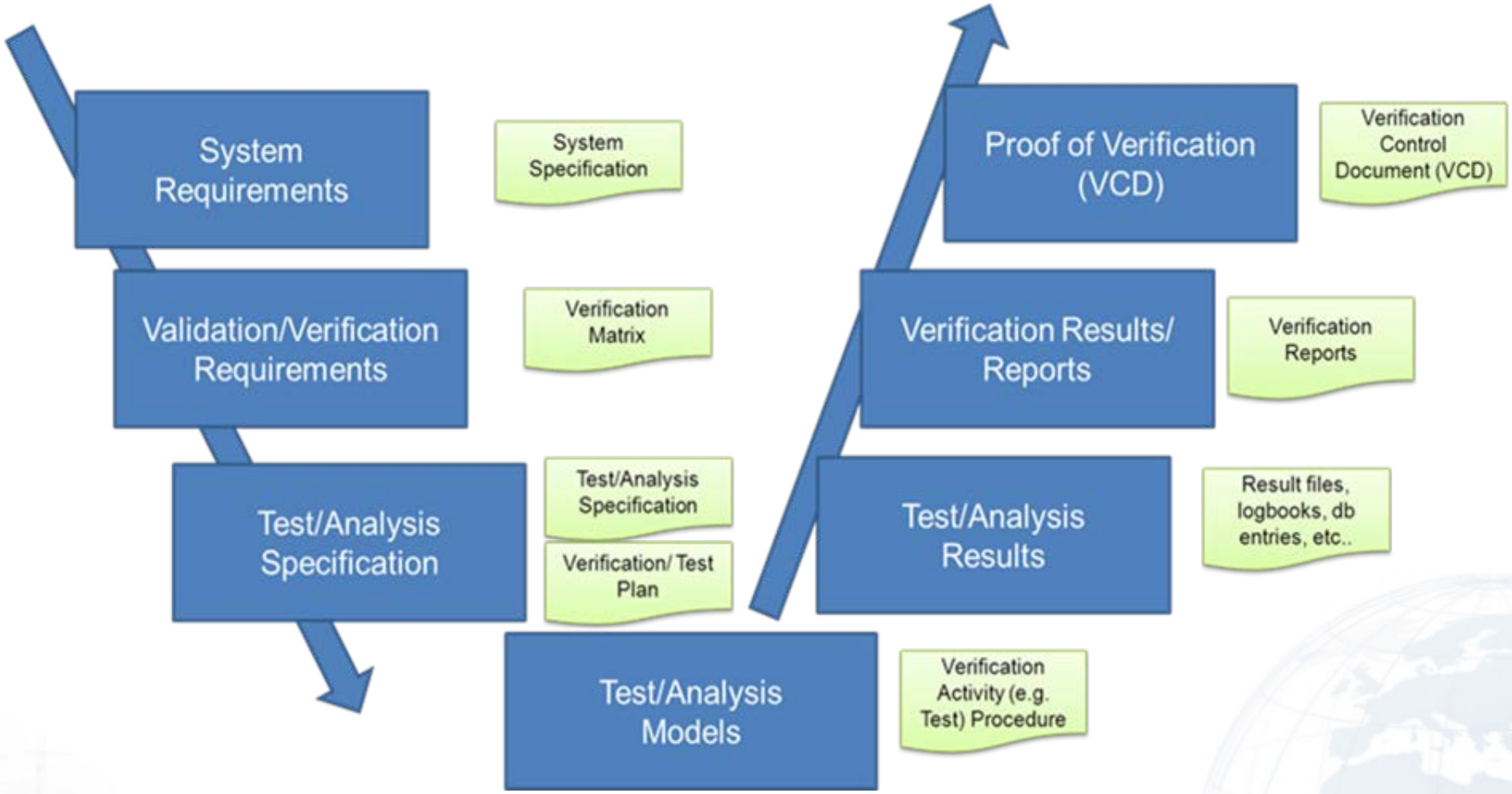
- How they are used along project phases is very different in terms of objectives, types and complexity of models

