The FoReVer MBSE Solution for System Composition Correctness Analysis

Silvia Mazzini, Intecs

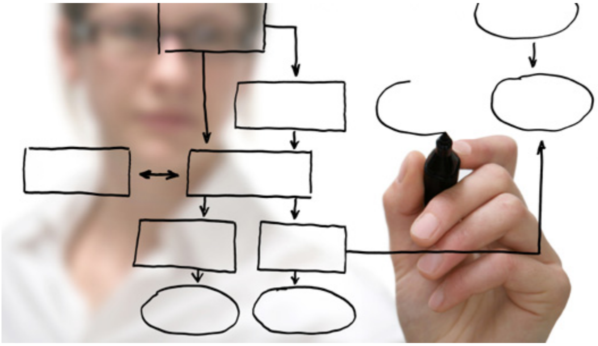
COMPASS Workshop, 22 October 2015

The FoReVer Project

- Functional Requirements and Verification Techniques for the Software Reference Architecture (FoReVer) is an ESA/ESTEC project
  - Consortium led by Intecs
  - Partners
    - Thales Alenia Space (Cannes)
    - Fondazione Bruno Kessler (Trento)
  - Running in the period January 2012 – May 2013

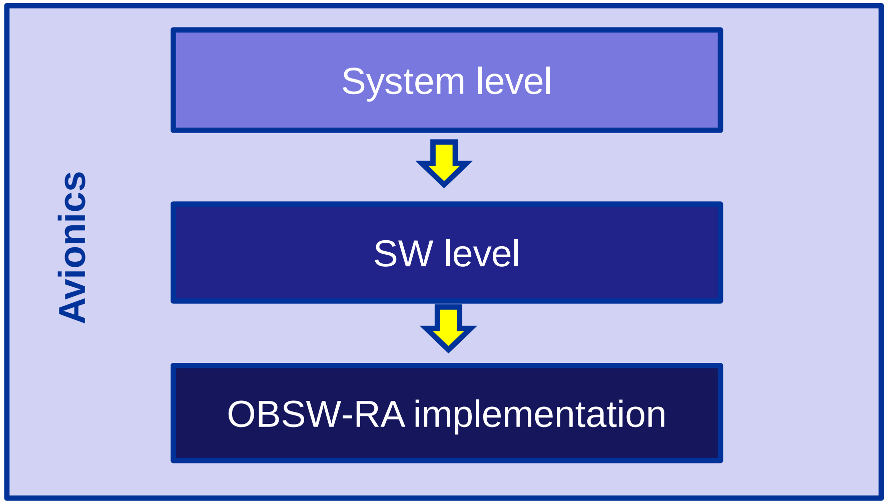
The FoReVer Formal Methodological Framework

- Model Based System Engineering (MBSE) Methodology and Technology to support system avionic development across phases 0, A, B, and C
- Early apply Formal Verification techniques in the context of MBSE for
  - Specification of requirements
    - Formal properties
  - Formal reasoning
    - Formal verification of properties
    - Step wise refinement from System down to SW

