The CONCERTO project: a open source methodology for designing, deploying, and operating reliable and safe CPS systems

Silvia Mazzini, Intecs
The CONCERTO Project

ARTEMIS JU project
Call 2012
Technical Coordinator
Intecs
Partners 15
Countries 8
Start May 2013
End April 2016
Total cost 9,6 M €
CONCERTO Partners

- **Industrial Partners**
  - Thales Communications & Security (F)
  - EADS (F)
  - Oilfield Technology Group (N)
  - Aensys Informatikai (BU)
  - Intecs (I)
  - X/Open Company Limited - The Open Group (UK)
  - ATEGO (F)
  - AICAS (D)
  - CSW (P)

- **Research Centres**
  - ISEP (P)
  - SINTEF (N)

- **Universities**
  - University of Padua (I)
  - Maelardalen University (SW)
  - University of Florence (I)
  - Budapest University of Technology and Economics (BU)
CONCERTO Objectives

“Guaranteed Component Assembly with Round Trip Analysis for Energy Efficient High-integrity Multi-core Systems” - ARTEMIS JU Call 2012

- Correctness-by-construction for multicore systems through model-driven engineering
- Advanced hardware modelling capabilities
- Enhanced hierarchical, multi-domain component model
- Support for separation of concerns into the multi-domain, multicore environment
- Wider coverage of industrial domains

Building on the results of the CHESS project (ARTEMIS-2008-1-100022)
CONCERTO application areas

- Space
- Avionics
- Petroleum
- Medical
- Telecom
- Automotive
CONCERTO industrial use cases

- Medical by AENSys
- Petroleum by OTG
- Telecom by Intecs Telecom
- Automotive Multi-criticality Infotainment by Critical Software
- Automotive AUTOSAR conformance by Intecs
- Avionics by AIRBUS
- Space by Thales for Thales Alenia Space
- Space by AIRBUS for ASTRIUM SAT
Building on the CHESS technical approach

- A multi-view, hierarchical cross-domain design space for complex next generation platforms
- Correctness-by-construction, iterative and incremental development
- Hardware modelling facilities equipped for partitioned, mixed criticality and multicore platforms
- Early model-based analysis, with automated back propagation
- Automated code generation
- Run-time monitoring of non-functional properties
The Modeling Language

- Standard profile for System (and Requirements) Modeling
- Standard Unified Modeling Language
- Standard profile for Modeling and Analysis of Real-Time and Embedded Systems

Imports subsets of standard languages
- ✓ avoid redundancy
- ✓ fix semantic variation points

Integrates and extends standard OMG languages

Introduces a Dependability Profile
The component model

**Exposes a set of cohesive functional services**

A component is a *pure functional unit*

**Declares the functional services required from other components or the system to operate correctly**

**Declares the applicable extra-functional constraints and requirements in terms of annotations of its functional interface**

**The source code of components is pure sequential code.**

Extra-functional concerns are realized (and warranted) by the component model infrastructure.

**Reuse of components under different extra-functional concerns → increased reuse potential**

enables
CHESS container and connector

- Wrapper responsible for the declared extra-functional attributes (e.g. the realization of tasking, timing behavior, fault containment and fault tolerance)
  - Provides the component with a mediated connection with the execution platform and the system in general

- Addresses interaction concerns
- Decouples the component from the other end-point(s) of a communication
- Realizes connection properties (best-effort, at most once, exactly once)
- E.g. procedure/function call, remote message passing, I/O file operation, …
The CONCERTO process

1. You construct a PIM to represent your solution to your problem, independent of any specific implementation.

1-2a. Dependability/safety analysis is performed at PIM system/SW and platform specification level, with back propagation of analysis results.

2. You complement the PIM with information on the target platform and the deployment plan.

This is a feature-rich specification space for multicore HW!

3. Automated model transformation produces a PSM from the user PIM

4. Real-time relevant analysis is performed on the PSM

5-6. The analysis results are back propagated to the PSM and to the PIM

The PSM is read-only! The implementation product is guaranteed to be deterministic

7-8. The implementation is deployed to the HW, with run-time verification support if needed. Run-time monitoring is activated to grab live data for run-time monitoring analyses and back propagation of results, as in 5-6.

The user iterates the 1-6 cycle as many times as needed
Cross-domain Core Methodology

- Reaching the final version of the CONCERTO Methodology and Toolset
  - Consolidation of the CONCERTO Modelling Language and Multi-concern Component Methodology
    - Matlab/Simulink Synchronous Block Diagrams (SBDs) support
    - Inter-component interactions and end-to-end response time analysis
    - Multicore deployment
    - Timing analysis for multicore: scheduling and workload analysis
    - Dependability profile and analysis
    - Modeling criticality
    - Run-time monitoring, with back propagation
    - CONCERTO Failure Logic Analysis (FLA)
    - Extensions to State Based Analysis

- Migration to Polarsys/Maturation of the toolset
  - Most of the tools are delivered to Polarsys

Intecs
De-CPS Workshop  22 June 2015
Specialized and Domain-specific Features

- **Petroleum domain**
  - Modelling and analysis for monitoring of safety barriers of petroleum installations

- **Telecare domain**
  - Definition of a specific profile
  - Sirius integration in the CONCERTO framework
  - Dependability analysis
  - Code generation

- **Automotive domain**
  - AUTOSAR conformance
  - ASIL association
  - Mixed criticality for infotainment

- **Avionics Domain**
  - Conformance with the ARINC-653 IMA principles
MyCCM and ARTISAN

- **Transfer of CONCERTO concepts to MyCCM**
  - Extensions for modelling of component behaviour and execution environment
  - Enhanced MyCCM Generation Chain

- **Extensions to PTC’s Integrity Modeler**
  - Support to the CONCERTO Methodology
  - Target to MyCCM
Future Extensions

- **Within the AMASS Project**
  - Extensions of the contract-based approach
  - Formalization of multi concern assurance properties of the architectural components
  - Integration with the AMASS assurance framework and toolchain
  - Improve reuse support
Questions?