MARVELS Study Logic

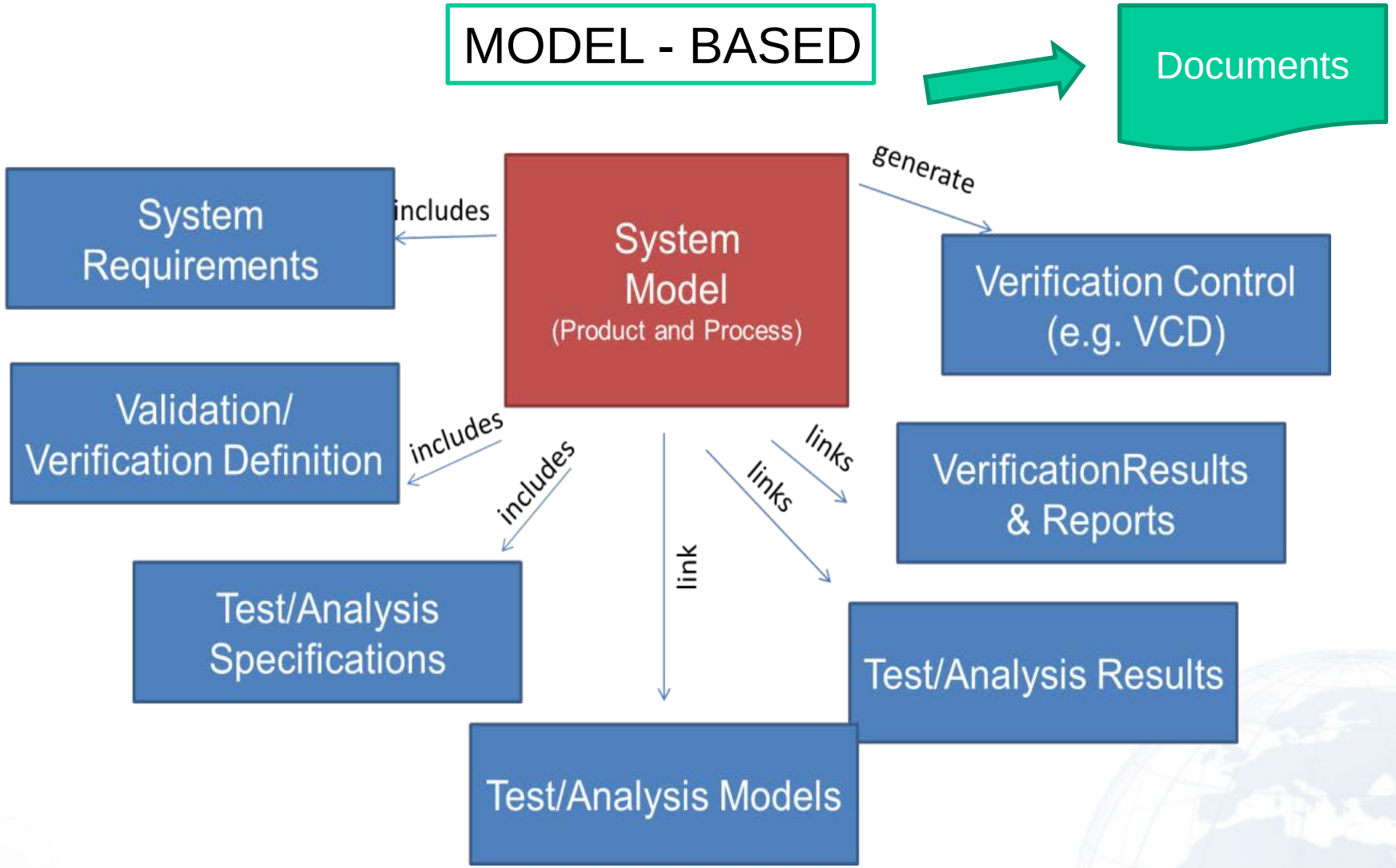


Verification Definition and Management supported by Modeling

DOCUMENT - BASED

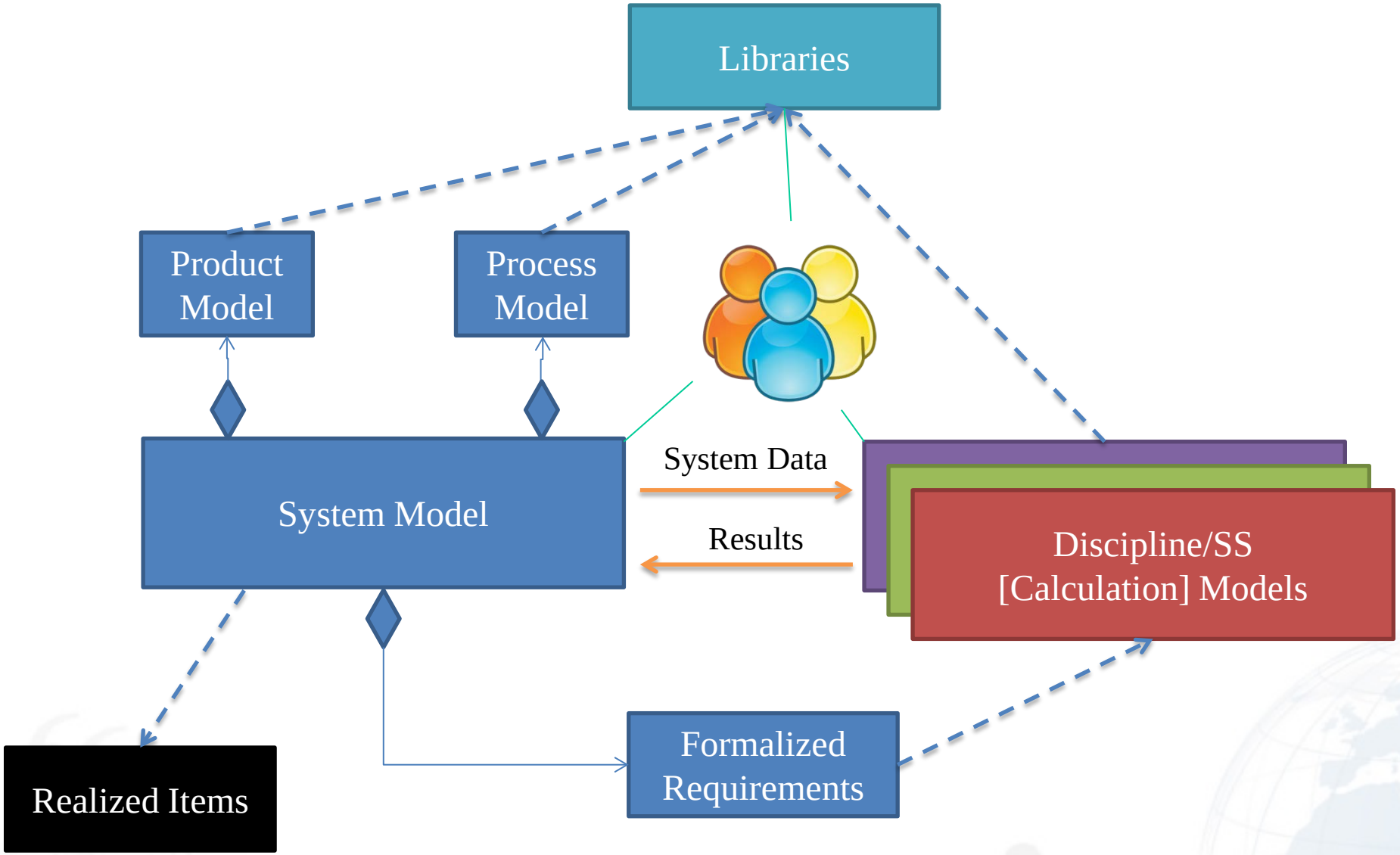


Verification Definition and Management supported by Modeling



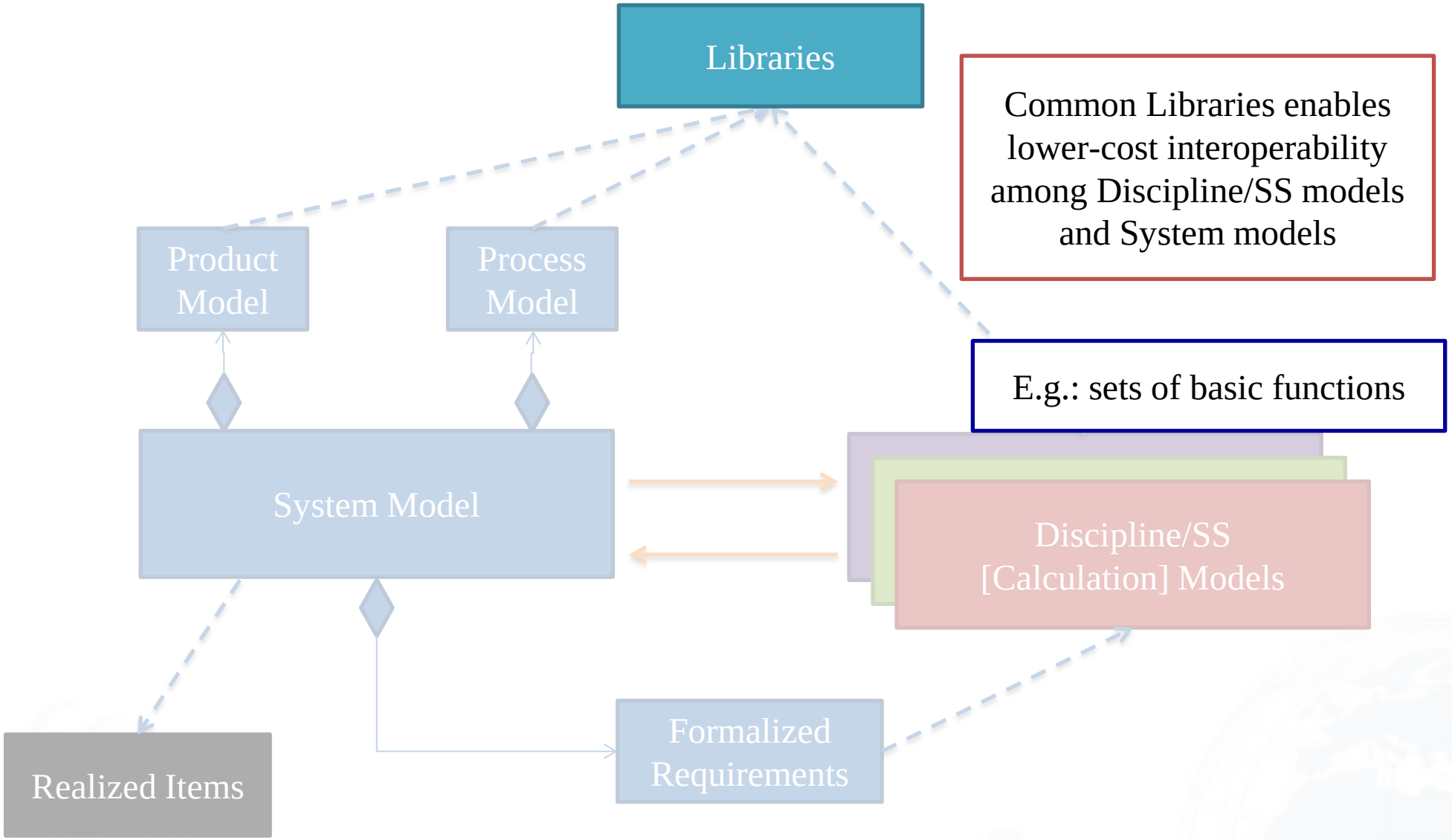
OPEN

Proposed methodology



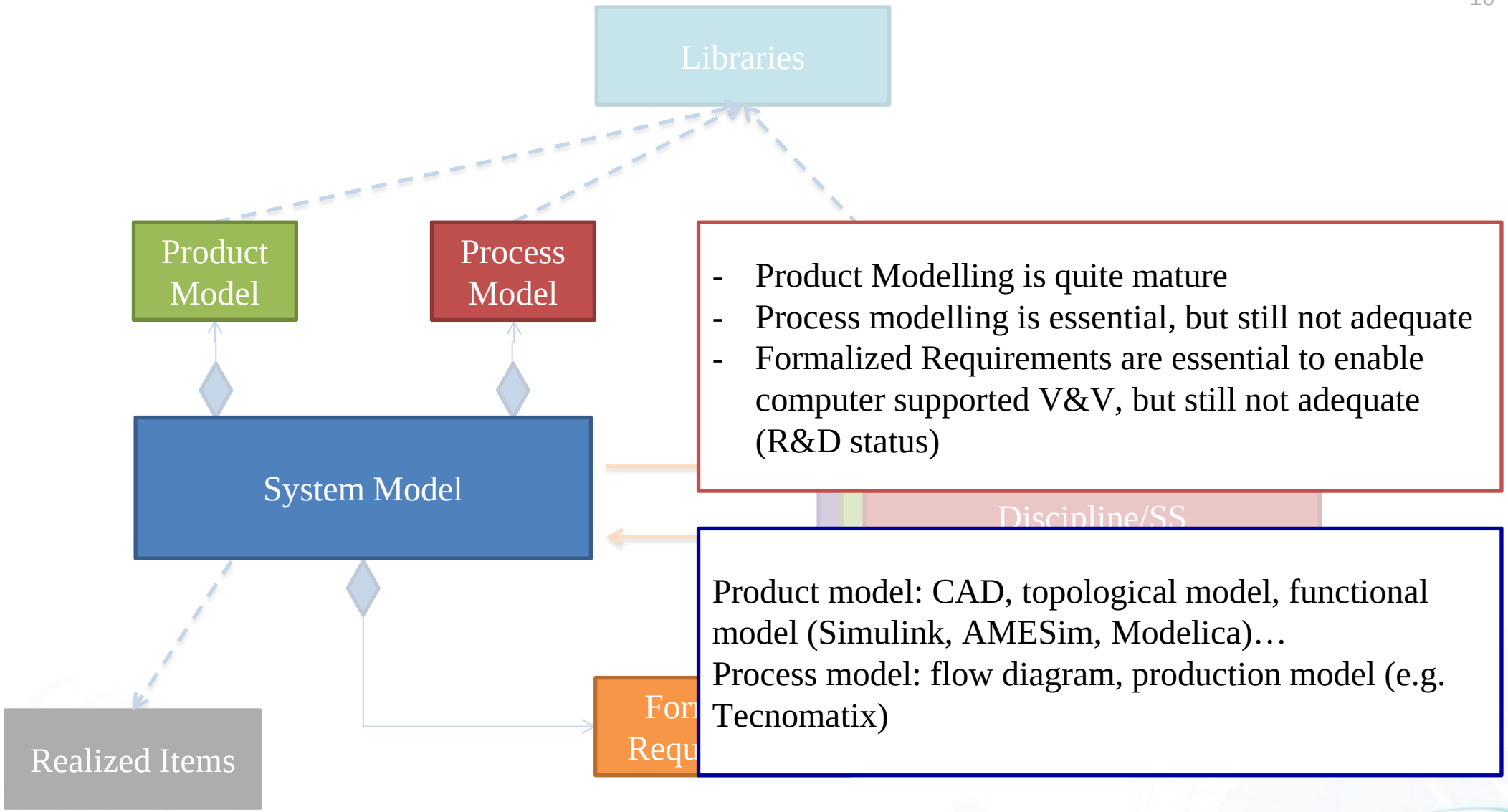
OPEN

Proposed methodology

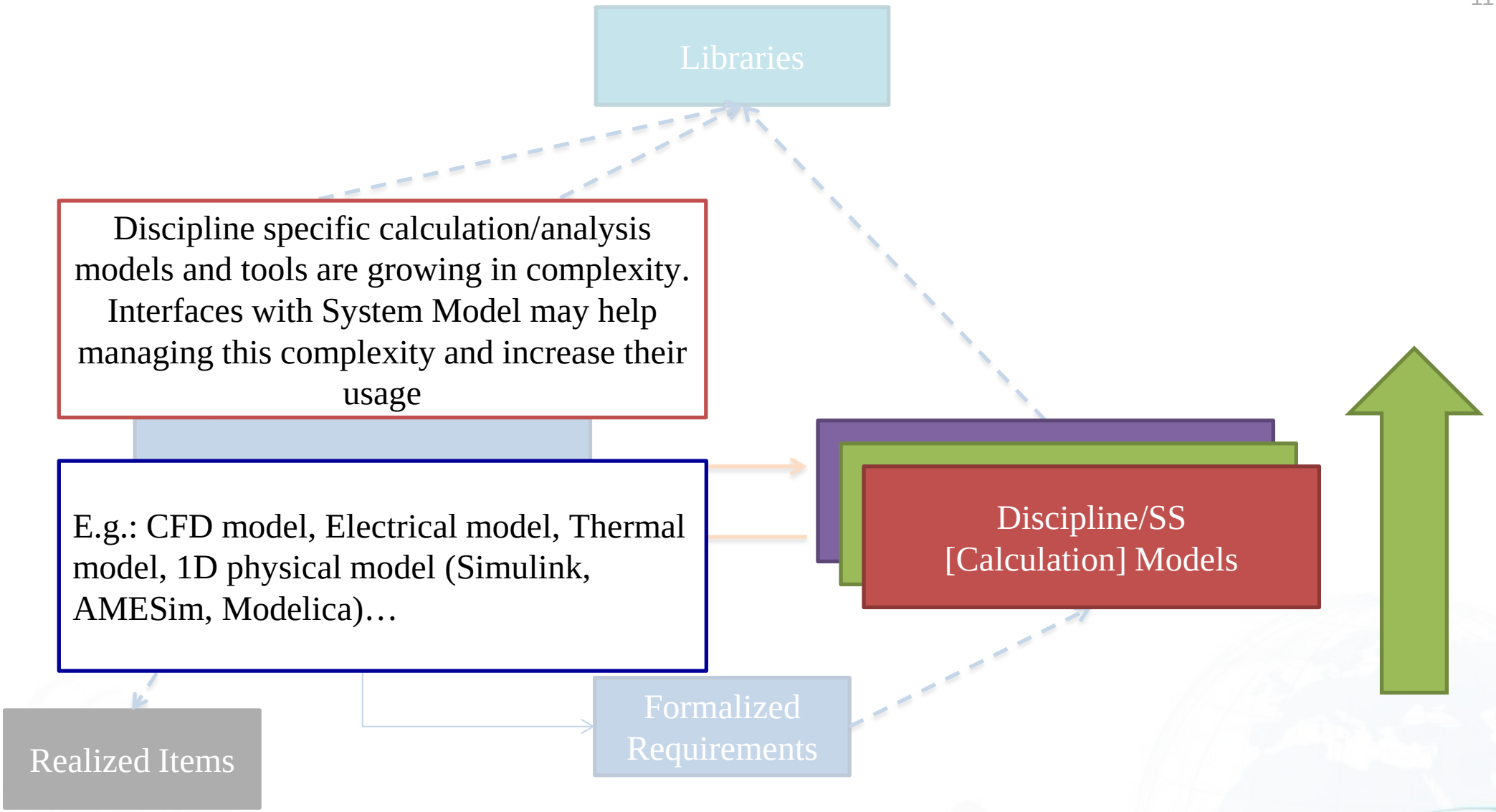


OPEN

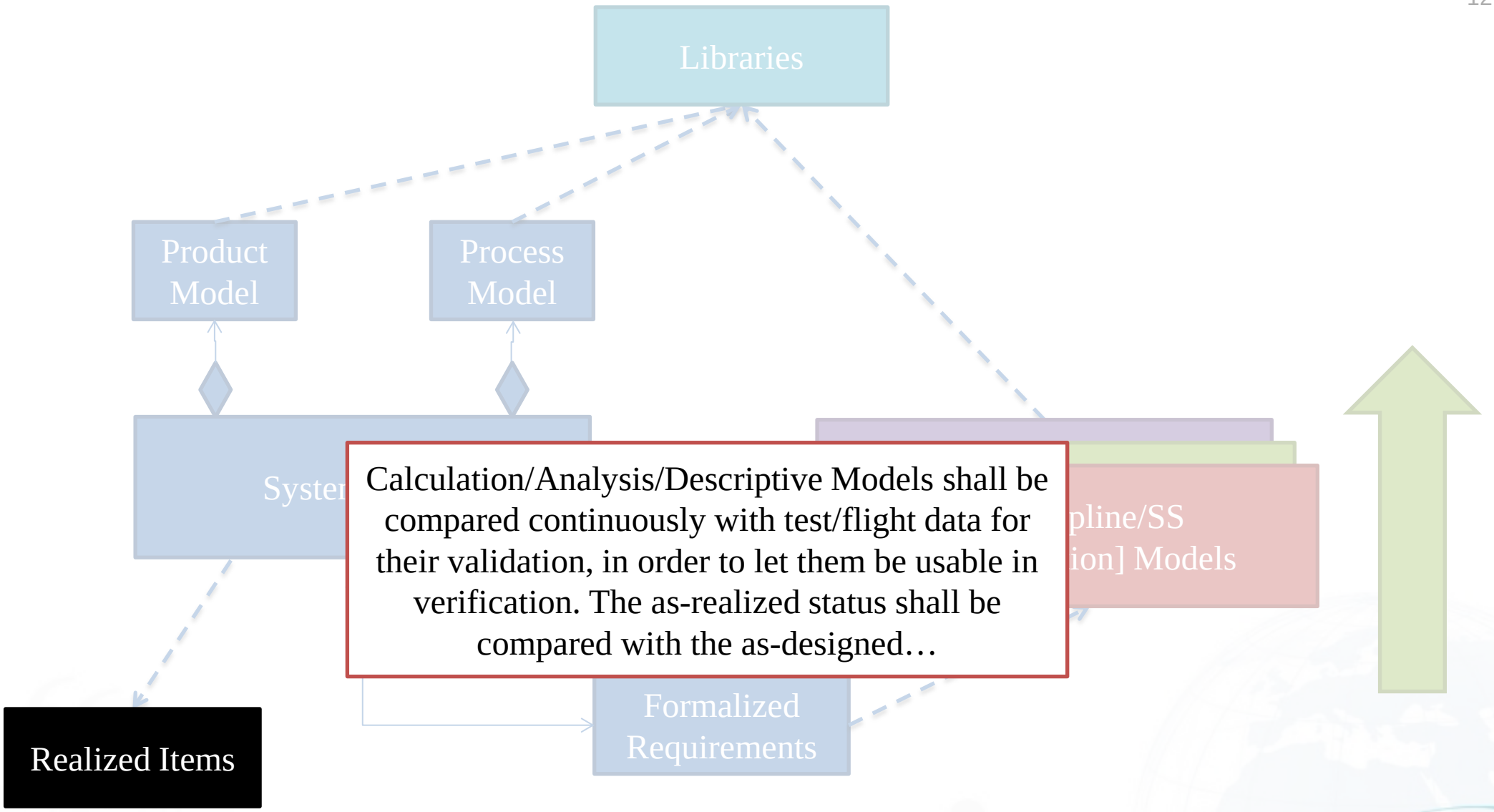
Proposed methodology



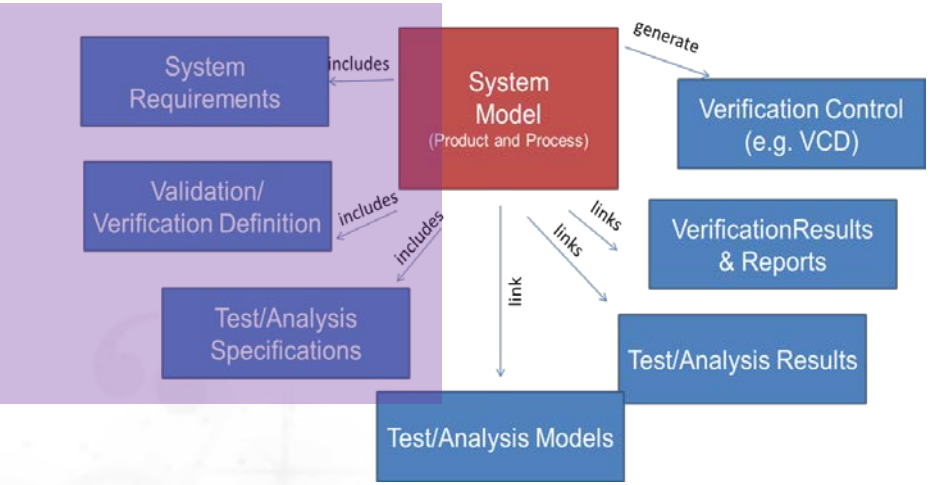
Proposed methodology

