THALES

→ **Experience Report on Implementing and Applying a Standard Real-Time Embedded Component Platform**

Gregory Haik – gregory.haik [at] fr.thalesgroup.com
V. Watine, V. Seignole, O. Hachet, J.-L. Gilbert, H. Balp
THALES Land & Joint Systems, France

Land & Joint Systems

THALES

Zoom out: Thales Group

- Electronics and optronics equipment vendor, and system integrator
- Addresses defense and security markets
  - Military telco, Aerospace, Naval, ATM & Air Defense, Homeland Security, e-gov't
- Sales: 12 billion €
- 70 000 employees in +50 countries, mostly France & UK

Zoom in: SC2 Lab

- Part of Land & Joint Division (radio-communications, optronics, C4I)
- In charge of Research & Technology activities on middleware
  - R&T on component frameworks for RTE systems
  - R&T on interoperability and integration of complex systems (SoS)
- Promotes R&T results in company's programs
- 25 people

THALES

- Who Are We ?

- Motivations

- Approach

- Use cases

  - FM3TR Software-defined Radio

- French & European Research Outlook

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- Standardisation Issues

Land & Joint Systems

THALES

Development of ***Real Time Embedded (RTE) systems*** suffers from the same productivity problems than ***large-scale information systems***, such as:

- Platform heterogeneity
- Difficult testability
- Complex internal communication and interaction schemes
- Difficult configurability…

… plus many others !

- Timing issues
- Certification/assurance issues: safety-critical, mission-critical, security-critical
- Memory footprint
- Domain heterogeneity: telecommunications, avionics, vetronics, robotics

> Software Engineering solutions for information systems must be ***adapted and extended*** to address RTE systems development

- **Who Are We ?**

- **Motivations**

- **Approach**

- **Use cases**

  - FM3TR Software-defined Radio

- **French & European Research Outlook**

  - Validation & Verification

  - Dynamic Reconfiguration

 - Flexible Scheduling

- **Standardisation Issues**

OMG RTE Systems Workshop
Washington, July 2007

Land & Joint Systems

THALES

- Addressed by IST **COMPARE** and **MERCED** and ITEA-Projects
- EJB, CCM target **Information Systems** and address:
    - Code reuse; Interoperability; Automatic deployment and configuration
- Non-functional needs of Information systems are
    - Communication support
    - Security
    - Persistency
    - Transactions
- **RTE systems** : no such list be *a priori* devised
    - *OMG Lightweight CCM specification* defines empty component enveloppes – no security, no persistency…
    - Up to the framework provider to *tailor enveloppes to a particular domain*
    - Still, it requires a fine requirement analysis of domain – product line – application

