CHESS

Composition with guarantees for High-integrity Embedded Software componentS assembly

Andrea Bondavalli, University of Florence

What is CHESS

□**ARTEMIS JU project** Call 1 2008 on **Design Methods and Tools**

□**Technical Coordinator** Intecs – Pisa, Italy

□**Partners** 18

□**Countries** 6

□**Start** February 1st, 2009,

□**Duration** 3 Years,

□**Total cost** 11.9 M €

CHESS Partners

Industrial Partners

Intecs (Co-ordinator) (I)
Italcertifer (I)
Thales Alenia Space (F)
Thales Communications (F)
Aonix (F)
GMV (E)
Atos Origin (E)
Aicas (D)
X/Open Company Limited-
The Open Group (UK)
Ericsson (SW)
Enea (SW)

Research Centres

CNR/ISTI (I)
INRIA (F)
Fraunhofer ESK (D)
Forschungszentrum
    Informatik FZI (D)

Universities

University of Padua (I)
Universitad Politecnica de
    Madrid (E)
Maelardalen University (SW)
**University of Florence (I)
    (subcontractor of ISTI/
    CNR)**

CHESS Objectives

- **Definition of a Multi-Concern Component Methodology and Toolset**
  - Definition of a multi-concern modelling language,
  - Enabling the expression, analysis, verification and preservation of extra-functional properties of components as contracts
  - Integration of tools for the analysis, verification and preservation of the extra-functional properties of component contracts
- **Adapting infrastructures for the integration and run-time support of components with preservation of extra-functional properties**
- **Validating the approach through multi-domain case studies**

CHESS Approach

- – Adoption of Component Based Development and Model Driven Engineering approaches
- – Capturing of extra-functional requirements
- – Property preserving component assembly
- – Separation of concerns
- – Correctness by construction
- – Guarantees at run-time
- – Traceability between the extra-functional requirements and the properties of software components

Focus on improving the development of embedded systems

About the Extra-Functional Properties in CHESS

- **The focus is**
  - to clearly separate the control and extra-functional part of a component from its functional part
  - to ensure extra-functional properties are asserted and validated at model level and preserved at run-time
- **Extra-functional properties addressed**
  - Real-time, predictability, isolation and transparency
  - Dependability (incl. Safety) and Security properties, considering both accidental faults and intentional threats