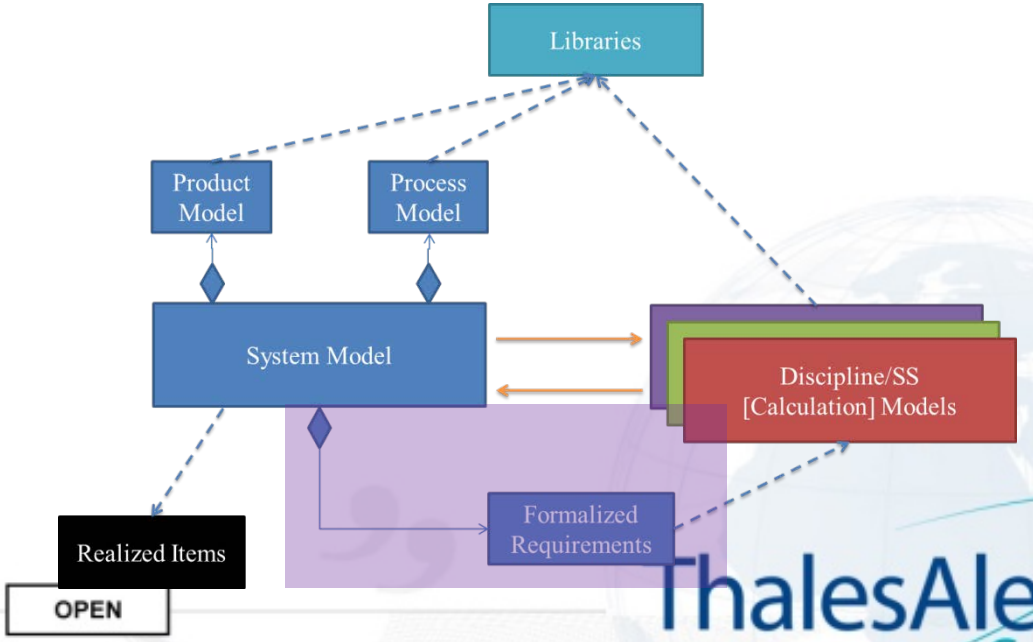


Proposed methodology



Requirements





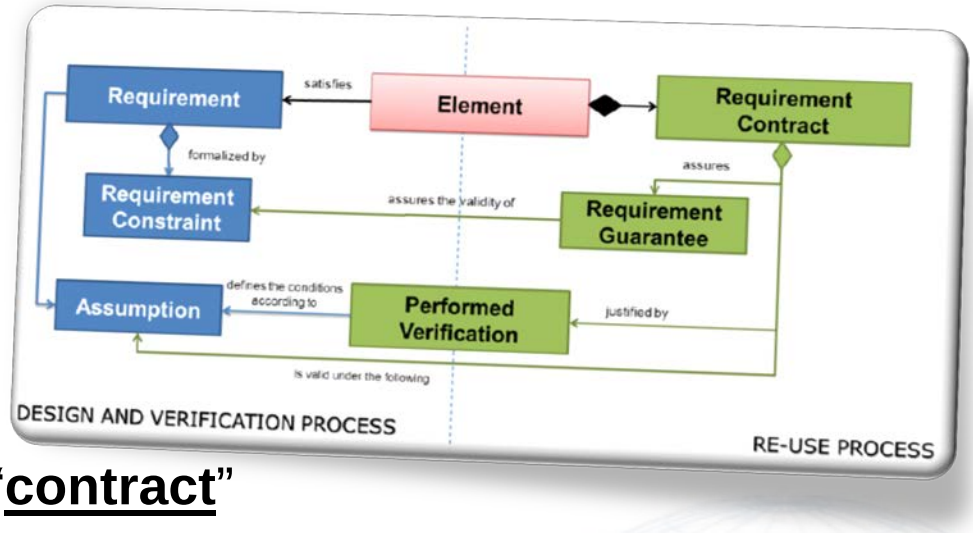
Verification and the Importance of Requirements

- Requirements as a Model
- Formal Constraints may help:
  - Automatic check of:
    - Design (Review of Design)
    - Simulation/Analysis Results (Analysis)
    - Test Results (Test)
  - Definition of:
    - Test/Analysis levels
    - Success criteria
- Conceptual models help the definition of a wide set of constraints
  - On acceptable ranges and imposed values