THALES

THALES
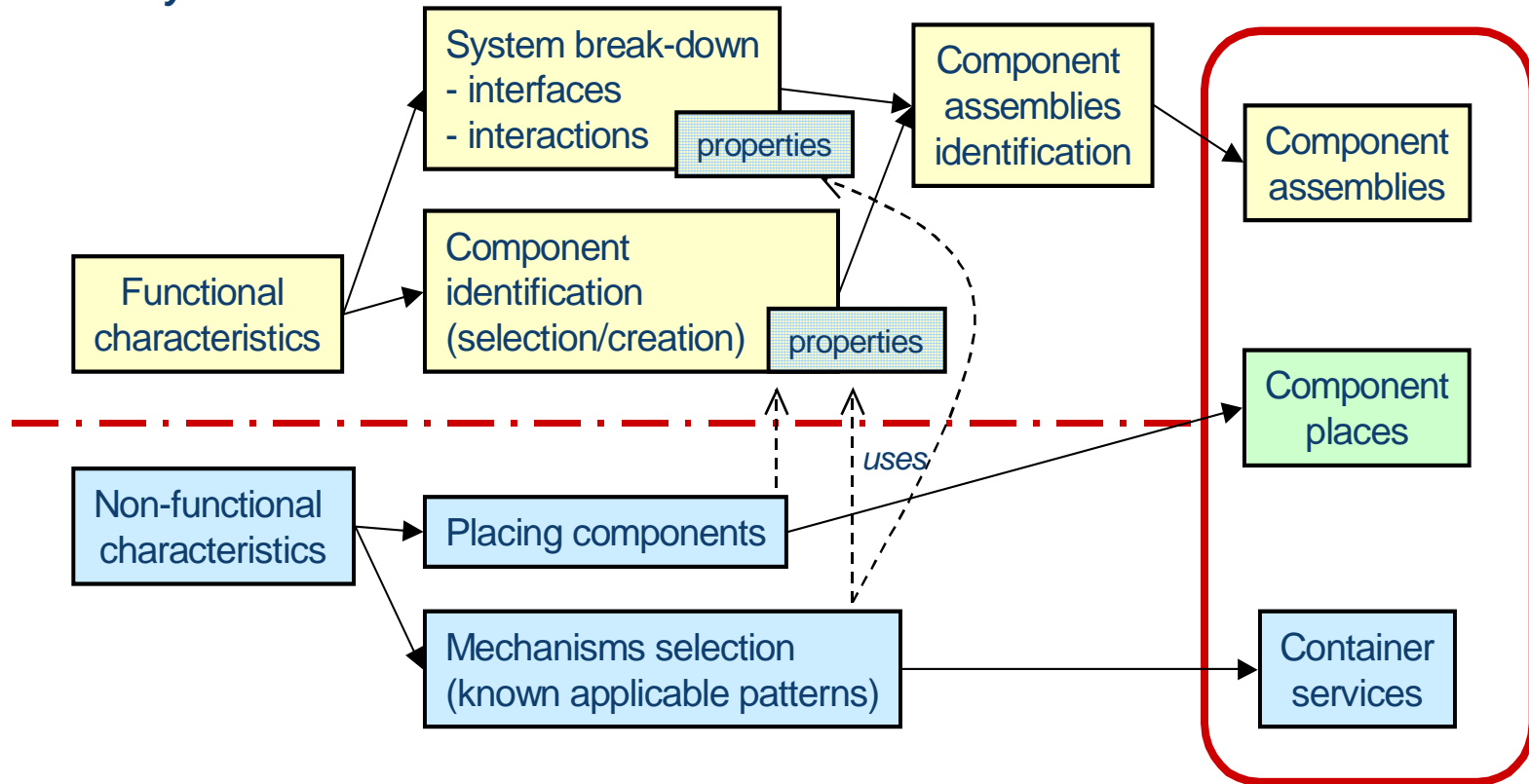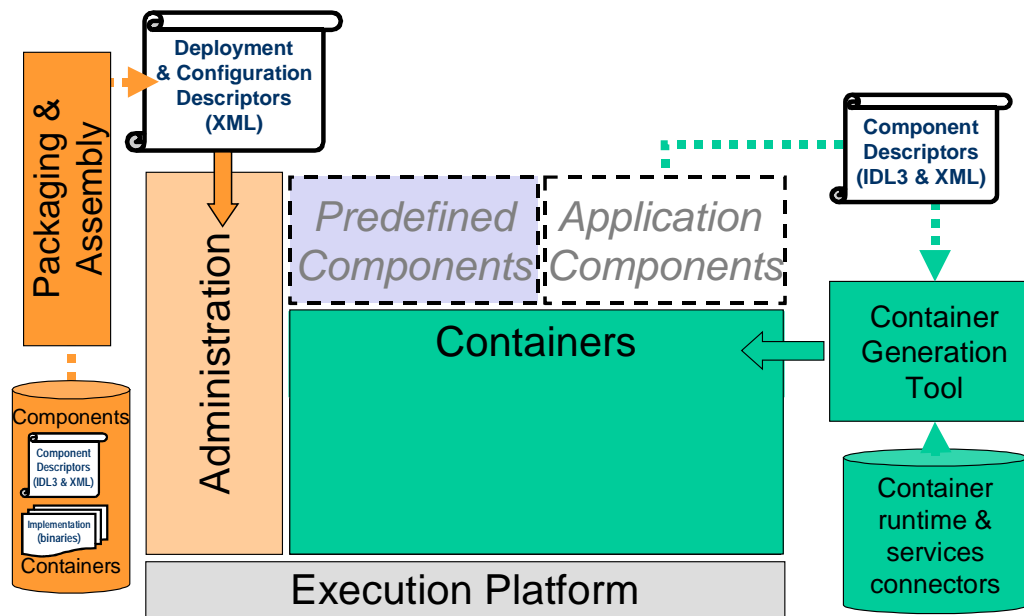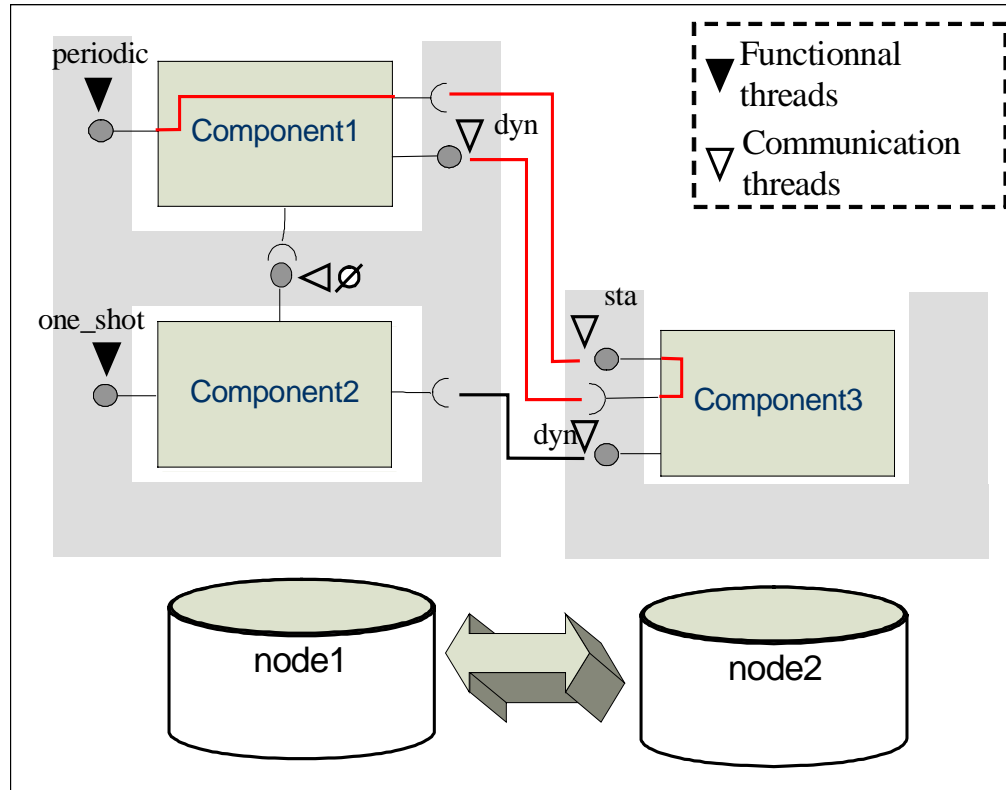
Tailoring enveloppes while minimizing memory footprint calls for a *modular architecture of the component framework* itself.

