Model-based Design and Analysis of Cyber Physical Systems

Jalil Boudjadar, Simin Nadjm-Tehrani, Ingemar Söderquist

Outline

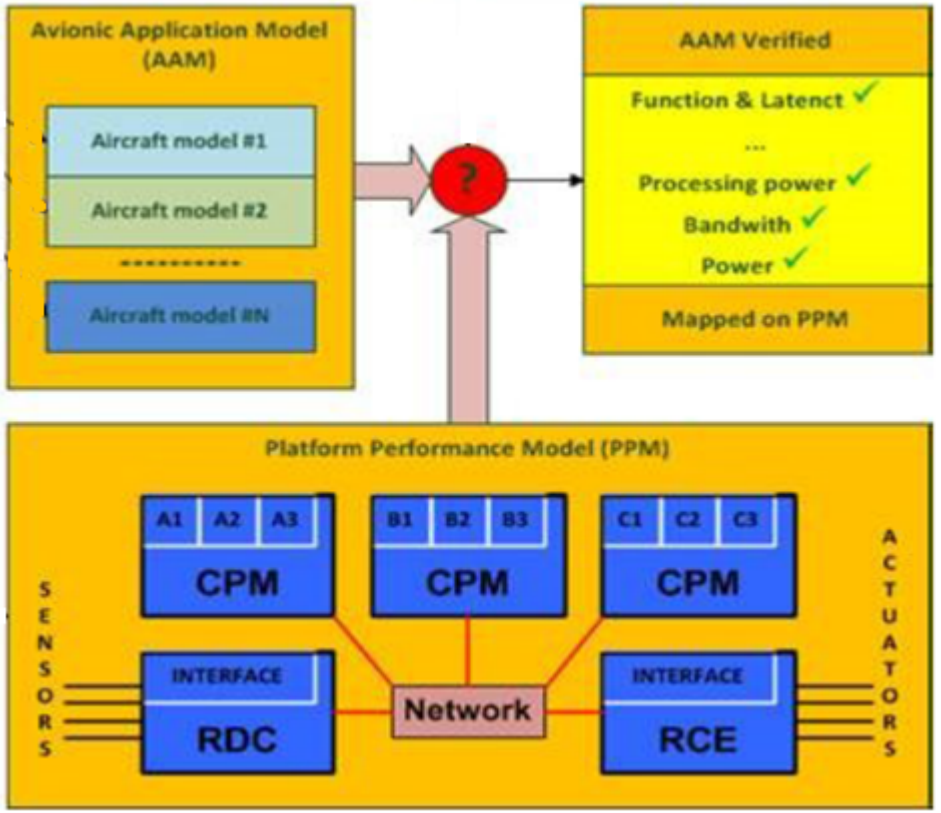
- Work context: NFFP6 project
- Modeling and analysis using Uppaal
- Modeling and analysis using AADL
- Intuitions for future avionic systems
- Conclusion

Work Context: NFFP6 Project

- Separation of platform and application descriptions.
- Model both elements at an early conceptual stage:
  - analysis is tractable;
  - design inconsistencies are discovered early.
- Scalable and formal analysis of performance and feasibility
- Exploit the analysis results of current platforms for future platforms.

Work Context: NFFP6 Project

- Use of model-based design to study design trade-offs.
- Investigation of methods and tools for high level description and automated analysis.
- Model different platform architectures: today's federated, forthcoming multicore, any emerging future platform.



