European initiative on predictable integration of Embedded Systems

Vincent Seignole (THALES Communications)
Spices consortium

Consortium

- FRANCE
  - THALES Communications
  - THALES Avionics
  - AIRBUS
  - CEA
  - FéRIA
  - VERIMAG
  - LESTER

- SPAIN
  - SQS
  - TCP/SI
  - University of Cantabria

- BELGIUM
  - BARCO Avionics
  - K.U Leuven
  - CETIC

- Industry
- Research centers
- Software Engineering consulting

Spices consortium July 08
Challenges in the field (1/2)

Distribution of defects origin

- Requirements: 56%
- Design: 27%
- Code: 7%
- Other: 10%

Upwind phases defects!

Cost of fixing design error at specific stage

Defects profile

- Analysis: 50
- Design: 250
- Coding: 450
- Developer testing: 225
- System testing: 169
- Operation: 56

Often identified in late phases only!

Note: Excerpts from CrossTalk Journal, 2003
Applies to «generic software»

Spices consortium
Challenges in the field (2/2)

Cut the costs

- Embedded sw Integration?
- Certification?

- Architecture Reuse?
- Embedded sw Reuse?
- Requirements traceability?
- Verifications?
- Leverage Heterogeneous Hardware?
- Architecture properties Prediction?
Spices consortium

Project General objectives

- Predictable integration of embedded software

- Modelling
- Analysis Prediction Verification tools

- Embedded fwk Generative techniques

- Maturation Assessment (demonstrators)
- Integration in development processes

- Certification

- Industry domains: Avionics, space, communications

- Standardisation

- Dissemination

Exploitation

Spices consortium

July 08
Technologies involved

**Tools**
- Requirements
- Architecture modeling
- Platform Modeling
- Verification
- Model simulation
- Real-time Schedulability analysis
- Power-consumption analysis

**Execution**
- Space target
- Avionics target
- Software radio platform
- Simulation
- Implementation
- Timing prediction

**Quality standards**
- DO-178B
- DO-254

**Power-mngt**
- Real-time integration support
- Verification

**Spices consortium**
July 08
Spices consortium

**Spices**

Comprehensive set of tools

Tools organised around open (and integrated) standards

AADL modelling language

Component model (CCM)

SPICES toolset

AADL model(s)

- ADELE
- OSATE
- Scheduling analysis
- Power consumption analysis

TOPCASED (integration)

FAUST
- Edit models
- Deduce initial models from formal requirements

OS-Explorer SoftExplorer
- Model checking
- Update timing model

TINA
- AADL/SCM/AADL mappings
- Conformity of software versus model

BIP
- Integrate code with AADL simulation
- Unitary estimate worst-case execution time

PathCrawler WCET
- Timed simulation

ADES
- Integration on target hardware

Component framework

Direct Generative techniques

Implementation code (CCM, AADL-C)
AADL Graphical modelling (ADELE)

- **ADELE** is a graphical modeler for component based languages.
  - Current implementation supports AADL 1.0 diagrams and generation of corresponding textual specifications.
  - It supports multi-models interactions and both top-down and bottom-up modeling processes.
  - A customizable description framework (ODS) is attached to each model entity which can also be used to support properties and target source code.
Verification based on AADL models

AADL model (threads + AADL Behavioural description)

Timed petri net analyser

TINA

BIP

Path analysis

States exploration

Animation

Simulation
Tools for embedded software components characterisation

- C language source code
- AADL model (with binding of sw to platform)

Worst case execution time tool

use

per C-function timing characteristics

Power Estimation tool

use

per C-function power characteristics

AADL model (including components’ characterisation)

Consumption analysis tool

Per hw-component energy consumption estimation

Spices consortium

Library of power models for hw components

Refers to
The **component based application** concept:
- Application made of reusable building blocks
- Organisation of these building blocks described formally

The **platform** concept:
- Combination of hardware & base software & Code generators
- More precisely
  - Providing resident sw components for access to the hardware devices
    - called **Hardware-abstraction components**
    - Examples: Serial link, Ethernet, GPIO, Radio-front-end,
  - Providing capacity to host component-based applications
Spices consortium

Steps / Technologies involved in CCM

Components specification
OMG IDL3

Components implementation
CIF, IDL mappings, C, C++, ...