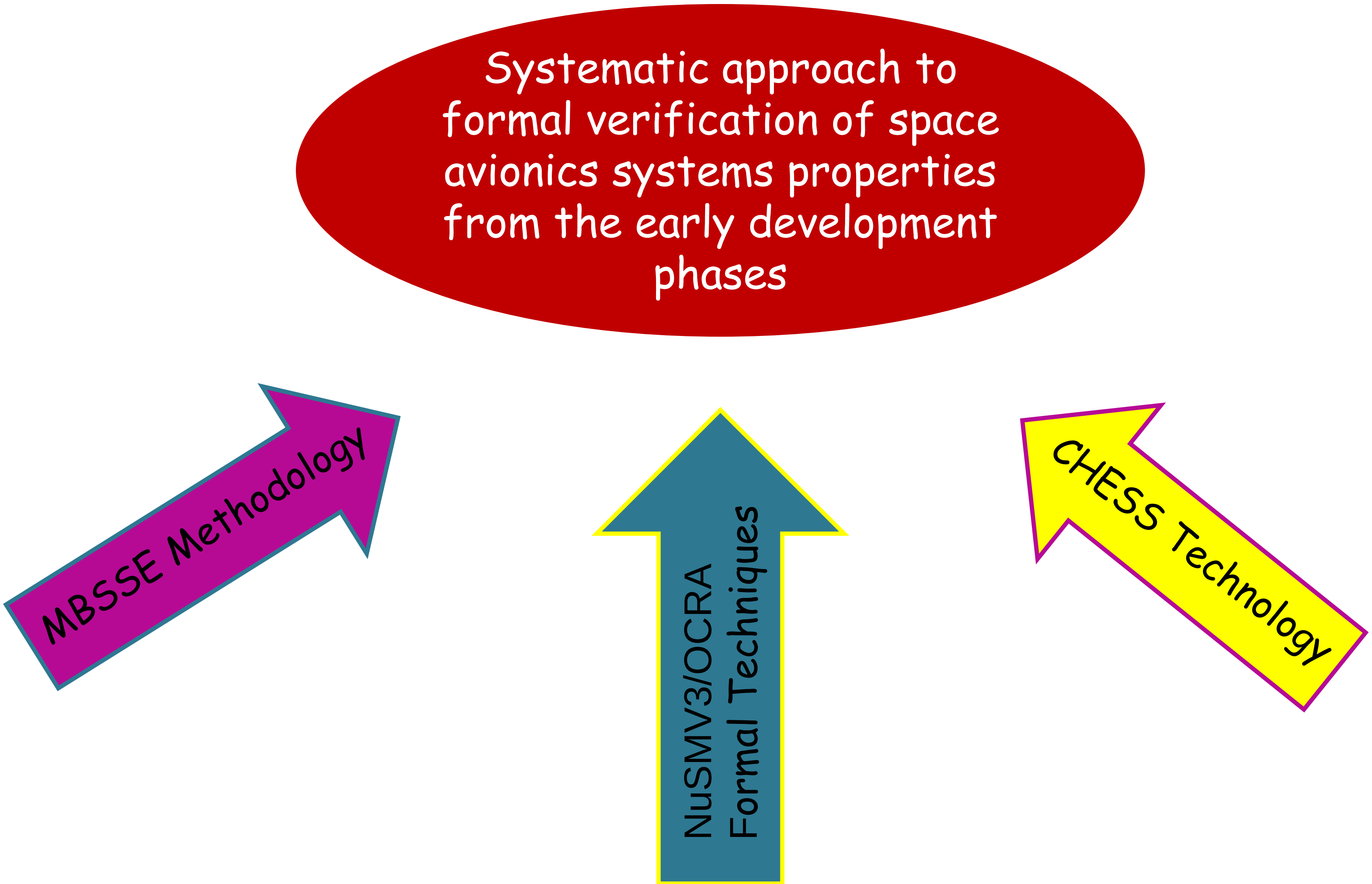


Software Reference Architecture

- Exploit the Software Reference Architecture (SRA) concepts from the context of the SAVOIR-FAIRE ESA initiative (COrDeT-2)
  - Refinement of avionics System level properties down to SW level and then to SW implementation on top of the on-board software reference architecture (OBSW-RA)



FoReVer Ingredients



MBSSE

- **M**odel-**B**ased methodology to support the **S**pace **S**ystem **E**ngineering (from SSFRT)
  - based on SysML: graphical, model based support for system modeling of requirements, functional decomposition, behavior, architecture, step-wise refinement and traceability

FoReVer

  - property formalization, formal verification, step-wise refinement with assume-guarantee reasoning for modeling the avionics at system and software level

NuSMV3/OCRA

- **NuSMV3** provides formal techniques for:
  - modeling of the avionics for system and software co-engineering and
  - property verification

