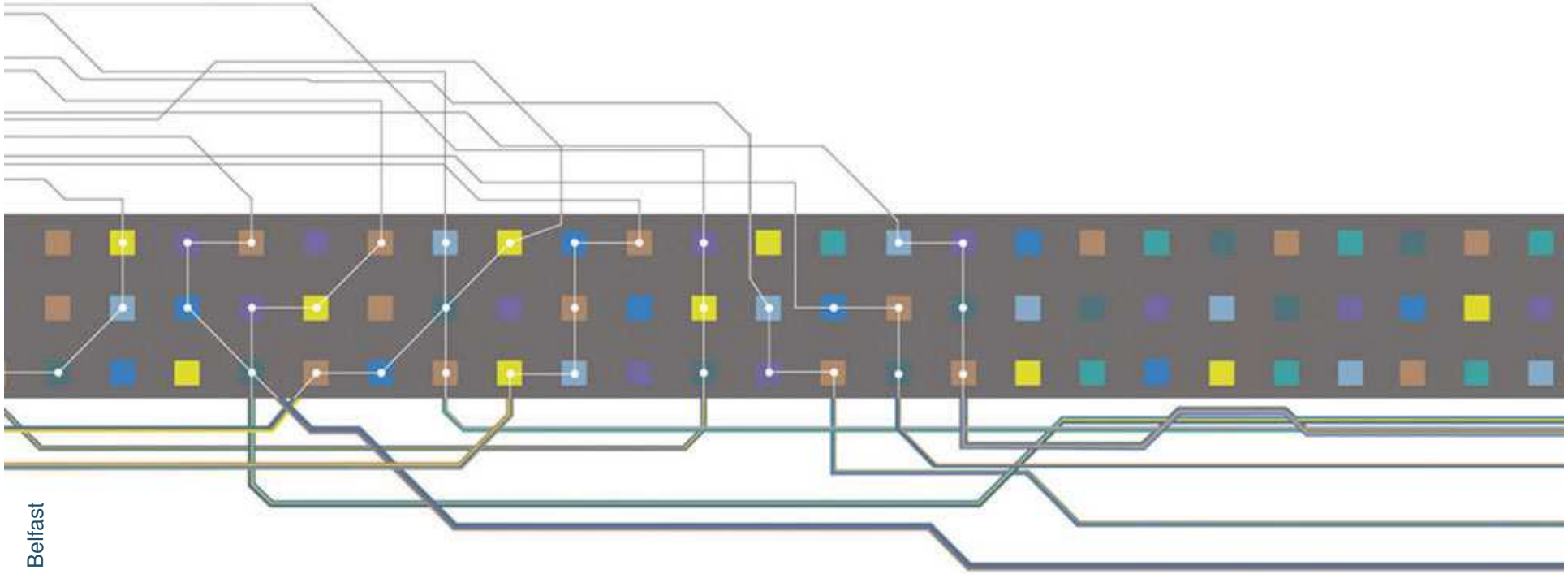
THALES



02/04/2008, AADL-UML 2008, Belfast

Automatic Composition of AADL Models for the Verification of Critical Component-Based Embedded Systems

Hugues Balp, Étienne Borde, Grégory Haïk, Jean-François Tilman

02/04/2008, Belfast

ITEA-SPICES*

The project global objective is to provide means to ***certify*** component-based applications thanks to modeling techniques.

Open standards technologies

- AADL (SAE) for ***modeling***
- Lightweight-CCM (OMG) for ***composition techniques***

Our approach consists in using a component-based (Lw-CCM) development process to automatically compose the analyzable (AADL) model of the system