Components assembly description
D & C

Components packages
OMG D & C

Composition (deployment) tool
OMG D & C

Deployed system

Library of predefined comps

Container modules
(QoS for CCM)

Connectors
(DDS for CCM)

Extensible Container
(QoS for CCM)

IDL3

Spices consortium

July 08
Spices consortium

AADL / CCM

- CCM: Architectural breakdown into functional components, and configuration entities for specification of execution semantics

  ➜ CCM has « so to say » no specified execution semantics: the execution semantics are the one of the target platform. Emphasis is put on the re-usability of components across different platforms.

  ➜ CCM does not include abstractions for execution concepts

- AADL: Description of coupled functional and non-functional architecture.
  ➜ AADL does provide execution concepts

Solution to benefit from both
SPICES Demonstrators
Range of demonstrators
Large coverage of requirements

- Functional aspects
- Non-functional aspects
- Complexity levels
- Degree of assurance
- Platforms
- Real-time Reqs

Interaction with humans
Reliability
Availability
Maintainability
Safety

- Small (10 Kloc) Level A
- Large (1 MLoc) Level C

- DO 178B Level A
- DO 178B Level B
- DO 178B Level C

- Avionics (IMA) pfts
- Embedded PCs
- POSIX RTOS
- GPP/ DSP FPGA
- C/C++/ADA Java/VHDL

Degree of assurance:
- DO 178B Level A
- DO 178B Level B
- DO 178B Level C

Platforms:
- Embedded PCs
- Avionics (IMA) pfts
- POSIX RTOS
- GPP/ DSP FPGA

Complexity levels:
- Small (10 Kloc)
- Large (1 MLoc)

Real-time Reqs:
- Soft
- ...
Demonstrators highlights

**Avionics:**
- A control, guidance and navigation system of an UAV (TCPSI + SQS)
- A Visualisation and a Maintenance system (BARCO Avionics + K.U.Leuven)
- A Flight Management System (THALES Avionics)
- An Air Traffic Control System (AIRBUS)
- A DMA Controller (AIRBUS)

**Communications:**
- A Radio System (THALES communications)

**Space:**
- Demonstrator under definition (TCP/SI)

We take benefit of a wide range of applications, technologies and platforms in order to validate a significant subset of SPICES tools
The complementary aspects of the use-cases

**Functional aspects:**
Interaction with human agents, signal processing, data processing, complex real-time functions

**Non-functional aspects:**
Reliability, Availability, Maintainability, Safety, ...

**Complexity levels:**
From small (10 KLoc) to very large applications (1MLoc)

**DAL levels:**
DAL A, B, C

**Platforms and operating systems:**
Embedded PCs, IMA platforms, POSIX compliant systems, A653 OS

**Development languages:**
Ada, C, C++, Java, VHDL

**Real-time requirements:**
From soft to hard real-time systems
A Control, Guidance and Navigation system of an UAV (TCPSI)

Spices consortium

July 08
A visualisation and a maintenance system (BARCO)
A flight management system (THALES Avionics)
Figure 4.2: Demonstrator simplified overview
An Air Traffic Control System (AIRBUS)
- generic enough radio hardware
- standard software platform running on the hardware
- ability to control R/F chain in software

Allowing a fully programmable and upgradable radio

Waveforms

Spices consortium July 08
More on SDR demonstrator (2/2)

Targeted hardware

- R/F front-end
- Conversion board
- Virtex 4 FPGA
- TI DM6446 SoC

- 32 bits FIFO A
- 32 bits FIFO B
- 2x32 bits Async control
- 2x MAC -Bsp
- SPI
- VPFE
- VPBE
- EMIF
- NAND flash

- ARM926
- TMS320 -C64+

- Ethernet
- Serial
- USB

Spices consortium

July 08
Spices consortium

Project roadmap

- Project execution launched 06 Sept 2007
- Project execution launched 08 Nov 2008
- Component based fwk v1 09 Aug 2009
- Demonstrators Evaluation Final Review 09 Aug 2009

- AADL modelling recommendations
- Analysis and verif techniques v1
- CCM fwk final
- tools
- CCM/AADL integration

Spices consortium July 08
Contact

- SPICES project website
  - http://www.spices-itea.org
  - Demos to be available end of summer there

- See our booth at Oct 2008 ITEA Symposium
  - Rotterdam (NL)

- SPICES will be present at Models’08 conf (Toulouse)

- For further discussions:
  - E-mail: vincent.seignole@fr.thalesgroup.com