Model-Driven Analysis of Security, Reliability, Test, Privacy, Safety and Trust of IoE Services

Eugenio Villar
University of Cantabria
Agenda

- Introduction
- Single-Source Embedded Systems Design
- Model-driven Analysis of IoE Services
- Conclusions
Introduction

▪ Model-Driven Design (MDD)
  ▪ High-abstraction level
  ▪ Mature SW engineering methodology

▪ State-of-the-Art
  ▪ Matlab-Simulink
    ▪ Proprietary, only one MoC, M language
  ▪ CoFluent
    ▪ Proprietary, a few MoCs, C/C++ language
  ▪ Ptolemy II
    ▪ Academic, any MoC, C/C++ inside a Java block
  ▪ ...
Introduction

- UML
  - Standard, any (user-defined) MoC, any language
  - Natural way to capture system architecture

- Semantic lacks
- Domain-specific profiles
- MetaMorph
  - Commercial, any (user-defined) MoC, language agnostic
- CHESS
  - Open Source, any (user-defined) MoC, language agnostic
Introduction

UML DC DSLs
- Java, ...
- MPI, ...

UML Smartphone DSLs
- HTML5, ...
- Java, ...
- Dalvik VM, ...

UML ES DSLs
- C/C++, ...
- Autosar RTE

UML ES DSLs
- ADA, ...
- C/C++, ...
- MCAPI, ...
Single-Source Embedded System Design

- UML MARTE
- ADA,...
- C/C++,...
- MCAPI,...

- Trust
- Simulation
- Verification
- Performance Analysis
- Privacy

- Safety
- Security
- Architectural Mapping
- Sw Synthesis
- Hw Synthesis

HW Synthesis

SW Synthesis

PIM (App)

Architectural Mappings

Scenarios
Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind
Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind
Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind
Model-Driven Analysis of IoE Services

- UML/MARTE System Modeling Methodology
- Platform-Independent
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation
Model-Driven Analysis of IoE Services

- UML/MARTE System Modeling Methodology
- Platform-Independent
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation
- Reusable
- Flexible
- Analyzable
  - Security
  - Reliability
  - Test
  - Safety
  - Privacy, Trust...
Model-Driven Analysis of IoE Services

- Properties of the Provided Port
  - NotAttendedService
  - Retry

- Properties of the Interface Methods
  - concurrency
  - exekind
  - syncKind

- Properties of the Required Port
  - queueSize
  - FullPoolPolicy
Model-Driven Analysis of IoE Services

- **Function Call/RPC/RMI**

<table>
<thead>
<tr>
<th>Required Port</th>
<th>RtService</th>
<th>Provided Port</th>
<th>MoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotAttendedService</td>
<td>retry concurrency</td>
<td>exekind syncKind queueSize FullPoolPolicy</td>
<td></td>
</tr>
<tr>
<td>infiniteWait</td>
<td>none G or C rem.lm. sync.</td>
<td>none none</td>
<td>exactly once</td>
</tr>
<tr>
<td>infiniteWait</td>
<td>none G or C rem.lm. async.</td>
<td>none none</td>
<td>at most once</td>
</tr>
<tr>
<td>dynamic</td>
<td>none G or C rem.lm. sync.</td>
<td>none none</td>
<td>exactly once</td>
</tr>
<tr>
<td>dynamic</td>
<td>none G or C rem.lm. async.</td>
<td>none none</td>
<td>at most once</td>
</tr>
<tr>
<td>timedWait 0</td>
<td>G or C rem.lm. sync.</td>
<td>none none</td>
<td>exactly once</td>
</tr>
<tr>
<td>timedWait 0</td>
<td>G or C rem.lm. async.</td>
<td>none none</td>
<td>at most once</td>
</tr>
<tr>
<td>timedWait &gt; 0</td>
<td>G or C rem.lm. sync.</td>
<td>none none</td>
<td>at least once</td>
</tr>
<tr>
<td>timedWait &gt; 0</td>
<td>G or C rem.lm. async.</td>
<td>none none</td>
<td>maybe once</td>
</tr>
</tbody>
</table>

- **Rendezvous**

<table>
<thead>
<tr>
<th>Required Port</th>
<th>RtService</th>
<th>Provided Port</th>
<th>MoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotAttendedService</td>
<td>retry concurrency</td>
<td>exekind syncKind queueSize FullPoolPolicy</td>
<td></td>
</tr>
<tr>
<td>infiniteWait</td>
<td>none G or C rem.lm. rendezvous</td>
<td>none none</td>
<td>CSP</td>
</tr>
<tr>
<td>timedWait 0</td>
<td>G or C rem.lm. rendezvous</td>
<td>none none</td>
<td>RV</td>
</tr>
<tr>
<td>timedWait &gt; 0</td>
<td>G or C rem.lm. rendezvous</td>
<td>none none</td>
<td>RV</td>
</tr>
</tbody>
</table>
Model-Driven Analysis of IoE Services

- Data-Flow

<table>
<thead>
<tr>
<th>Required Port</th>
<th>RtService</th>
<th>Provided Port</th>
<th>MoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>notAttendedService</td>
<td>retry</td>
<td>concurrency</td>
<td>exekind</td>
</tr>
<tr>
<td>infiniteWait</td>
<td>none</td>
<td>G or C</td>
<td>deferred</td>
</tr>
<tr>
<td>infiniteWait</td>
<td>none</td>
<td>G or C</td>
<td>deferred</td>
</tr>
<tr>
<td>dynamic</td>
<td>none</td>
<td>G or C</td>
<td>deferred</td>
</tr>
<tr>
<td>timedWait</td>
<td>0</td>
<td>G or C</td>
<td>deferred</td>
</tr>
<tr>
<td>timedWait</td>
<td>&gt; 0</td>
<td>G or C</td>
<td>deferred</td>
</tr>
</tbody>
</table>

- Discrete-Event/Time-Triggered/Timed Data-Flow

<table>
<thead>
<tr>
<th>Required Port</th>
<th>RtService</th>
<th>Provided Port</th>
<th>MoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>notAttendedService</td>
<td>retry</td>
<td>concurrency</td>
<td>exekind</td>
</tr>
<tr>
<td>dynamic</td>
<td>none</td>
<td>G or C</td>
<td>rem.Im.</td>
</tr>
</tbody>
</table>
Conclusions

▪ The IoE demands new CPSoS design methods and tools
▪ Model-Driven system design is a powerful candidate
  ▪ A CPSoS system modeling language is required
  ▪ Supporting Mega-Modeling
  ▪ Analysis & design of the whole IoE service
▪ Single-Source Approach