  - On presence, absence or a number of specific items
    - On architecture, functions, verification, design, etc.

Verification and the Importance of Requirements

- Not only constraints
  - **Assumptions**:
    - Establish what is the validity of the constraint
    - Determine which are the conditions of the associated tests or analysis

- Once the verification is successfully performed, the verified constraints, according to specific assumptions, are considered as **Guarantees**

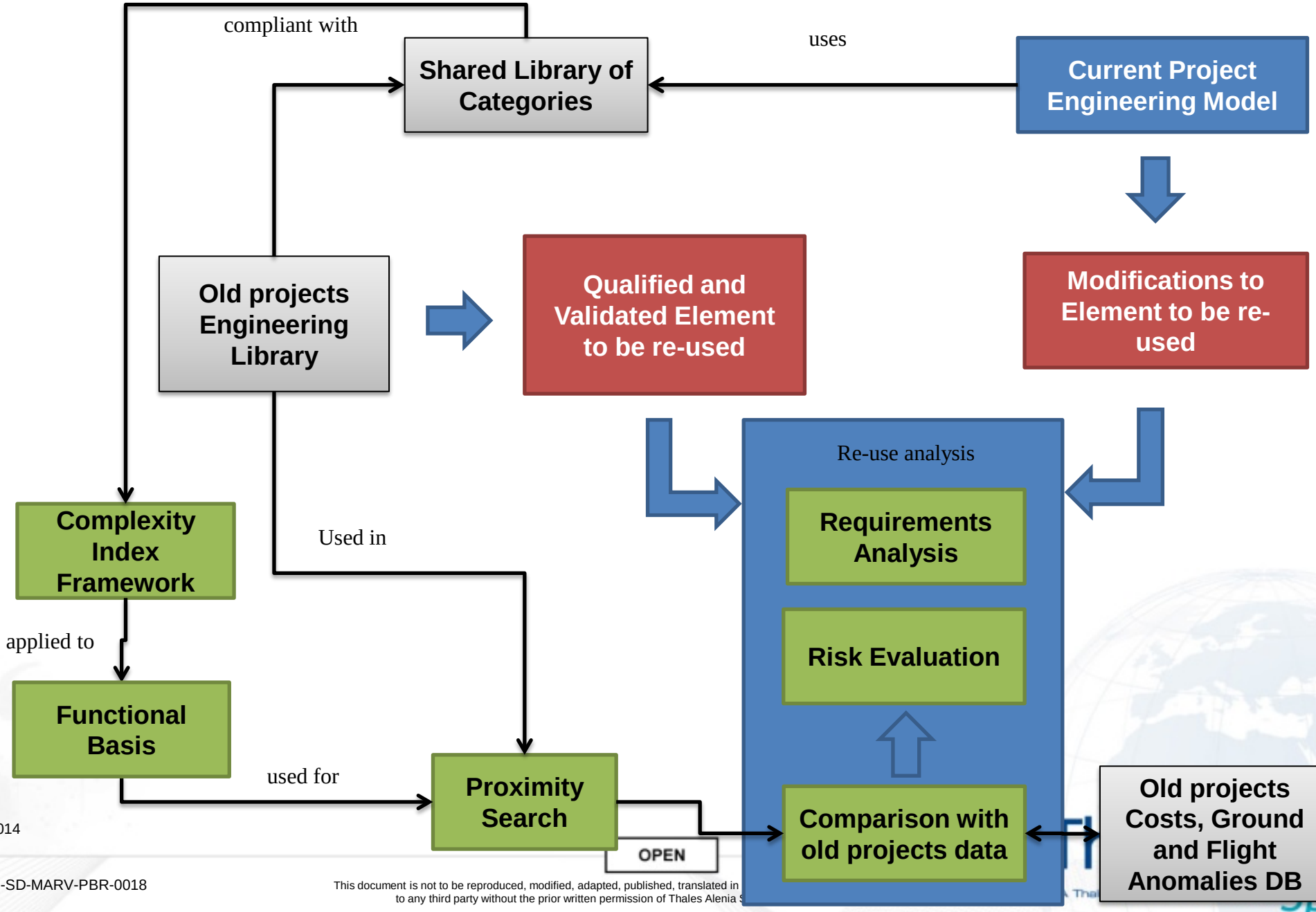


→ the qualified or accepted element has a "**contract**"