- **OCRA** package provides methodological framework for:
  - stepwise refinement verification
  - assume-guarantee reasoning
  - traceability

FoReVer

- formal means for verification, step-wise refinement with assume-guarantee reasoning applied to MBSE

CHESS

- Model-driven Component Based methodology for high integrity software development from the ARTEMIS CHESS/CONCERTO projects
  - modeling of requirements, traceability and properties
  - formal verification techniques for **non-functional properties** of software (real-time and dependabiltity)
  - correctness-by-construction (by automated code generation)
  - SRA component model

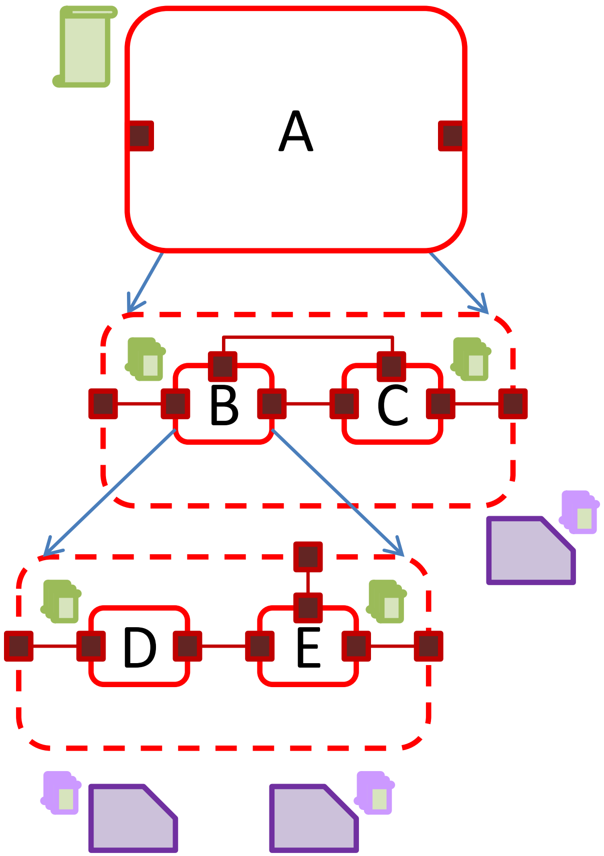
FoReVer

  - system level support
  - system and software co-engineering support
  - stepwise refinement with integration of formal verification means

The FoReVer Approach

- Component-based
  - The system is described in terms of architectural components with their **well-defined interfaces and related properties**
  - Components are refined into lower levels as black boxes until they are refined
- Contract-based
  - Formalize properties of system and components in terms of **component contracts**
  - Formal verification of **contract refinement**

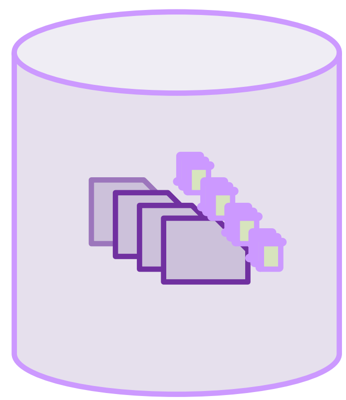
Contract Based Approach
Compositional Verification