The extra benefits of this approach (beyond those of CBD) are :

➤ The ability to plug-in only what is strictly necessary

➤ The ability to adapt to various domains or product lines or even applications

MyCCM enables the ***configuration of real-time scheduling parameters*** to:

- Define an activation model based on "periodic" and "one shot" "functional threads"

- Set the scheduling parameters of "communication threads" handling the component interaction mechanisms

OMG RTE Systems Workshop
Washington, July 2007

THALES

- Who Are We ?

- Motivations

- Approach

- Use cases

  - FM3TR Software-defined Radio

- French & European Research Outlook

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- Standardisation Issues

OMG RTE Systems Workshop
Washington, July 2007

THALES

THALES

THALES

THALES

- **Who Are We ?**

- **Motivations**

- **Approach**

- **Use cases**
  - FM3TR Software-defined Radio

- **French & European Research Outlook**
  - Validation & Verification
  - Dynamic Reconfiguration
  - Flexible Scheduling

- **Standardisation Issues**

OMG RTE Systems Workshop
Washington, July 2007

This document is the property of Thales Group and may not be copied or communicated without written consent of Thales
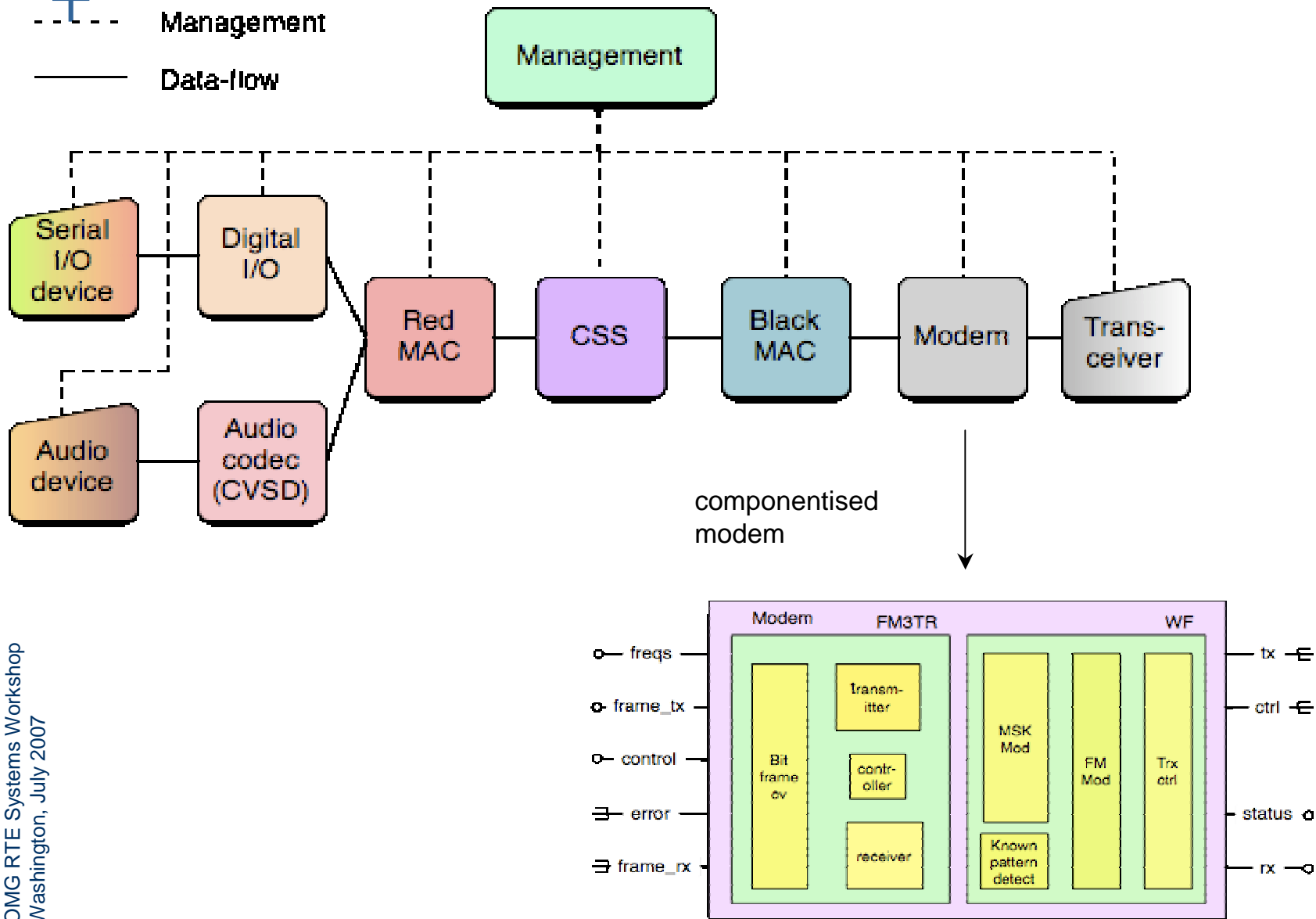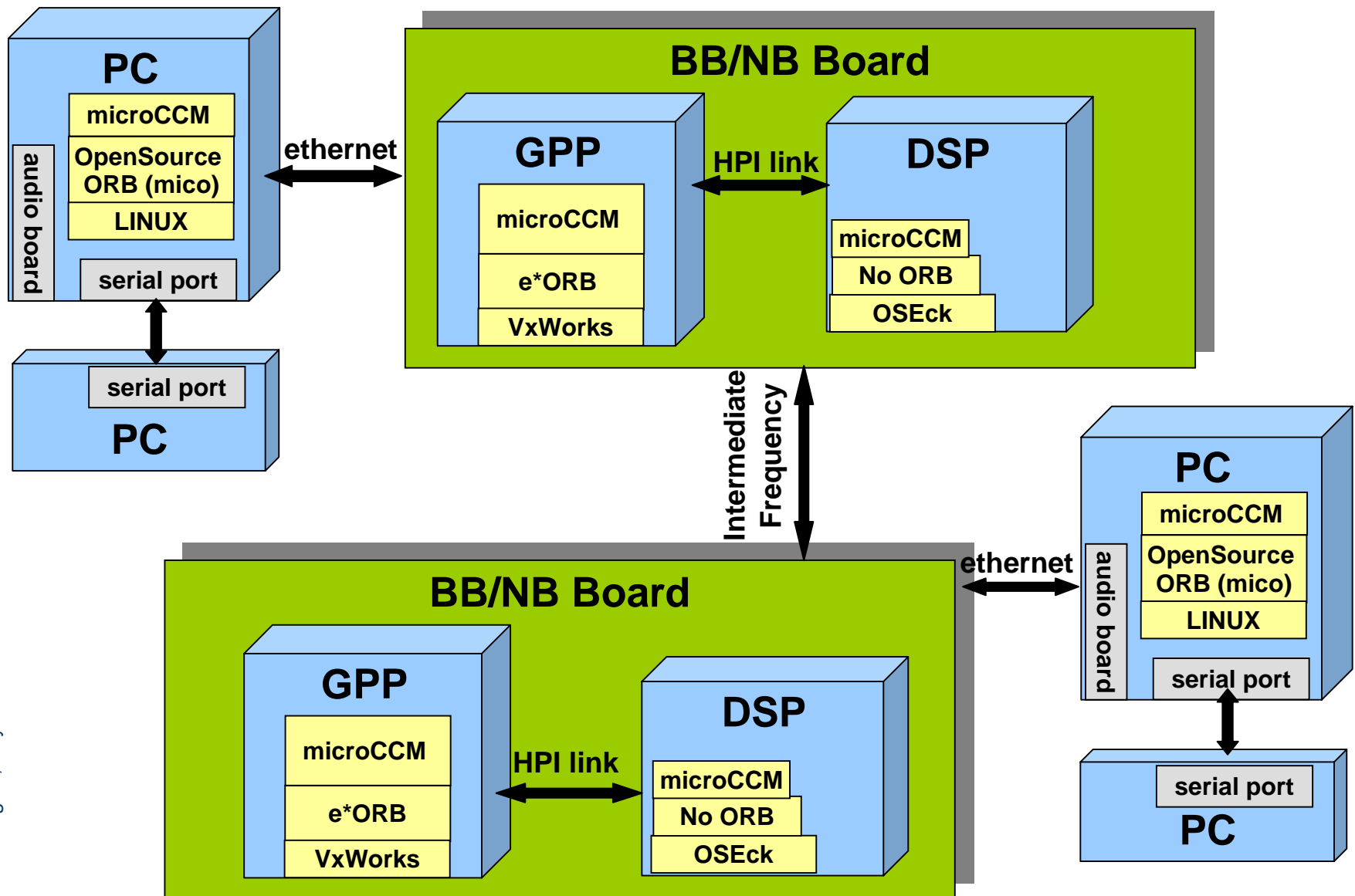
THALES