*Support for Predictable Integration of mission Critical Embedded Systems

Lw-CCM Based Development Process 1/2

- Guarantees a clear ***separation of roles***

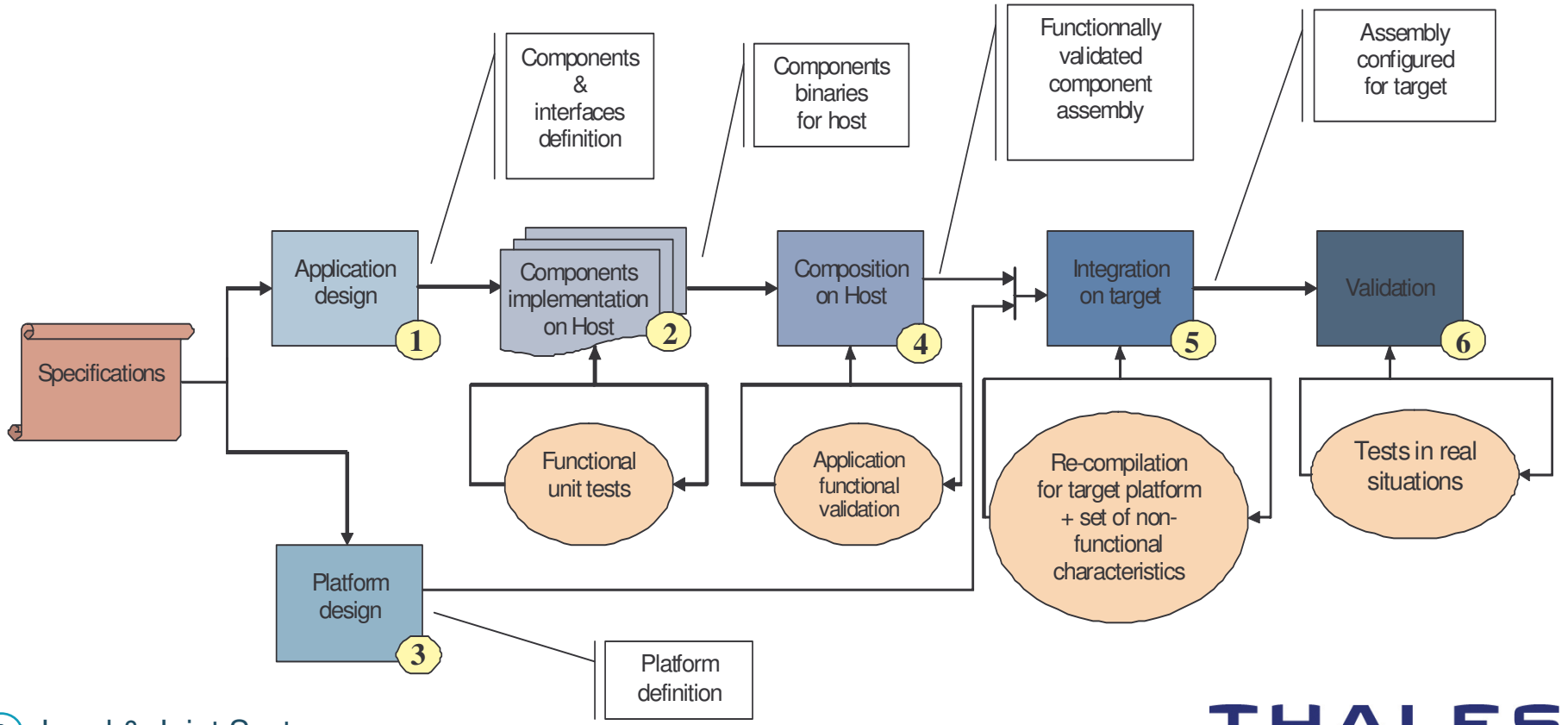
  Application designer, component designer, framework designer, platform designer, and system integrator

- Uses non-functional ***code generation*** so as to enforce functional code portability
  - Components envelopes code is ***generated by the component framework*** from their IDL3 definition
  - Application migration from host to target only consists in using a different ***generation configuration***

- Enables early ***validation on host***
  - Functional unit tests and functional validation can be made on host since the functional code is the same on host and target.