- Contract = collection of the guarantees and related assumptions

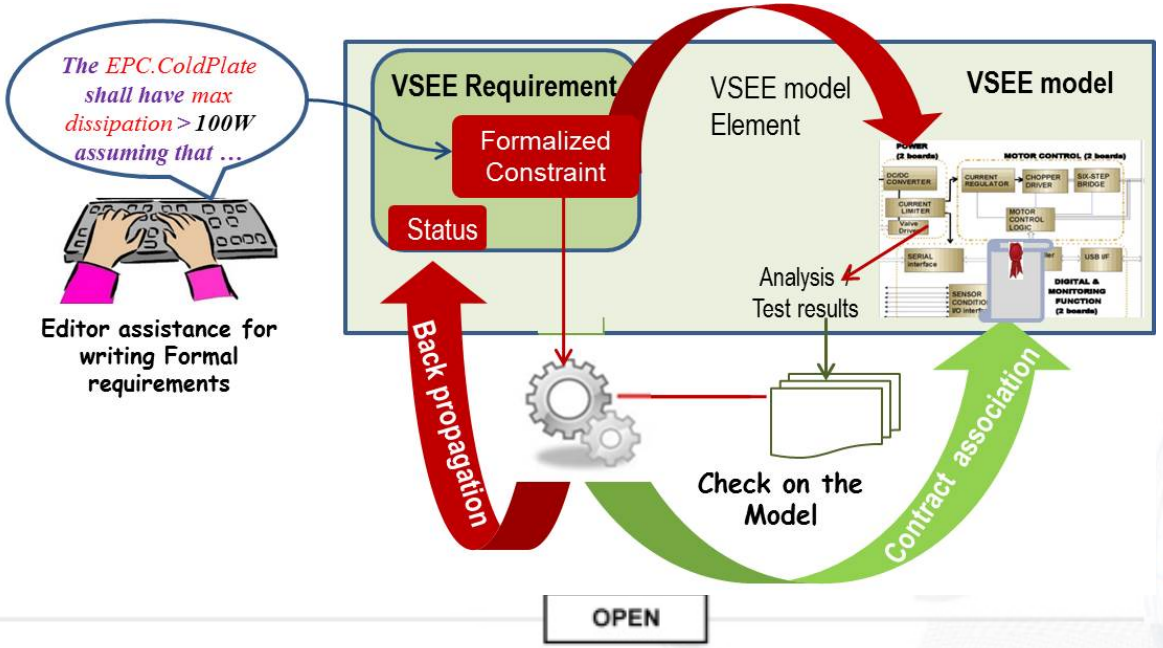
- This is a key part of the re-use process. Such contracts are essential parts of the object libraries of previous projects, to be introduced or easily re-analyzed in the new projects, since initial phases.

Re-use: proposed methodology (excerpt)

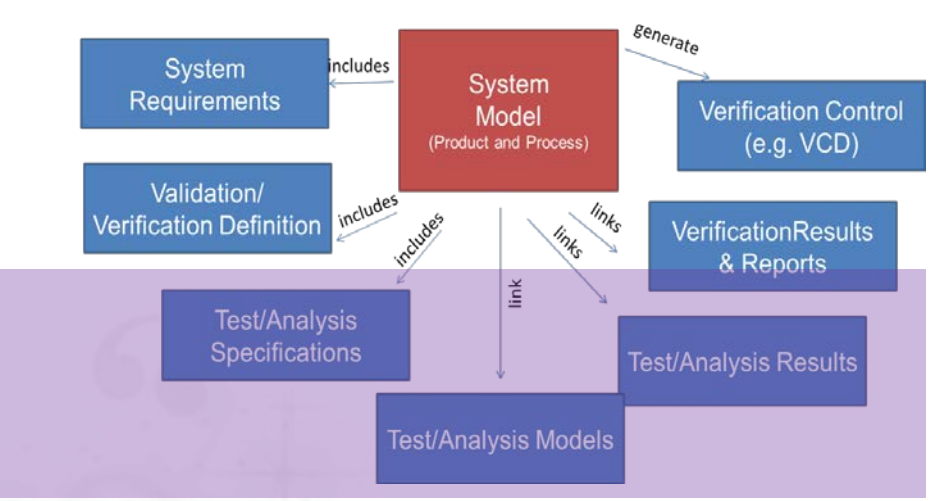


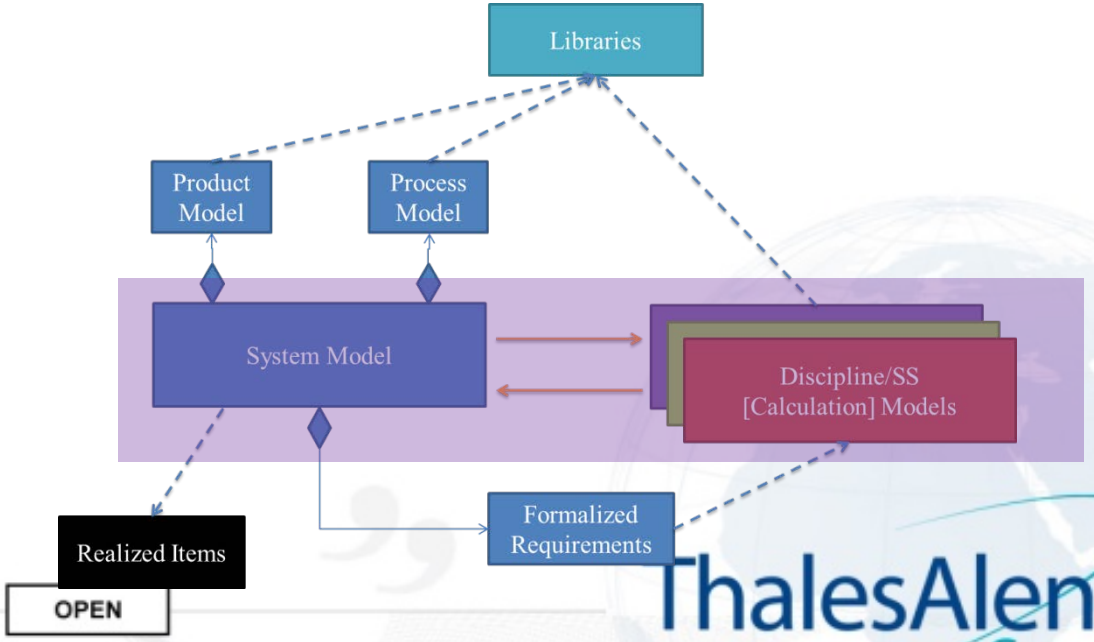
Verification and the Importance of Requirements - Prototype

- MARVELS toolset
  - *Based on VSEE model*
  - *Formalization of requirements – editor assistance for writing*
    - *Value constraint requirements*
    - *Architectural requirements*
    - *Structural requirements: agnostic w.r.t. Metamodel*
  - *Automatic generation/association of contracts upon successful check of formal requirements satisfaction*



T, A, RoD, I





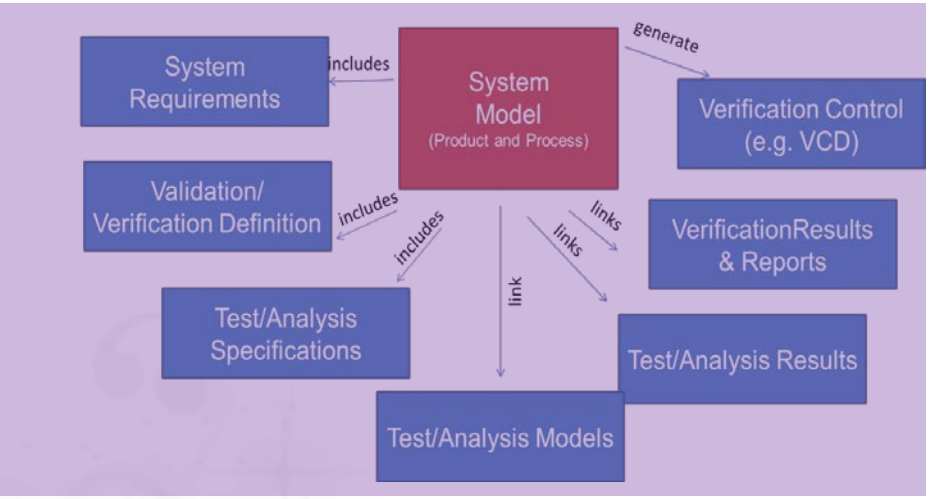
Verification activities supported by Modeling Analysis (incl. Simulation)