Component's Contract

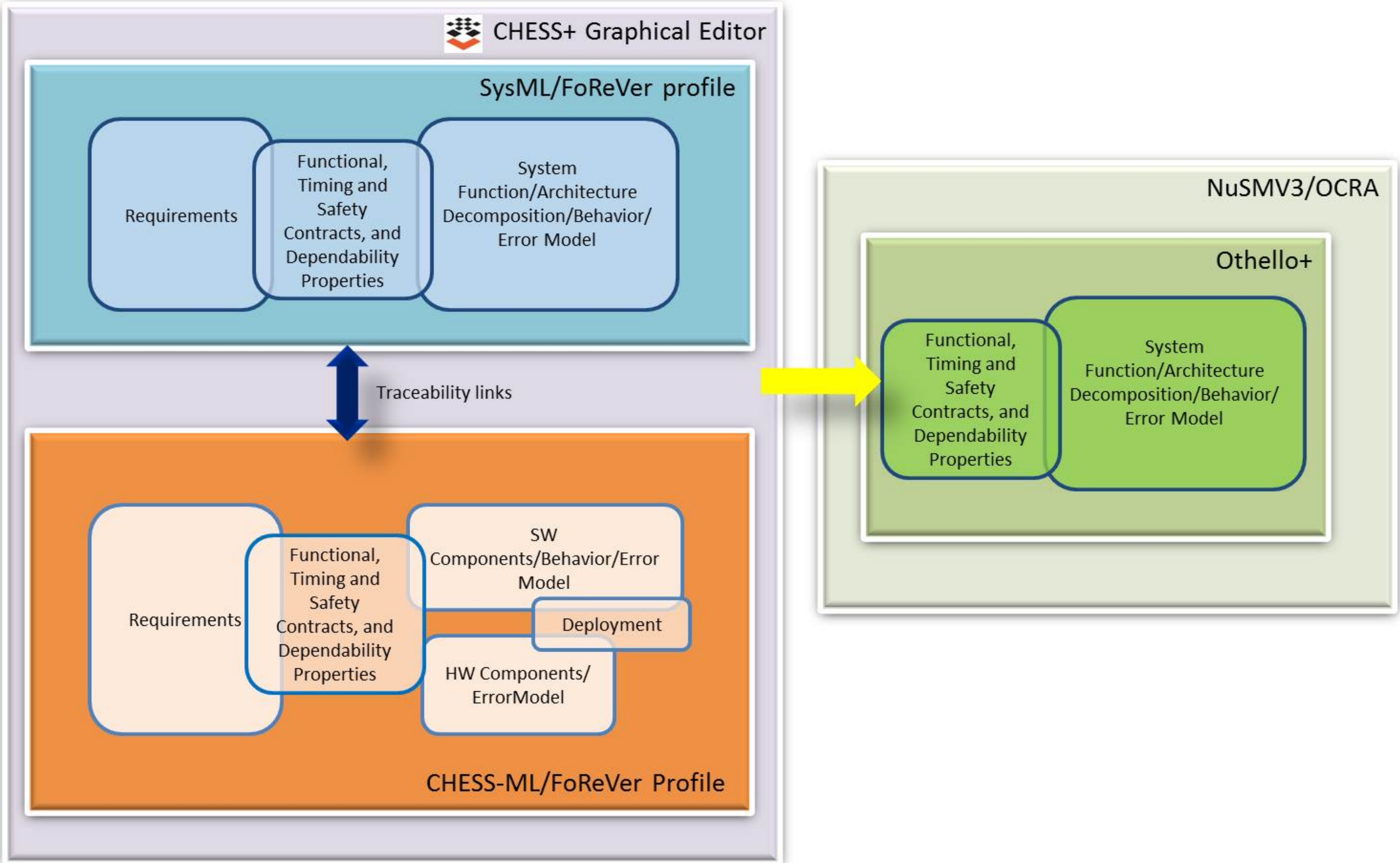
Contract Refinement

Library of Components with Contracts

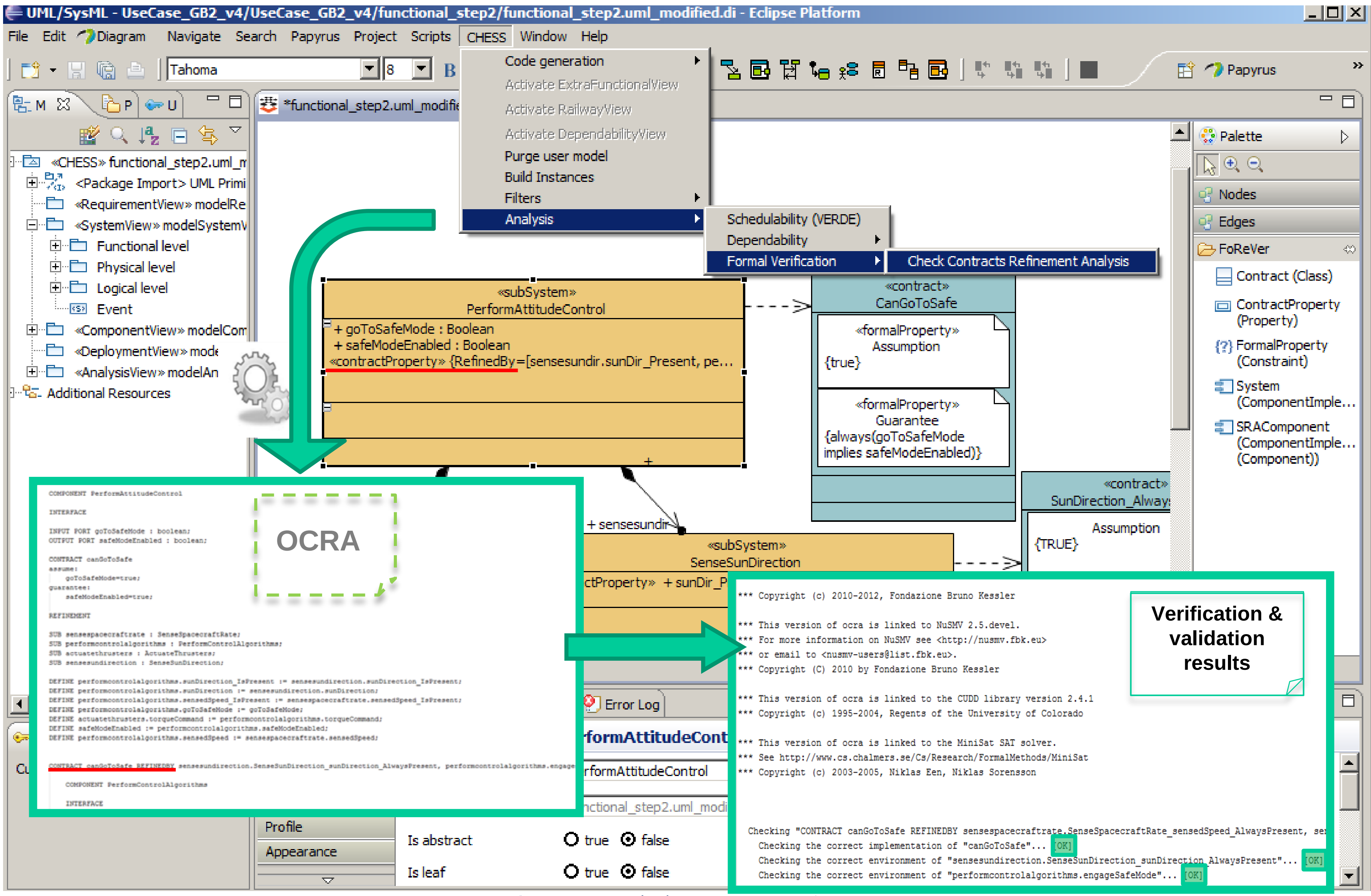


If the refinement steps are proven correct, then any implementation of the leaf components that satisfies the component contracts can be used to implement the system.

