Overall project goals and structure

L. RIOUX (THALES)
DECPS – 17 June 2016
PISA, Italy
High Level Goals

Multi-Core technology fulfills the ever increasing demands of highly automated systems, but additionally raises new challenges concerning programming complexity and safety properties.

ASSUME addresses these challenges by developing methods for:

- Efficient parallelisation of safety-relevant, performance-critical functionality
- Improved traceability of safety-relevant functionality in the development process
- Efficient verification of large systems
Project Partners

5 countries
39 partners
  16 industrial partners
  9 SMEs
  14 research partners
224 PY
Project outputs

• new static analysis algorithms implemented in various tools
• synthesis of real-time parallel code with formal guarantees of functional and non-functional correctness,
• standards and APIs for incorporating meta-data,
• standards for static analysis tool interoperability,
• integrated into a Static Analysis Platform (SAP)
Quantified objectives

• Increase performance (run-time) of analysis tools by 50%.
• Analyze single-core code with much higher precision, reducing spurious warnings by 60%.
• Significant reduction of false positives in runtime-defect analysis of concurrent software.
• Incorporate at least three new error classes (mainly for multi-core software) into analysis tools.
• Reduce the effort for inspecting runtime errors by 40% in a typical industrial setting.
• Build and demonstrate a complete software synthesis chain.
• Methodologies will be potential candidates for standard extensions to relevant standardization bodies.
• Build and demonstrate a fully certified compiler for a synchronous language.
• Exchange format specification captures the results of 75% of the analysis tools.
• Traceability of run-time errors back to the model level will be successful for at least 80%.
• Witnesses can be generated will be generated for close to 100% of error classes.
• Analysis on Simulink/Stateflow will be implemented for 60% of the modeling language.
Partners along the Value Chain

Tier 2 Supplier
Koc Sistem, NXP, Verum

Tier 1 Supplier
Arcelik, Bosch, Sagem, Thales

Original Equipment Manufacturer (OEM)
Airbus, Daimler, Arcelik, Ford Otosan, Ericsson, Scania, VDL, Havelsan

Technology vendors & Research
ENS, FZI, INRIA, KIT, KTH, Kiel Univ., Koc Univ., MDH, OFFIS, TNO, TUE, TUM, UT

Vendor for development tools
absint, Arcticus, B&M, BTC, Esterel, MES, UNIT, Verum
Management Structure

General Assembly (GA)

Technical Project Committee (TPC)

Project Coordinator (PC)

Project Steering Board (PSB)

Country Coordinators

Work Package Leaders

WP1 WP2 WP3 WP4 WP5 WP6

Project Mgmt (PM)

Quality Mgmt (QM)

France Germany Netherlands Sweden Turkey WP1 ...

WP6
### Roadmap

<table>
<thead>
<tr>
<th>Long term</th>
<th>Mid term</th>
<th>Short term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool Interoperability on a Static Analysis Platform</td>
<td>„Zero Code Defects“ for concurrent software</td>
<td>Next generation static analysis</td>
</tr>
<tr>
<td>Methodology for safe and efficient systems evolution</td>
<td>Correct-by-construction parallel applications</td>
<td>Analysis of MC specific defects</td>
</tr>
<tr>
<td></td>
<td>Static Verification of system concepts</td>
<td>Formally verified compilers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Formal Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Core Competencies

- **Requirement formalization**
  - B&M, Bosch, BTC, ENS, Esterel, INRIA, OFFIS, Scania, TNO, UNIT

- **Synthesis of concurrent software**
  - Bosch, ENS, Esterel, INRIA, Koc, Univ, NXP, Thales, Kalray

- **Program Verification**
  - absint, Arcticus, B&M, Bosch, BTC, Esterel, FZI, KIT, MDH, MES, UNIT

- **Traceability Solutions**
  - B&M, BTC, Esterel, KIT, Koc Univ., KTH, OFFIS, Scania

- **Integration**
Work Package Structure

Use Cases

System Engineering Methodology

- Scalable Zero Defect Analysis for Single Core
- Scalable Zero Defect Analysis for Multi Core
- Synthesis of Predictable Concurrent Systems

Dissemination, Exploitation and Standardisation

Management
Use Cases

Avionics
Airbus
Sagem
Thales

Automotive
Bosch
Daimler
Ford Otosan
NXP
Scania
VDL
...

Consumer Electronics
Arçelik
Ericsson
Havelsan