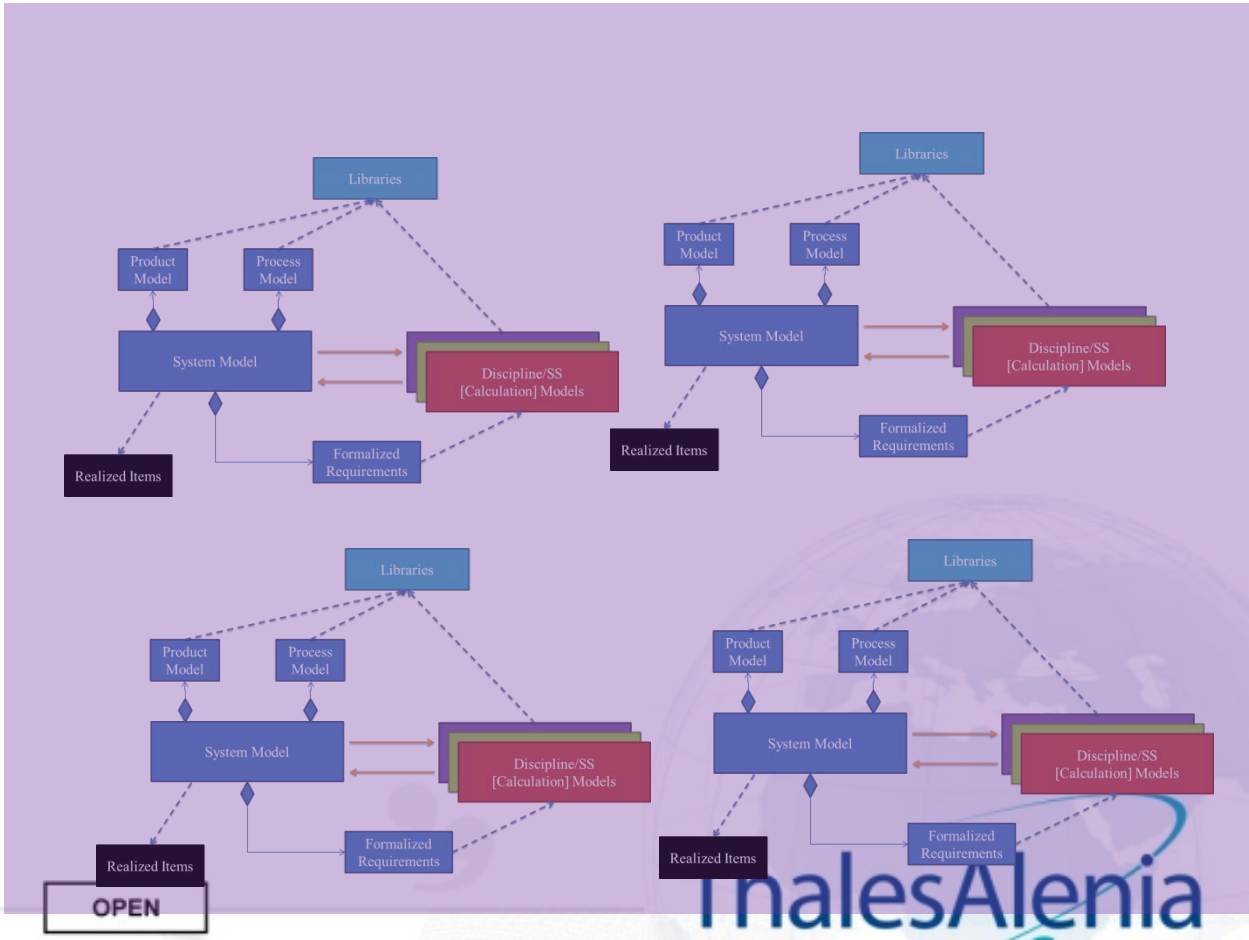
- Model transformation? It depends..
  - **Subscription**
    - the analyst requests and subscribes to the items that impact on his/her model, and is notified each time there is a change
  - **Formatted input**
    - the analyst prepares an input file (e.g. a text file, a MS Excel workbook, a Matlab file) in the format that can be used to configure his/her parameterized model
  - **Model-to-model**
    - the analyst writes some code that is able to generate a discipline specific model, according to specific data items (e.g. belonging to particular categories or with specific properties)
- Analysis results may be checked at discipline level by the calculation model and/or checked at system level in the MBSE platform
  - If the requirements are properly and formally expressed
  - If the user has proper means to track and analyze requirements w.r.t. model items

Verification activities supported by Modeling
Review of Design, Inspection, Test

- Inspection
  - Planning, definition, link to requirements and model items, tracking of technical results
- Review of Design
  - Substantially supported by model checking, automated and/or assisted
- Test
  - Preparation of test specifications and procedures
    - individuation of critical conditions w.r.t. requirements
    - evaluation of representativeness of tests w.r.t. real conditions
  - Identification of hardware/software needed (since early phases)
  - Easier evolution of simulations/analysis models from early stages to latter stages (to EGSE or functional simulator)
  - Post processing and correlation with analysis/simulation results