MyCCM improves RTE software development *productivity*

- **Intensive code generation**
  - Abstraction and generation of internal communication protocols
  - Generation of deployment code
  - Generation of threading artefacts

- **Integration with modelling tools**
  - Improving communication between team members
  - Facilitating verification (yet a promise)

- **Ease of testing**
  - Functional validation on host platform

- **Late binding to the target platform**
  - Reduced integration risk

OMG RTE Systems Workshop
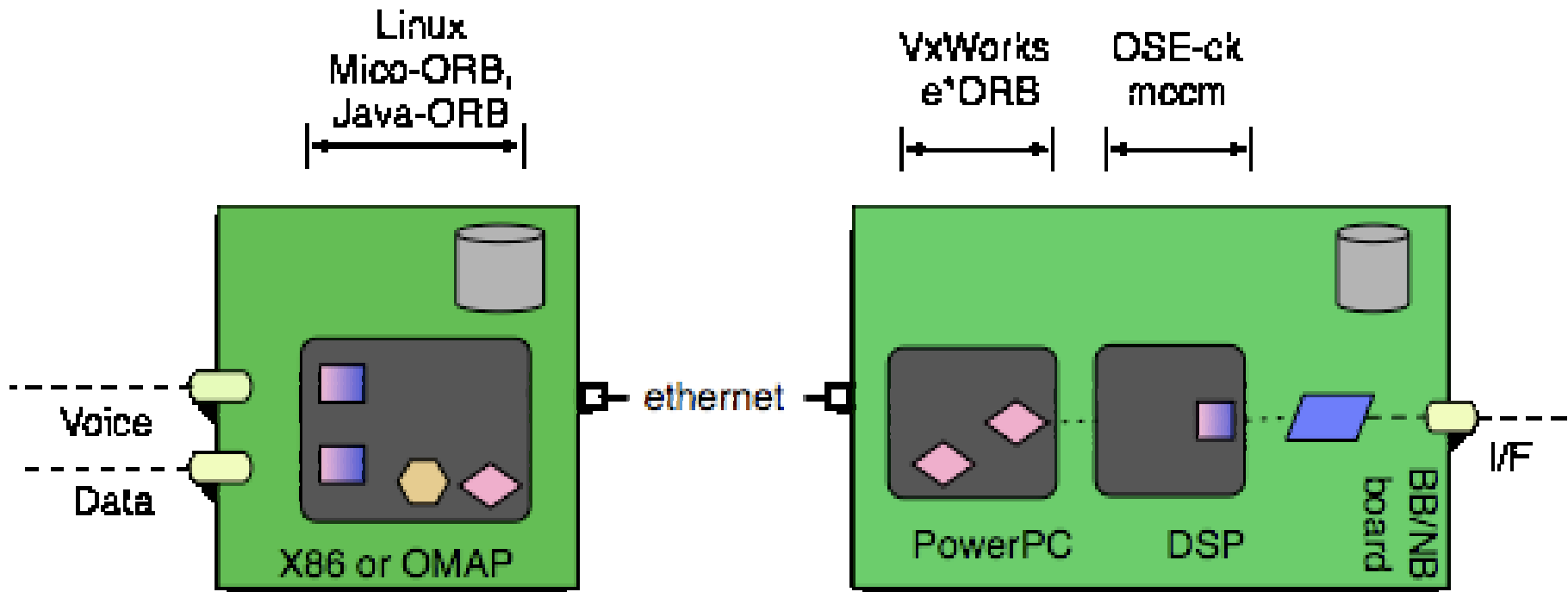Washington, July 2007

THALES

- Who Are We ?

- Motivations

- Approach

- Use cases
  - FM3TR Software-defined Radio

- French & European Research Outlook

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- Standardisation Issues

OMG RTE Systems Workshop
Washington, July 2007

Land & Joint Systems

THALES

To address ***hard real-time critical*** systems development, the framework must come with means to check that the deployed architecture will meet its <u>timing requirements</u>.

As a first step towards component-based architecture verification and validation, ***schedulability analysis*** should be performed:

- This requires the framework user to provide a characterisation of the ***temporal properties of each component***.
- Combining this information with the activation model and corresponding communication threads, end-to-end ***execution times*** can finally be estimated.
- Transcribing this information in a tool like MAST, ***temporal analysis*** may be performed.

Many other requirements may be verified…

THALES

AADL Modelling of Component-based Architecture

PowerPC 860 ⟷ RamBus
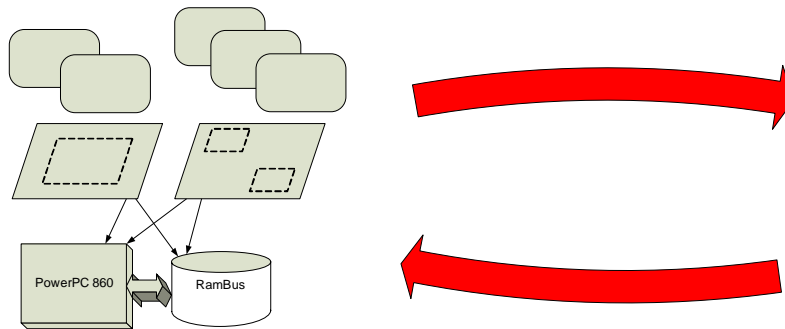
Lightweight CCM descriptors