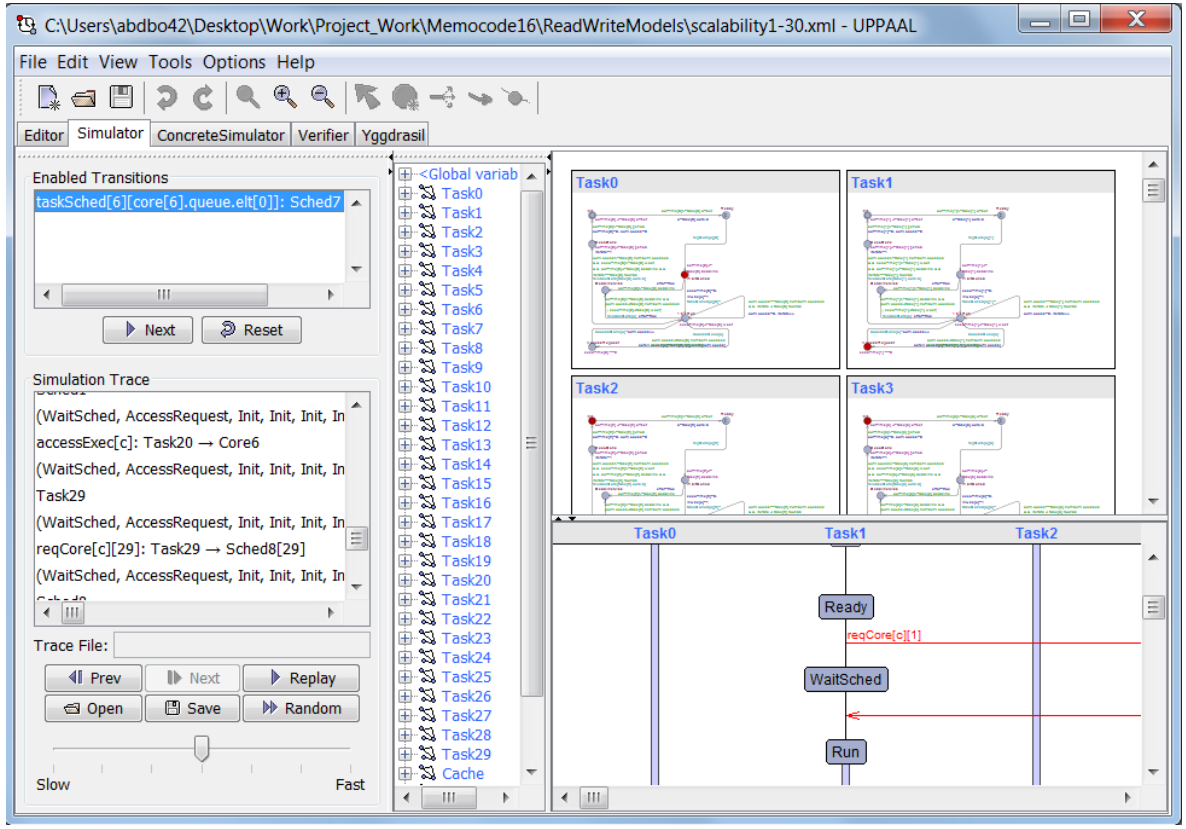
Current work

- Formal tool-supported design and analysis
  - Study the modularity and scalability of Uppaal for application deployment on a single node multicore platform.
- Model-based design using AADL
  - Understanding the benefits and limitations of the AADL descriptions and supporting tools for multi-node networked platforms.
- Provide methods to estimate shared resource access patterns and analyze utilization in a multicore setting.

Model-based design and Analysis of Avionic Systems using Uppaal

Uppaal Toolsuite

- Automata-based modular description.
- Simulation and formal verification.
- Reconfiguration and flexibility.