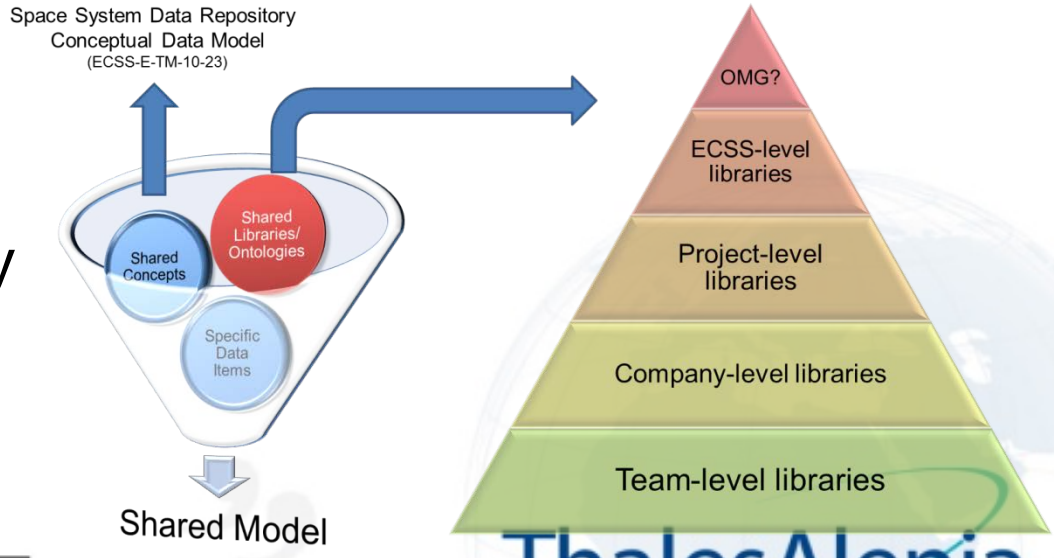
Ver. Management and Teamwork





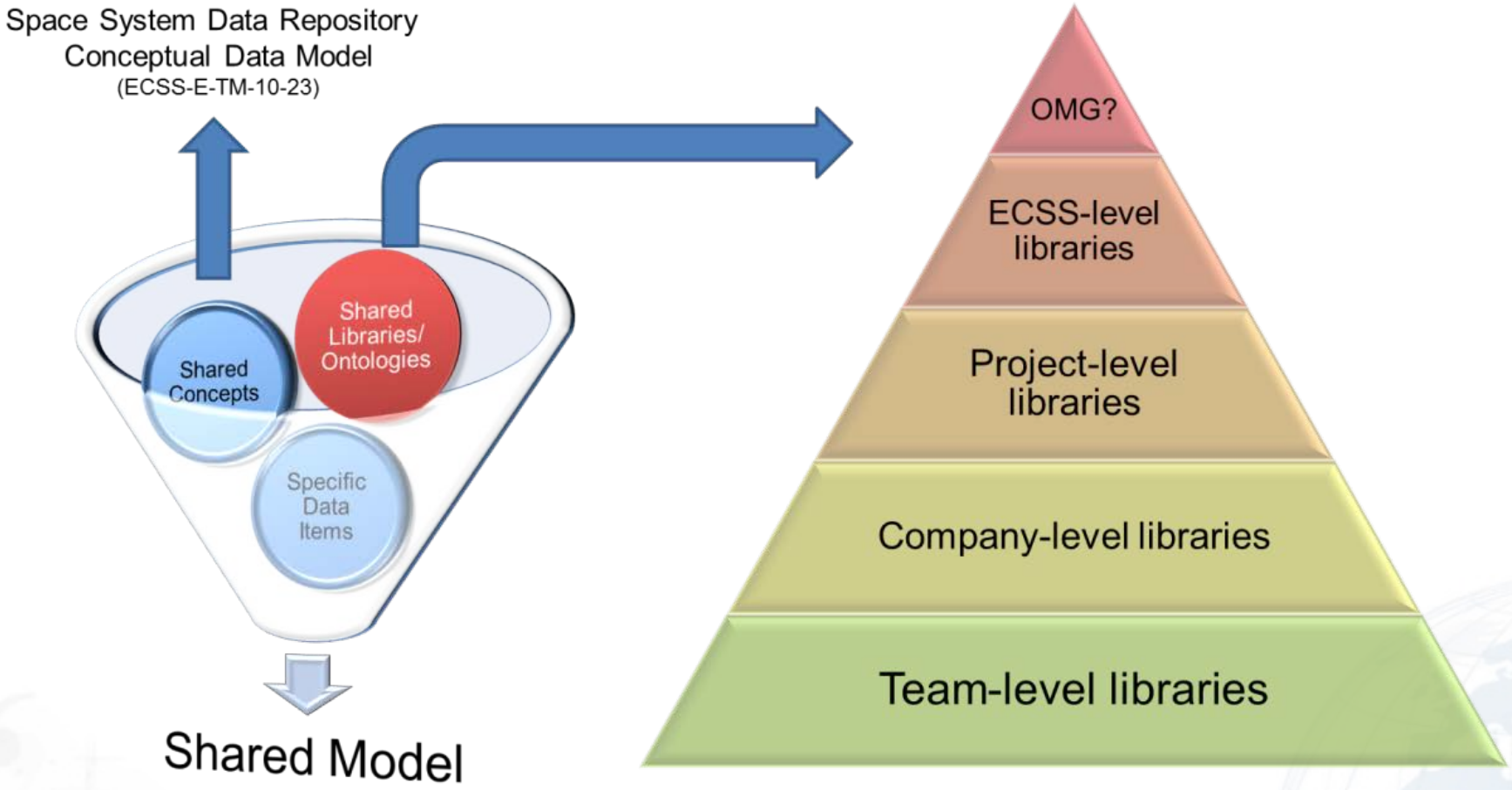
Expected Impacts on Project Activities

- Technical System? Socio-technical system!
  - People are fundamental part of the process, in all the project phases
  - Design, Verification, Operations, but also intra- and extra-company Collaboration, Reviews, Investigations
- Document-based means “I know what I am sharing”
- Model-based should mean “I am sure of what I am sharing”
  - Shared objects libraries
  - Shared concepts
  - Project items filtered sharing
- Sharing should not limit flexibility and creativity
  - Different levels



OPEN

From a model perspective



Impact on Review Process

- Reduction of RIDs
  - Customer-Supplier strengthened co-engineering should reduce RIDs and identify key issues
  - Other key issues are identified by a third party team (review team)
- Co-engineering
  - Customer-Supplier as a team (as expressed by IAW participants)
- RIDs are identified directly on the model
  - In early phases this shall improve the quality of the model
- The data-package is generated for records once the RIDs are solved, and for the review authority, not for the whole review process
  - Reduced time for documentation generation
- The intervention of the review team can be associated not only with a review stage, but during the phases, once the items are stabilized
  - Third party assessments can be easily requested by customer or supplier on specific tasks, because they do not require documentation

Demonstration

Use MARVELS tool for requirements formalization

Use VSEE to define system and verification activities

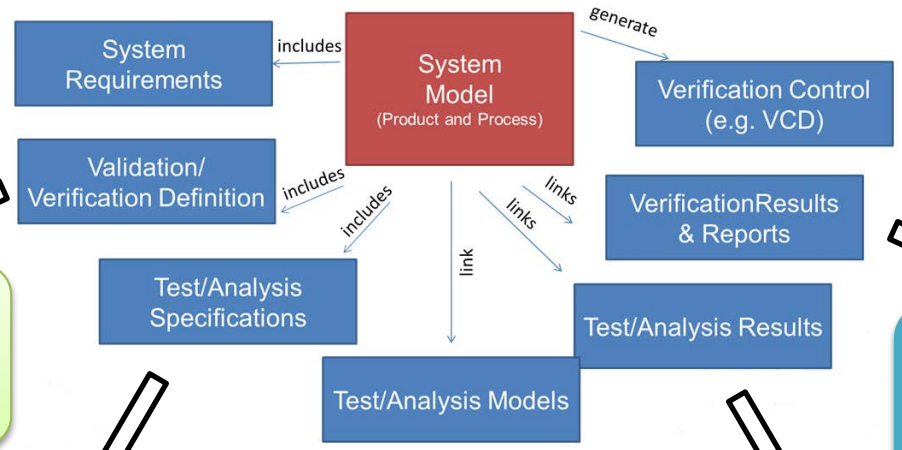
Use VSEE to define analysis and test activities and models

Configure dummy calculation models with VSEE data

Connect results to VSEE

Check results with MARVELS tool

Generate VCD Dashboard (TAS WE)



VSEE – use as is

New development

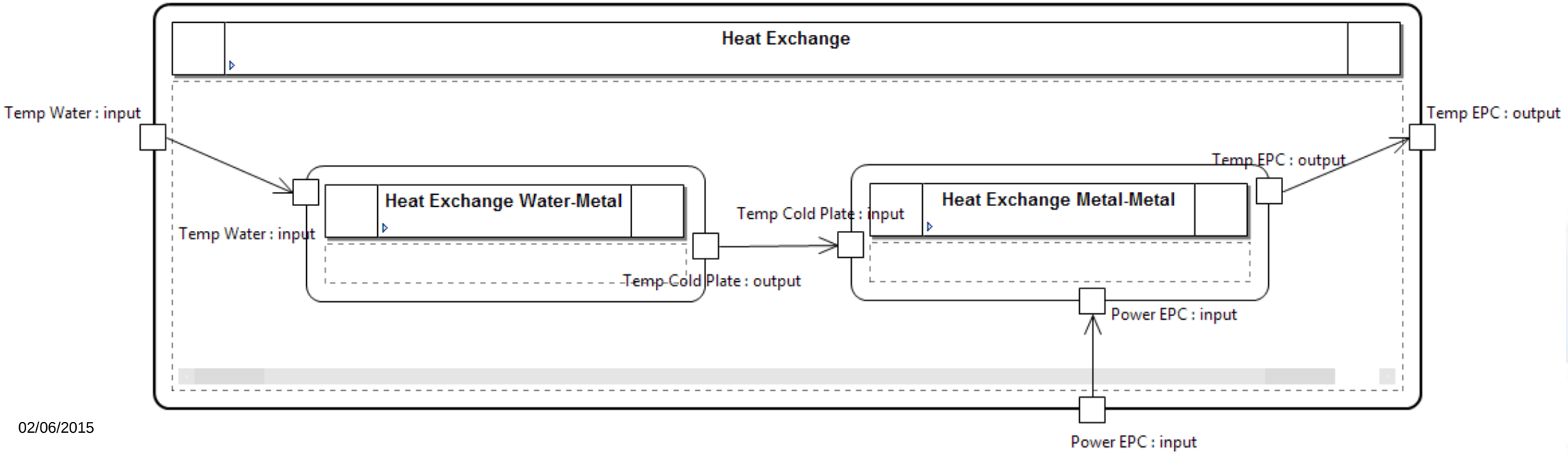
MARVELS tool

Defined separately

A small project (**Water Pump** of **Columbus** module of the **ISS**) has been modelled with the MBSE methodology and a demonstration for verification purposes has been achieved

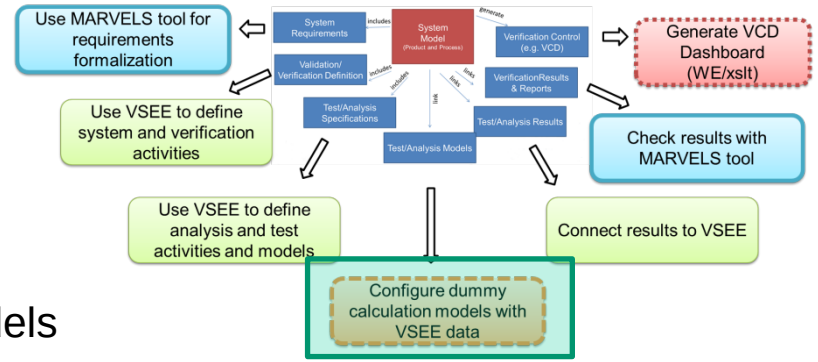
VSEE Topological/Functional models

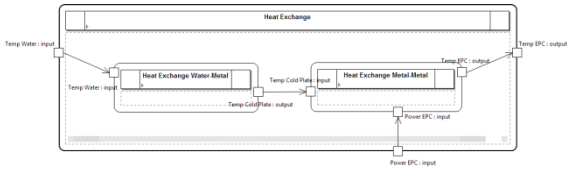
- SSDE is used to define the different objects
  - Relevant parameters
  - Discipline model
  - Categories (in this case, a category for materials is used, assigning properties relevant to heat exchange)
- SSDE is used to build a functional diagram for the Heat Exchange
  - It links each object (separately defined) with its respective functions
  - Thermal interfaces are created and linked to joint objects