Application Components Packages
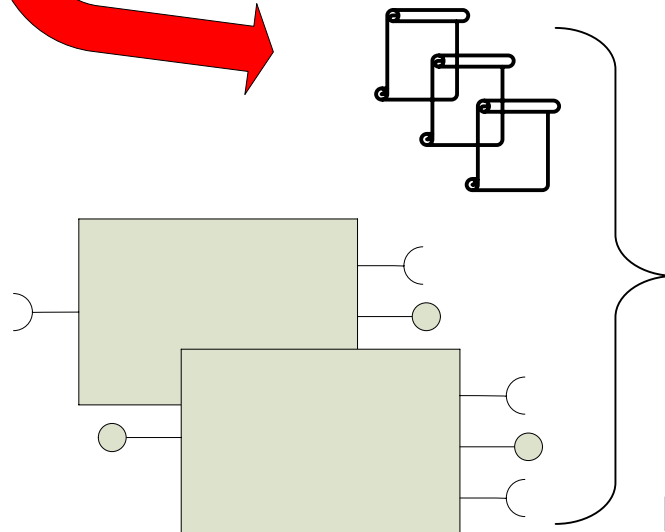
Verification Techniques

- **Schedulability, energy, memory analysis**
  - MAST, Cheddar…
- **Model Checking**
  - BIP, TINA, CPNTool
- **Simulation**
  - SystemC, MyCCM, Ades
- **Middleware code generation and verification**
  - PolyORB-HI, Occarina

Administration	Application Components	Pre-defined Components
	Containers	
	Infrastructure	
	Technical Service	Technical Service	Technical Service

Execution Platform for **General-Purpose Processors**, **DSP** and **FGPGA**
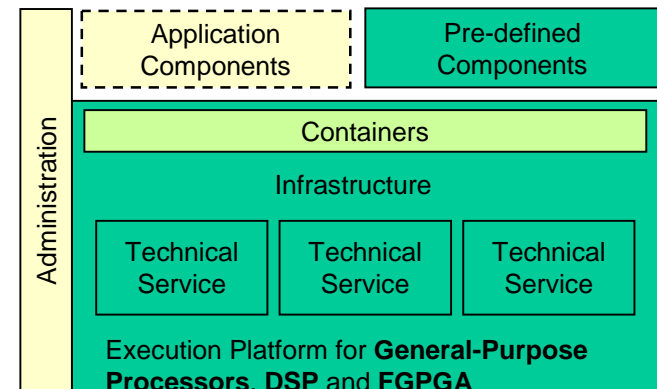
Running System

THALES

- **Who Are We ?**

- **Motivations**

- **Approach**

- **Use cases**
  - FM3TR Software-defined Radio

- **French & European Research Outlook**

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- **Standardisation Issues**

THALES

Flexibility: Dynamic Reconfiguration

- Increased adaptability of RTE applications
  - Bug correction,
  - Power limitations,
  - User requests
  - Fault tolerance …

- Means evolvability of the system architecture
  - Functionality removal
  - Component migrations, deletion, replacement.

- Direction
  - Generative reconfiguration language
  - Analysis of reconfiguration policies for validation purposes

- Addressed by Paris Region-funded project *Usine Logicielle*
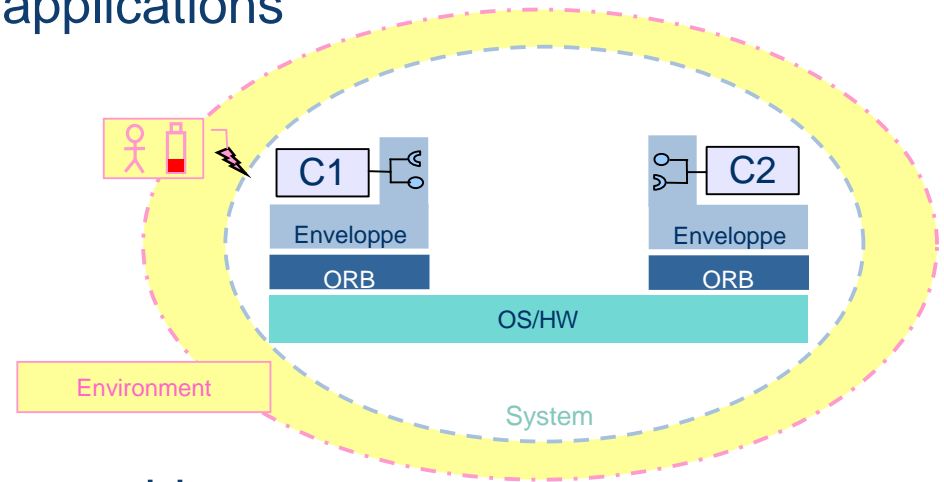
THALES