Lw-CCM Based Development Process 2/2

Design Actor		Role
application designer	1	design of the component-based software application
component designer	2	design and implementation of components
platform designer	3	design of the target platform
framework designer	4 5	design of the component framework add-ons: services and connectors
system integrator	4 6	deployment of the application on the targeted platform

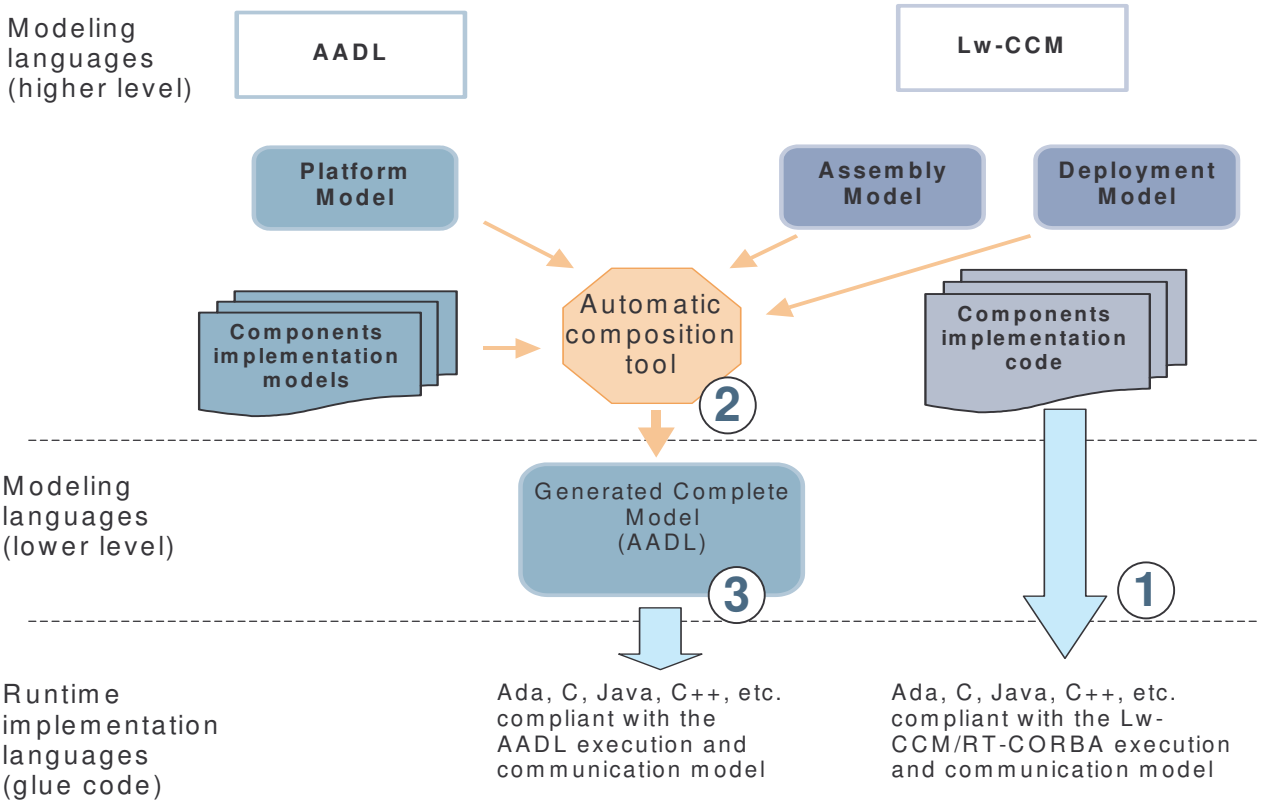


Model-based Early Verification

- Problem: The PSM of the system is evolving all along the design process
  - Error prone
  - Time consuming
  - Difficult maintenance

- Approach : Automate the production of this model

Global Modeling Approach



Tool (1): Already existing and deployed on an industrial project

Tool (2): Prototyped in the scope of SPICES

Enables to model precisely component-based architecture using the *common subset* of AADL and Lw-CCM/RTCORBA/POSIX constructs.