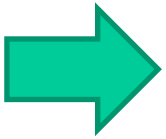


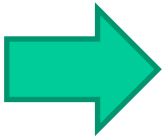
Demonstration scenario: discipline model generation

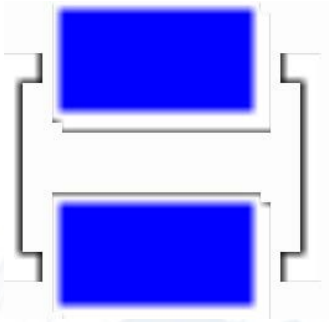
- A Python script is used to:
  - Read the content of the topological model (from SSDE) and save it into separate arrays:
    - Elements (ID, Modelica model, material)
    - Interfaces (ID, name in Modelica, name in SSDE)
    - Materials (ID, properties)
  - Build the Modelica system-level model:
    - Assemble element-level models
    - Insert material properties inside element-level models
    - Build system-level script with the assignment of interfaces



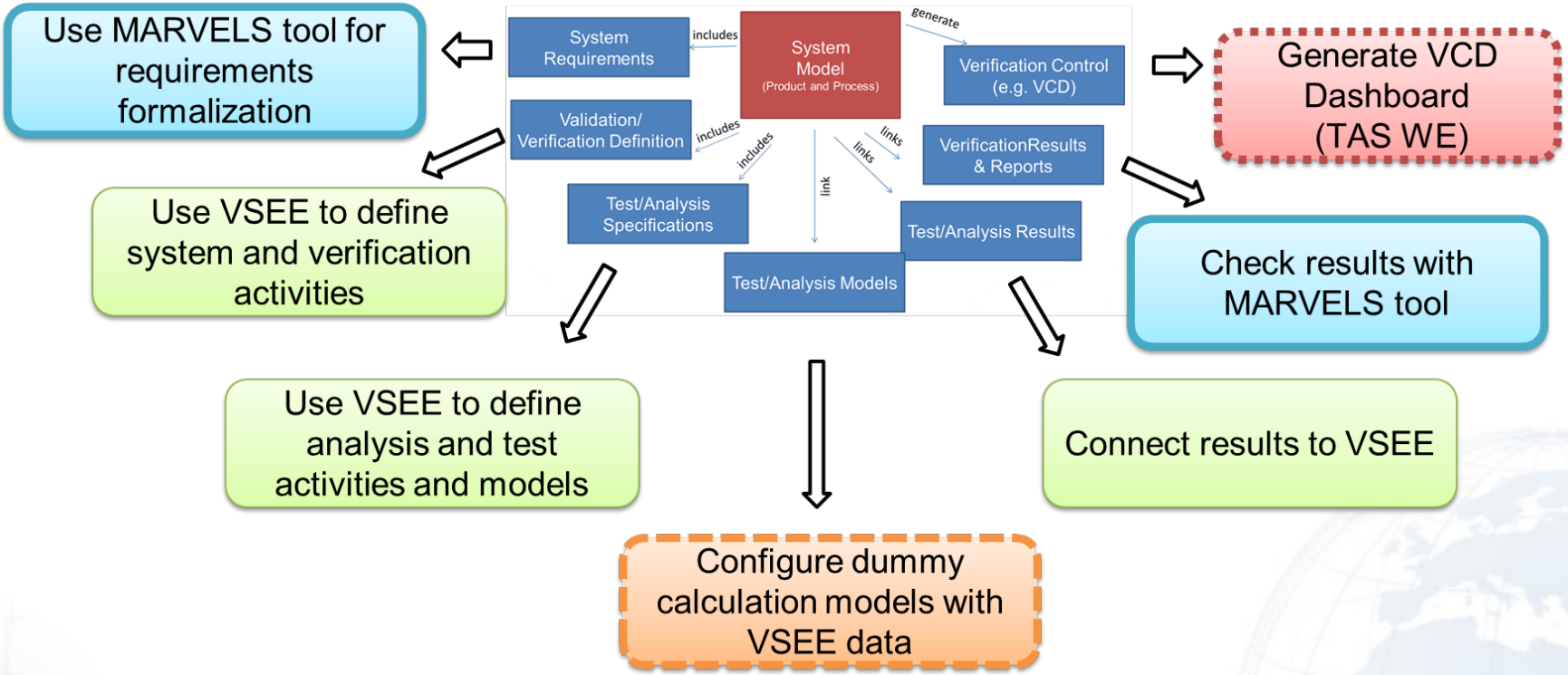








MARVELS Video



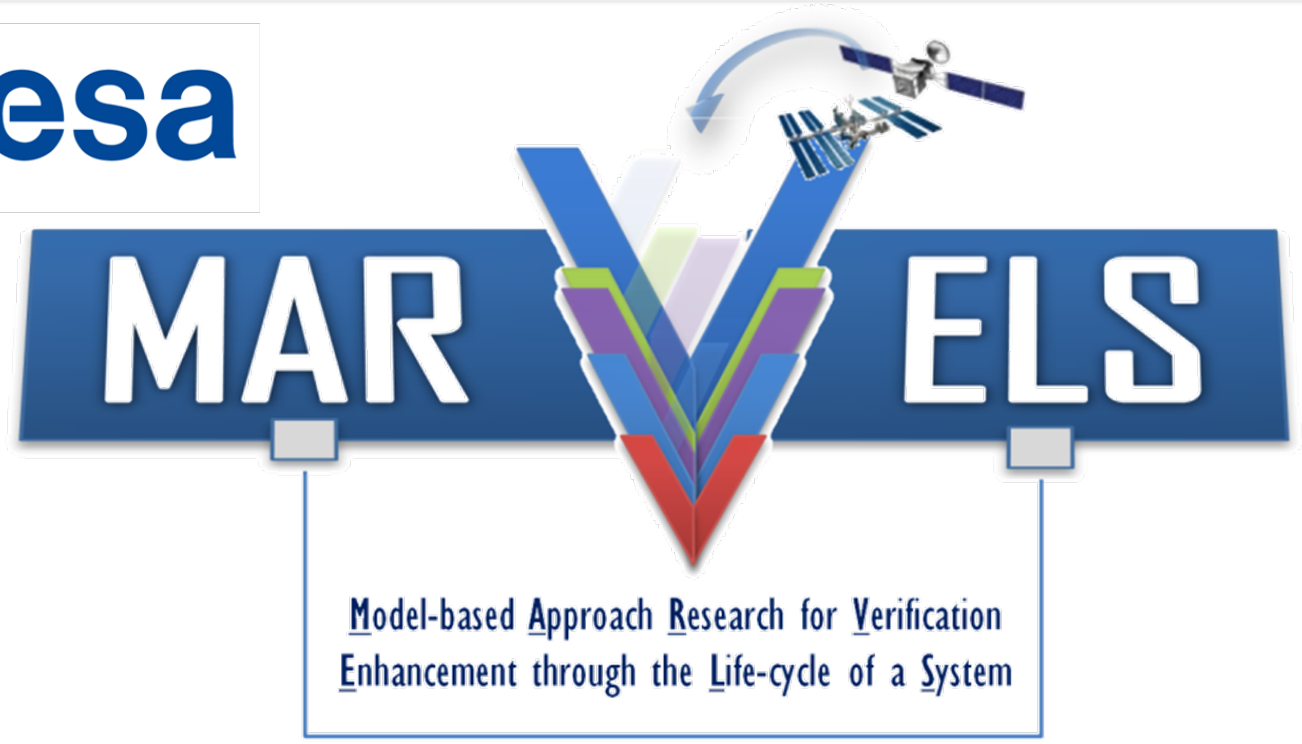
OPEN

Conclusions and future developments

- The capability to apply the MBSE to verification has been conceived, detailed and demonstrated
  - The demonstration was able to walk through the lifecycle in a simplified case and, without loss of generality, it helped to preliminary validate a set of concepts on the data structure, methodology and requirements for operational tools
  - The VSEE data model has been commented, and extensions/changes have been proposed to exploit as much as possibile the model-based approach in terms of SE management, support to T, A, RoD, I and for collaboration
  - TAS, INTECS, Polito and VTT heterogenous background and experience have been merged, providing near-term and long-term solutions

- Broader application is needed to
  - Validate the approach w.r.t. an entire project, siding and supporting the traditional document-based approach (requires the adoption by a team)
  - Highlight issues that may emerge, so to refine the methodology
  - Involve people and make them used to the new approach
    - Physiological resistance to innovations to be overcome by easy-to- (and funny-to-) use tools, web-based and with support of 2D/3D graphics

Thanks for your attention!



Questions?

mauro.pasquinelli@thalesaleniaspace.com