Towards the Integration of UPPAAL for Formal Verification of EAST-ADL Timing Constraint Specification

Tahir Naseer Qureshi,
DeJiu Chen, Magnus Persson, and Martin Törngren
Department of Machine Design.
KTH - The Royal Institute of Technology, Stockholm, Sweden. {tnqu, chen, magnper, martin@md.kth.se}
Presentation Outline

• Background
• Objectives and methodology
• Base technologies
  – EAST-ADL
  – UPPAAL
• Transformation scheme
• Results and Conclusions
Background

• Automotive system development
  – Paradigm shift

• Software and distributed computing
  – Innovations and features
  – Increased safety and performance

• Increased complexity
  – Life Cycle
    • Maintenance, product variability, information exchange across domains and enterprises
  – Run-time
    • Modes, dependencies ...
Background (Contd.)

- Technologies for system specification (UML, SysML, EAST-ADL, AADL, AUTOSAR etc.)
  - Requirements,
  - Functions, software / hardware
  - Behavior and non-functional constraints
  - Variability
  - Verification and validation
- Different views, concerns, scope
  - Consistency
  - Communication
  - Automation
- Tools and tool integration
Objectives

• To investigate
  – The support for formal verification of execution timing constraints by external tools
  – Automation possibilities

• To identify possible transformation scheme and challenges
Approach

- Case studies
  - Emergency Braking Assistant
  - Brake-by-wire

- Base technologies
  - EAST-ADL
  - UPPAAL

- Prototype transformation
  - MDWorkBench (MQL)

- Results
Behavior taxonomy

- Application logic and interaction
- Execution and timing
- Nominal vs. error
- Required vs. provided
- Discrete vs. continuous time
EAST-ADL

• Electronics Architecture and Software Technology
  – Architecture Description Language (2001 – present)
    – Addresses current industrial needs
    – Embraces de-facto standards
    – Complement best industrial practices
  – Tool Support
    • Specification tools (e.g. PapyrusUML)
    • External analysis tools (e.g. HIP-HOPS)
EAST-ADL (Contd.)
UPPAAL

- Uppsala and Aalborg Universities
- Industrial usage
  - Philips audio protocol, Gear controller by Mecel AB
- Timed Automata
  - Quantitative treatment of time
  - Easy and flexible modeling
- Formal verification
  - Modeling
    - Graphical and C like syntax
  - Simulation
    - Non-exhaustive analysis
  - Verification (Query Language)
    - CTL
      
A[] (ECU.TaskFinished imply ECU.Timer <= Deadline)
### EAST-ADL vs. UPPAAL

<table>
<thead>
<tr>
<th>UPPAAL</th>
<th>EAST-ADL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Function type</td>
</tr>
<tr>
<td>Process</td>
<td>Function prototype</td>
</tr>
<tr>
<td>States</td>
<td>Implicit</td>
</tr>
<tr>
<td>Transitions</td>
<td>Implicit</td>
</tr>
<tr>
<td>Channels</td>
<td>Implicit through connectors, execution events</td>
</tr>
<tr>
<td>Time guards and clocks</td>
<td>Timing constraints</td>
</tr>
</tbody>
</table>

**Contribution:**
Make explicit transformation

**Result:**
Transformation algorithm
Semi-automated transformation
EAST-ADL vs. UPPAAL
Transformation Scheme - 1

EAST-ADL::Design Function Type
  -->
UPPAAL::Template

Define a clock in the declaration of the new template.

clock LocalClock;
Transformation Scheme - II

- Create standard locations and transitions
  - Periodic

  ![Periodic Diagram]

  ![Aperiodic Diagram]
Transformation Scheme - III

- EAST-ADL::Timing
  - Period and execution time
- UPPAAL::Conditions & State Invariants
Transformation Scheme - IV

- EAST-ADL::FunctionPort
  -> UPPAAL::synchronization event
Transformation Scheme - V

- EAST-ADL::System (FDA) -> UPPAAL::system
- FunctionPrototype->UPPAAL::Process
- FunctionConnector -> UPPAAL::Channel

broadcast chan DesiredTorque;

ActFR=WActuator(ACComFR, stopClock2);

system BTC,GBC, ABSRR, ABSRL, ABSFL, ABSFR, ActFL, ActFR, ActRL, ActRR, TMFL, TMFR, TMRR, TMRL;
Transformation Scheme - VI

- Time logging for end-to-end timing constraint verification
  - Additional templates
    - $A[] \ (\text{TMRR.Finished \ imply \ (TMRL.TimerClock<300)})$
Transformation Prototype

- MDWorkBench and MQL
- Partially automatic
  - EAST-ADL EMF meta-model to UPPAAL EMF meta-model.
  - EMF to UPPAAL XML (manual)
BBW case verification

• Deadlock free
  – Only for sender-receiver interface
  – Client-server type for future enhancement

• Specification consistency
  – Execution time w.r.t period
  – End-to-end timing constraint w.r.t. local timing constraints
    • Reaction time ≤ 300ms
Summary

• One EAST-ADL and UPPAAL integration effort for verifying consistency of timing constraint specifications.
• Automated transformation possible but with challenges
  – Distributed information
  – Task allocation to hardware.
  – Multiple response times and event chains.
Future Work

• Supporting the upcoming EAST-ADL extension for native behavior specifications and the verification.

• Consistency checking between constraints specified at two different abstraction levels in EAST-ADL.

• Bi-directional transformation utilizing requirements to generate queries and V&V package for analysis results.
Questions