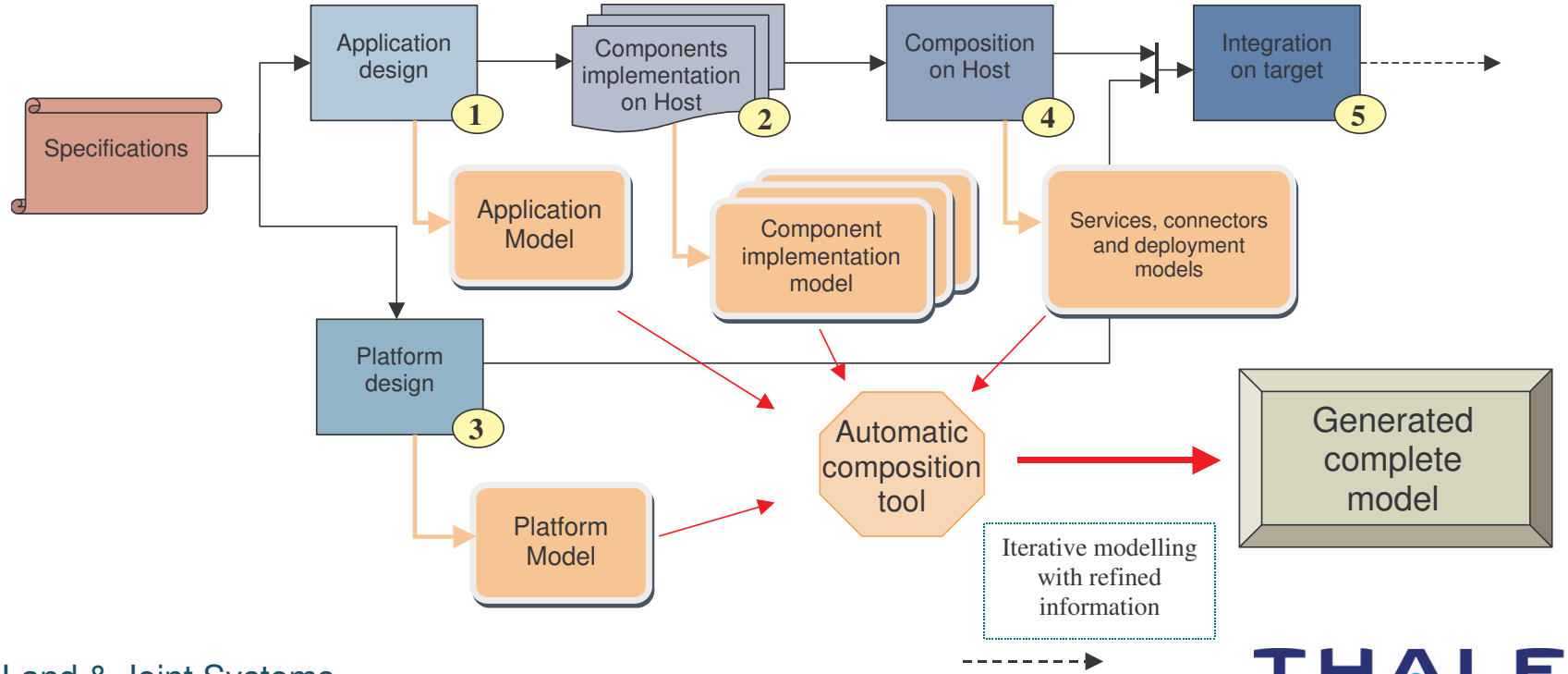
Tool (3): Perspective of our work

Enables to improve confidence between runtime implementation and lower level model

THALES

Modeling and Development Process

Design Actor	Modeling Constructs
application designer (1)	Lw-CCM components assembly
component designer (2)	AADL component implementation models
platform designer (3)	AADL Platform model
framework designer (4) (5)	AADL models of framework add-on: predefined components + technical services + composition mechanisms
system integrator (4) (6)	Lw-CCM deployment plan



THALES

AADL models

Models	*AADL constructs*
AADL Platform model	**Memory, processors, buses.**
AADL components implementations models	**Set of subprogram types and implementations with subprogram calls and event data ports and requires subprogram group access with AADLv1.6**

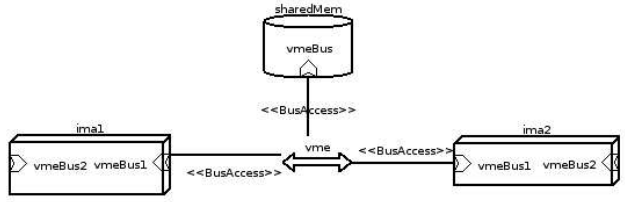
Lw-CCM models (1/2)

