Whitepaper
A timing annex for the AADL

SAE/AADL meeting
Jacksonville, April 22-25., 2013

Loïc Besnard, CNRS

Thierry Gautier, Paul Le Guernic, Jean-Pierre Talpin, INRIA

Acknowledgements to Oleg, Peter, Jérôme, Etienne, Franck and Pierre
Whitepaper
A timing annex for the AADL

PLAN

Goal of the proposal
State of the art and background
A model of time and clock automata
Timing AADL concepts and annexes
Conclusion
A formal definition of the AADL in a synchronous multi-clocked model of computation and communication

- A formal, thorough and unambiguous specification of the AADL

- A framework for verification
  - Multi-clocked synchronous automata
  - Compatible with PSL use with CA and Maude

- A framework for implementation
  - Synthesis of reactive and control systems
  - Globally asynchronous locally synchronous architectures

- A pivot model of automata: behavioral annex, SyncCharts, StateCharts, StateFlow, Esterel, Mealy machines, …
Recommendations

Choose where a timing model best fits
  • core (property set)
  • annex (TA)
  • Review implications/links on/with annexes

  • Isolate synchronous subset/profile of AADL v2

Consensus
  • An abstract, relational, logical model of time
  • Define clock domains and protocols
  • Causal scheduling constraints between threads
  • Propose a refinement methodology (from clocks to ports)
A software-centric model of time

- A syntactically light-weight proposal
  - Time as sensed from software
  - Synchronization, causality, clocks, relations

- Based on Polychrony and the MARTE/CCSL standard

- How does it extend the AADL synchronous core?
- Implications on the behavioral annex
  - Model of reactive automata
  - Model of constrained automata (controller synthesis)
- Implication on the constraint annex
  - Expression of timing relations
  - Expression of regular expressions over time
Implications and (modular) containment

- Refines (or abstracts) core timing property specifications
- Implications on the behavioral annex (timed/clocked automata)
- Implications on the constraint annex (timing invariants)

- Compatibility with the ARINC annex (previous work)

- A possibly extensible proposal (as CCSL)
  - Abstraction/refinement between time domains
  - Hardware real-time (discrete)
  - Physical real-time (continuous)
Whitepaper
A timing annex for the AADL

PLAN

Goal of the proposal

State of the art
A model of time and clock automata
Timing AADL concepts and annexes
Workplan
State of the Art – Verification

• “Expressing and enforcing user-defined constraints of AADL models”. Olivier GILLES, Jerome HUGUES. IEEE ICECCS, 2010.


Definition of specification formalisms based on PSL to formally express and verify (synchronous) timing properties of AADL objects
State of the Art – Semantics


Definition of an implicitly synchronous subset or profile of the AADL amenable to formal verification
Background on AADL


Synchronous multi-clocked interpretation, simulation, verification and scheduling analysis
Background on CCSL


Controller synthesis from timing constraints