Extra-functional is used in place of non-functional, as non-functional may have connotations of not working or not functioning
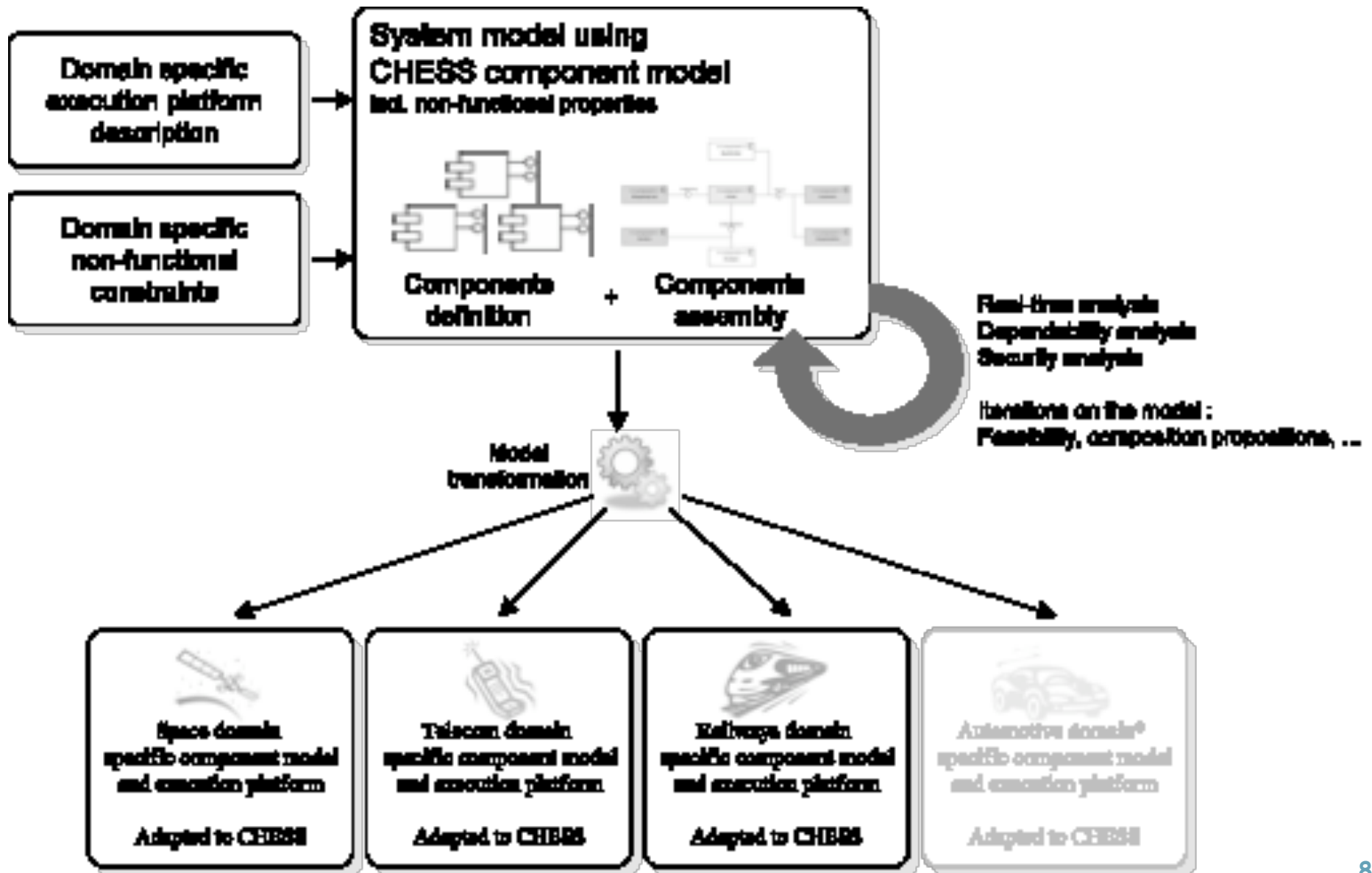
CHESS Application Areas

- Space
- Railways
- Telecom
- Automotive

CHESS will guarantee a required level of service for the assembly of hetereogeneus software components assets on the target execution platform

The CHESS Methodology

The CHESS Modeling Language

- Based on the OMG MDA world
  - MOF, UML2 and related Domain Specific Languages
  - MARTE, SysML, HRT-UML/RCM
  - QoS and FT profile
  - CORBA CCM, LwCCM
- Inputs also from EAST-ADL2, AUTOSAR

Ongoing project activities

Requirements and Specification (WP1)

– Identification of use-cases non functional requirements (*industrial partners*)

– Specification and characterization of the kinds of platforms to support the execution of CHESS multi-concern components (*industrial partners*)

– Provision of specific requirements for CHESS multi-concern model-driven development (*industrial + research partners + technology providers*)

- **ISTI-UNIFI**: Identification of the specific non-functional properties to be addressed in the project and the requirements for the modeling languages, <u>focusing on dependability aspects</u>

Ongoing project activities

Multi-Concern Component Model (WP2)

- – Inspection of the available component modeling languages and tools (*research partners + tool providers*)
    - • **ISTI-UNIFI**: focus on MARTE, QoS&FT and SysML profiles
- – Definition of the CHESS modeling language to be used for the description of component-based architectures (*research partners + tool providers*) through metamodeling and/or profiling
    - • **ISTI-UNIFI**: Definition of the language elements, properties, constraints, rules and mechanisms to be included in the CHESS modeling language, <u>focusing on dependability aspects</u>

Next activities
(starting end of July)

Dependable and Secure Component Concerns (WP3)

- It will produce the transformation and analysis backend infrastructure to WP2, providing scientific solutions and technology support for dealing with non-functional concerns related to dependability and resiliency properties in the CHESS multi-concern framework
  - **ISTI-UNIFI**: WP technical coordinator

Predictability, Isolation and Transparency Component Concerns (WP4)

- It will produce the transformation and analysis back-end infrastructure to the multi-concern component model (mostly timing analysis)