Models	*Lw-CCM constructs*	*Corresponding AADL constructs*
Assembly model	**1. Predefined components**	**1. Depends on the Lw-CCM component type: Threads for RT-Timer component**
	2. Technical services	**2. Set of subprogram types and implementations: One must be "service_pre_invoke", another must be "service_post_invoke".**
	3. Connectors	**3. Depends on the connector type**

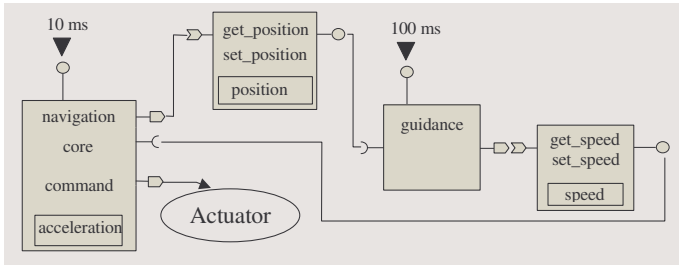
Lw-CCM models (2/2)

Models	*Lw-CCM constructs*	*Corresponding AADL constructs*
Assembly model	**4. Connections** **5. Instances** **6. instances configuration**	**4. Connections between event data ports + requires/provides subprogram group access with AADLv1.6** **5. Subprogram calls (with AADLv1.0) / subprogram group instance with AADLv1.6** **6. Insertion of technical services subprograms calls** **+ Instantiation and initialization of data corresponding to attributes**
Deployment Plan	**1. Nodes** **2. instances allocation on nodes**	**1. Processes definition and allocation on processors** **2. Allocation of activation and/or communication threads into processes** **+ server subprograms and Actual_Subprogram_Call property for remote components (with AADLv1.0)**

Automatic Composition Experimentations: Autopilot Example

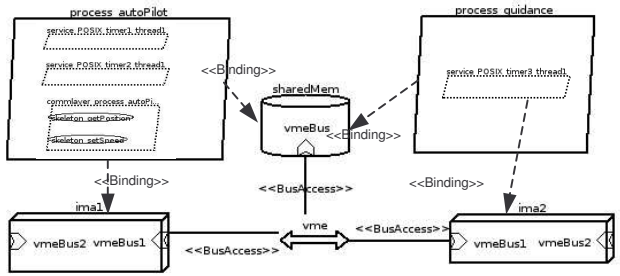


+



Guidance → proc_guidance
Autopilot → proc_autopilot
PositionShM → proc_autopilot
SpeedShM → proc_autopilot

\+ Components implementation models → Automatic composition tool → **for analysis**



\+ Components implementation code → MyCCM D&C tool → **for realization**

THALES

Objective

Check feasibility of verification and validation ***all along*** the development process

Realization : a three steps schedulability analysis

1. Use of OSATE schedulability plug-in to budgetize threads execution time and allocate their execution on processes
2. Use of MAST to experiment more precise analysis, including operation sequence calls on a component model
3. Use of UPPAAL so as to include control flow in the schedulability analysis

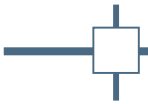
Results show the importance of refining models all along the design process.

The approach presented

- Provides a methodology to master complexity when designing complex and critical real-time distributed embedded systems
- Permits early and iterative design space exploration thanks to model analysis
- Enables to reuse pieces of development as well as corresponding models
- Authorizes iterative refinements of the models
- Eases the maintenance of the global model

Perspectives

- Usage of AADL v1.6 or higher simplifies the definition of mapping rules between AADL and Lw-CCM.
- Code generation: non-functional and deployment code should be generated from the AADL global model
  - Considered tool: ***Ocarina*** code generator for PolyORB-HI.
  - Objective: improve insurance to respect the AADL semantics and enable to master links between AADL global model and non-functional code implementation.



Thank you for your attention,

Do you have questions ?

Etienne.Borde@fr.thalesgroup.com