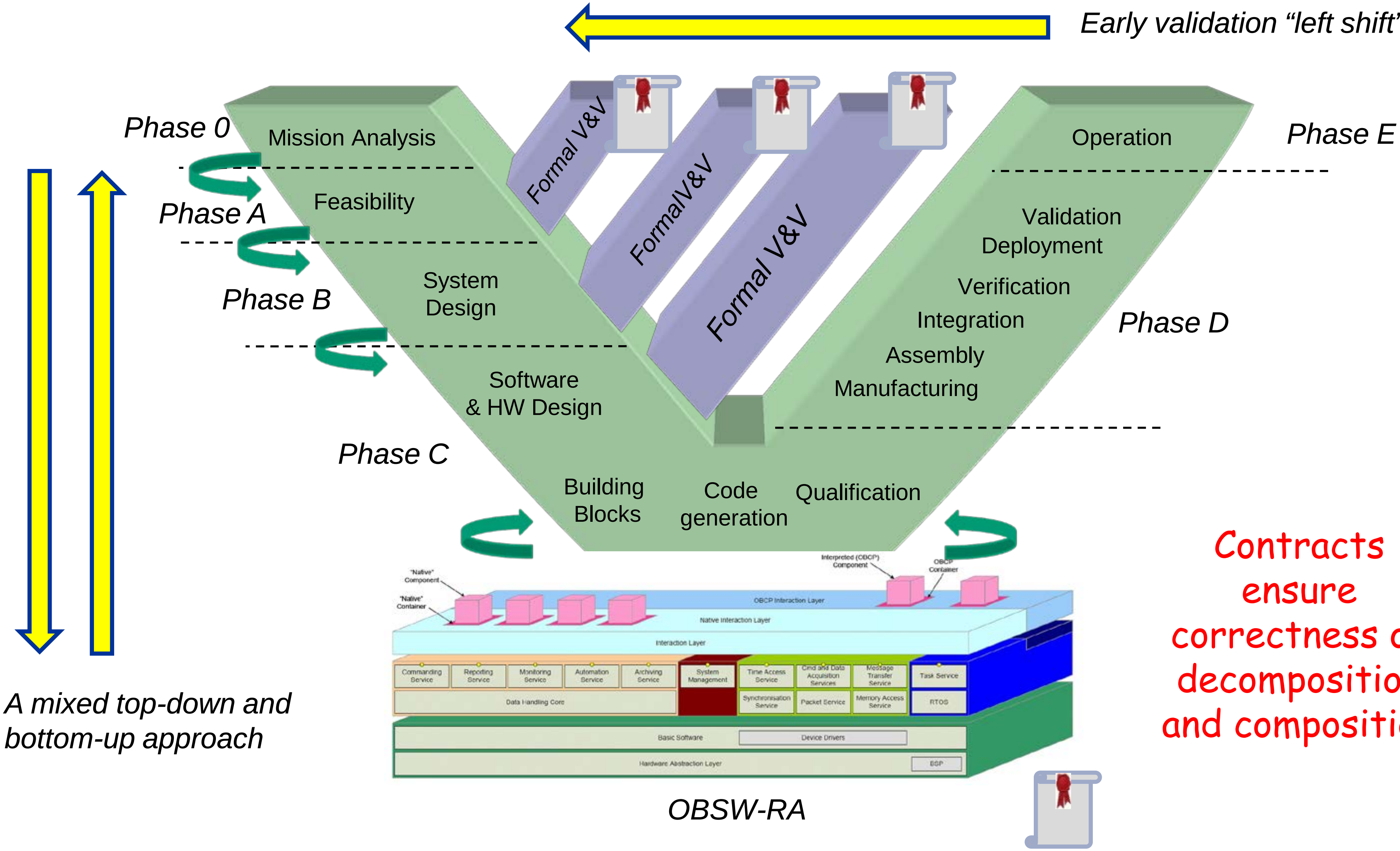
The FoReVer Integrated Environment



The FoReVer Toolset At Work



The Vision for a Model Based Systematic Approach



A mixed top-down and bottom-up approach

Contracts ensure correctness of decomposition and composition

Conclusion

- A MBSSE solution for system composition correctness analysis
- Integration in the CHESS toolset
  - An front-end for the COMPASS-STAR technology in the OMG UML MBSE world
  - Availability as open-source in the Polarsys/Eclipse open community
    - Increase the potential for other R&D extensions and user experimentation/maturation

Thank you for

your attention!

Questions?