- Who Are We ?

- Motivations

- Approach

- Use cases

  - FM3TR Software-defined Radio

- French & European Research Outlook

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- Standardisation Issues

- **Beyond fixed priority scheduling**, *à la* POSIX
- Typically valuable for processing sound/video
    - Use case is a UMTS protocol stack
- Applicability criteria
    - Hard real time, i.e. overrun is a fault… BUT
    - Not safety- nor mission- nor security-critical
    - What is critical is resource usage optimization
    - WCET >> Average Execution Time
        - Schedulability Analysis is too pessimistic
- Proposed Solution (Univ. Cantabria, Univ. York)
    - Dynamic allocation of resources to processing tasks
    - Components come with a range of implementations
        - Fast computation, low quality
        - Slow computation, high quality
- Addressed by EU-funded FRESCOR Project

THALES

- Who Are We ?

- Motivations

- Approach

- Use cases
  - FM3TR Software-defined Radio

- French & European Research Outlook

  - Validation & Verification

  - Dynamic Reconfiguration

  - Flexible Scheduling

- Standardisation Issues

Land & Joint Systems

THALES

- **Lightweight CCM std has limitations**
    - No definition of insertion contracts for technical services
    - Interaction models are restricted to
        - Facet and receptacles (RPC)
        - Push-Push events
- **Deployment and Configuration std needs adaptation for RTE**
    - Multi-domain, multi-application deployment should be optional
    - Semi and fully static deployment should be considered
- **Ongoing standardisation activities**
    - *QoS for CCM* addresses insertion & config of technical services
    - *DDS for CCM* addresses extensions of interaction models
    - Nothing directly targeting D&C spec
- **Major conformance points**
    - Source-level conformance of components with CIF
        - Enables re-use of components in various deployment contexts
    - Conformance of descriptors to XML schemas of D&C std
        - Provides stability to modelling tools
    - Standards are a starting point for further adaptation

THALES

- **MyCCM is beyond the *proof-of-concept***
  - Foundations of SW development for FREMM's IRST
- **Many research activities presently conducted**
  - V&V, dynamic reconfiguration, flexible scheduling
  - But also: FPGA, ARINC 653, MILS…
- **Standardisation activities should go on**
- **Relevance of LwCCM is maximum when leveraging architectural descriptions**
  - RT/E systems with stringent time/memory/energy constraints
    - Careful mapping of SW architecture to HW platform
    - Fine-tuning deployment and configuration at integration time
  - Reasonably small amount of SW components
  - Performing early V&V on architectural models
  - Otherwise DDS might be more relevant
    - More straightforward, less architecture burden
    - Still good opportunities for code re-use

THALES

D&C profiles

- fully-static
- semi-static
- dynamic

Footprint versus Dynamicity Tradeoffs

Multiple languages

- ISO-C++
- E-C++
- Ansi C

Availability of the three IDL mappings

Local seamless cohabitation of languages

Multiple targets

GPP
- X86, Linux, e*ORB C++ / e*ORB C
- X86, Linux, mico, TAO
- MPC860, VxWorks, OrbExpress
- MPC860, VxWorks, e*ORB C++
- generic, VxWorks, Orbless

DSP
- C5510, OSE-ck, Orbless (C)
- C5510, OSE-ck, e*ORB C
- C5510, DSP/Bios , Orbless (C)

Micro controllers
- ARM7, OSEK (auto RTOS), EC++
- ColdFire, OSE-epsilon (C)

Reusable services and connectors

Technical services
- messaging code generation
- real-time CORBA integration
- real-time trace
- performance measurement
- RT locking mechanisms

THALES