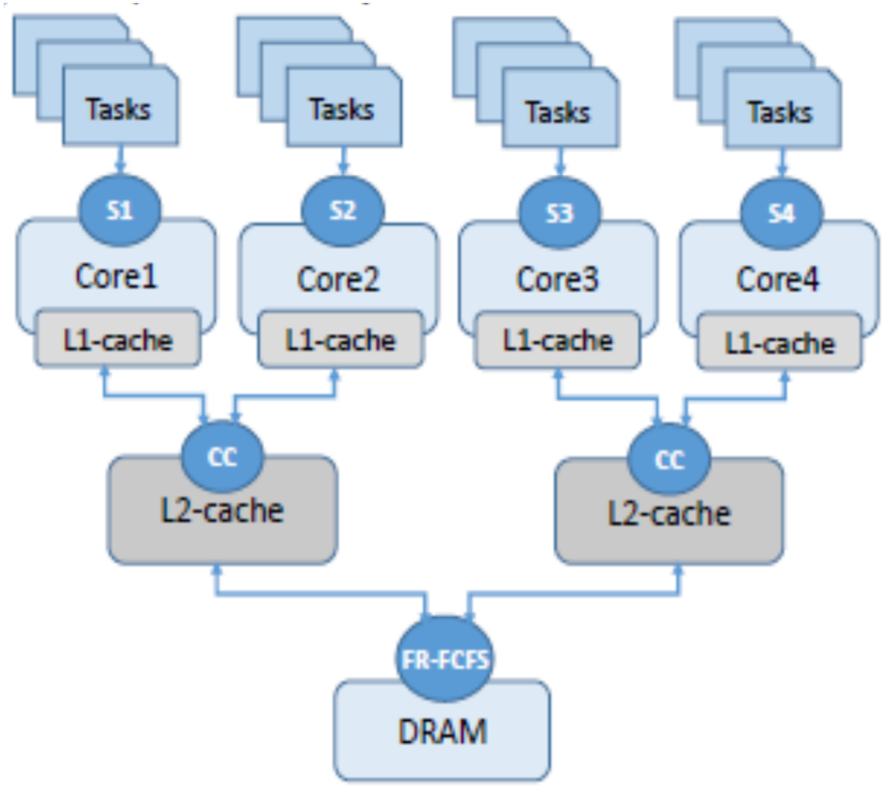


Model-based design and Analysis using Uppaal

- Multicore platforms with a hierarchy of memories (local caches, shared L2 cache and DRAM).
- Local scheduling at each core level.
- Application described by a set of periodic processes.
- Each process has parameters:
  - Worst case execution time (WCET)
  - Worst case resource access (WCRA).
- Outcome: Schedulability, core utilization and maximum interference per access to shared memories.

Reusable and reconfigurable frameworks

- Modular design.
- Statistical model checking for performance estimation.
- Case study size: Currently 30 tasks running on 8 cores.



Model-based design and Analysis of Avionic Systems using AADL

Model-based design using AADL

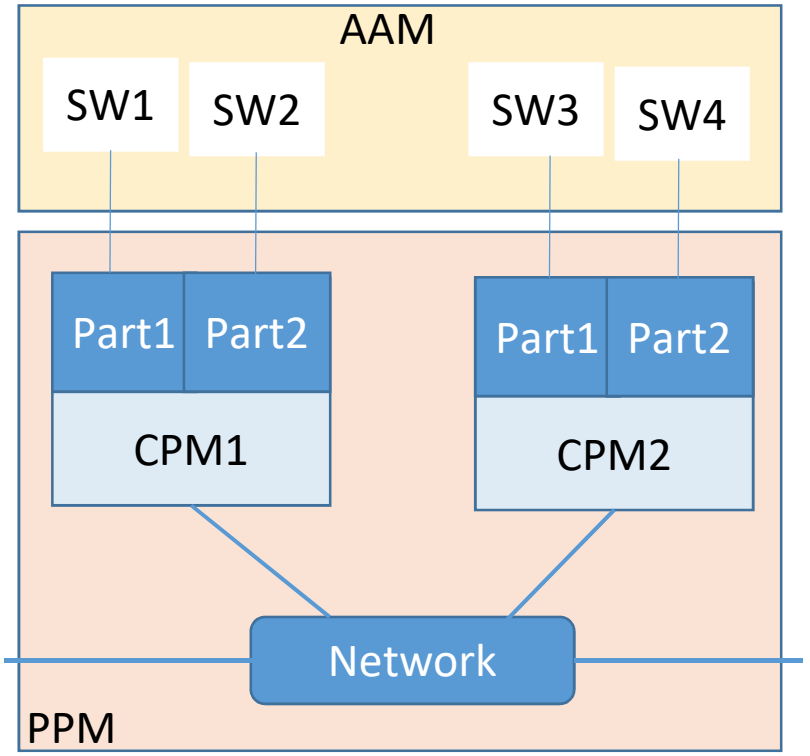
- AADL (Architecture Analysis & Design Language) is a modeling language to describe architectures and applications.
- Concepts to describe the computing and communication elements, and the software applications.
  - Independently!
- Flexible mapping of the application elements to the hardware.

AADL for Multi-processor Platform description

- Alternative design models as a proof of flexibility
  - Each CPM has a single core.
  - Each CPM is a multicore processor.
  - An imaginary future platform.
- Analysis of schedulability and performance using AADL Inspector tool.
- Study the scalability.

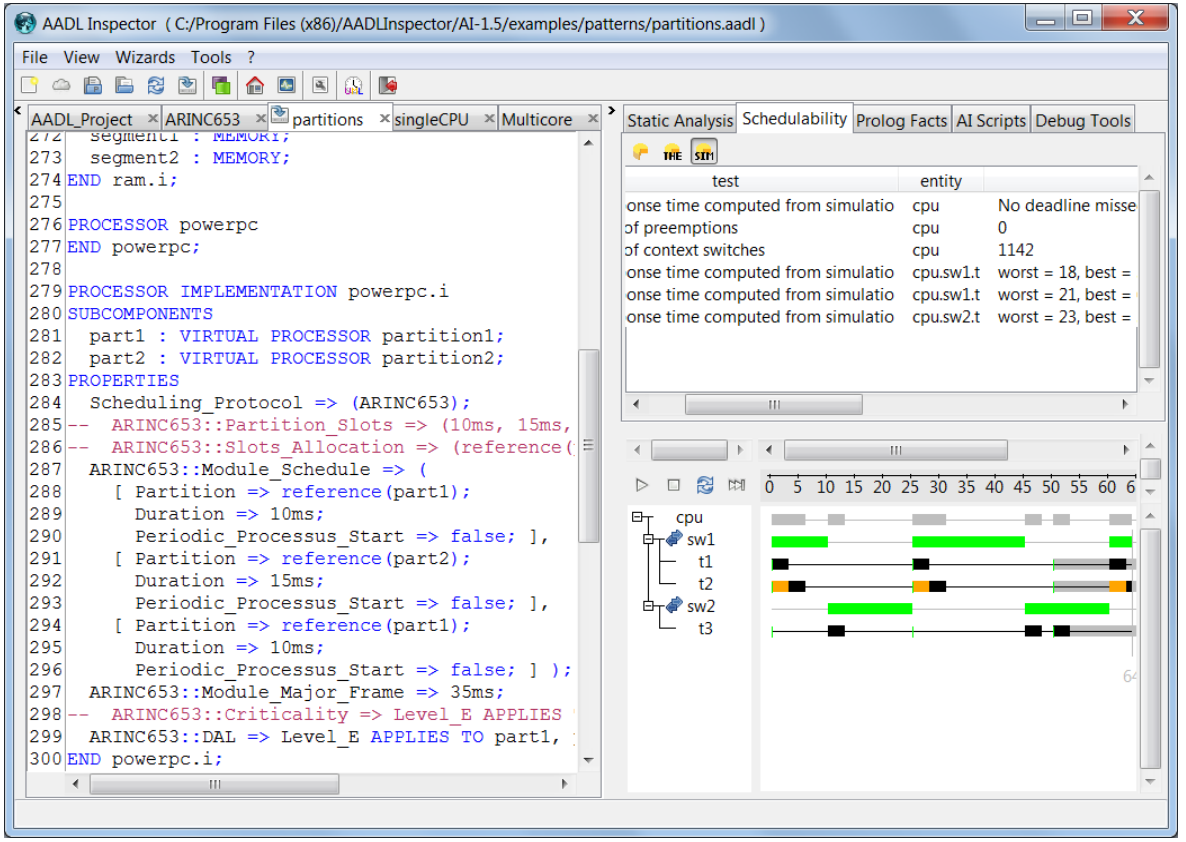
Multi-CPM single core platform

- PPM includes 2 CPMS and a network.
- Each CPM schedules 2 partitions using ARINC653.
  - major frame, criticality, partition slots
- AAM includes 4 SW applications, each consists of 2 threads.
- Threads are scheduled using a local scheduler (alternative algorithms).
- Bandwidth and latency constraints for network and individual connections.



AADL analysis tool: Inspector

- Execution simulation
- Schedulability analysis
- Processor utilization and response time analysis



Multi-CPM multicore networked platform

- Alternative design models as a proof of flexibility
  - Each CPM has a single core.
  - Each CPM is a multicore processor.
  - An imaginary future platform.
- Reuse the experience from the Uppaal study and add network characterization in AADL

Imaginary Future Avionic Platforms

Rough sketch of approach

- Goal: will the design decisions taken earlier for the original platform be suitable for the new platform?
  - Describe the future platform to some extent and reuse the application model in analysis.
  - Or, analyze the application using a current platform, relate the future platform to the current platforms and reuse the analysis process.

Summary

- Two different model-based tools to describe avionic systems.
  - Uppaal: timeliness
  - AADL: Engineer-friendly
- Two different types of architectures
  - Single processor or multicore & networked
  - Scalability studies ongoing…
- Challenge: identify future platform!

Questions?

www.ida.liu.se/~rtslab

- [1] Performance-aware scheduling of Multicore time-critical systems. J. Boudjadar, J. Kim, S. Nadjm-Tehrani. Memocode 2016.
- [2] A. Löfwenmark and S. Nadjm-Tehrani, Experience Report: Memory Accesses for Avionic Applications and Operating Systems on a Multi-core Platform. ISSRE 2015.

LINKÖPING UNIVERSITY

Challenges for future platforms

- The static time slot-based scheduling of ARINC653 may lead to non efficient utilization of the processing resources.
- It could be interesting, in the event of a hardware failure, to be able to reconfigure the system, which means reallocating functions to safe modules.