Formal Verification of Device State Chart Models

Original

Availability:
This version is available at: 11583/2402456 since:

Publisher:
IEEE Computer Society

Published
DOI:10.1109/IE.2011.36

Terms of use:
openAccess
This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)
Formal Verification of Device State Chart Models

Fulvio Corno, Muhammad Sanaullah
Outline

- Design process
- Formalisms
- Verification Methodology
- Results
- Conclusions
Design process for IE

- Intelligent environments gaining acceptance
  - More installations
  - Standard solutions
- Need more structured design process
  - Less “art”
  - More “engineering”

Diagram:
- Requirements → Validation
- Analysis, Design → Verification
- Project → Simulation
- Implementation → Emulation
- System
  - HW
  - SW
Reference model

- **Devices**
  - Sensor
  - Meter
  - Actuator
  - Bus
  - Wearable
  - Wireless

- **Middleware**
  - Access point
  - Protocols
  - Gateway
  - Model
  - Framework

- **Intelligence**
  - Agents
  - Fuzzy
  - Rules
  - Algorithm

- **User Interface**
  - Wall switch
  - Tangible
  - PC
  - Smartphone

Formal Verification

IE'2011, Nottingham UK
General Goals

- Adopt **formal representations** to allow a sound design process
- Enable validation and verification **throughout** the design process
- Integrate the solution in the Dog2.1 gateway toolset
## Adopted formalisms

<table>
<thead>
<tr>
<th>Level</th>
<th>Design artifact</th>
<th>Technique</th>
<th>Formalism</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td>System requirements</td>
<td>Temporal Logics</td>
<td>UCTL</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Intelligent algorithms</td>
<td>State machines</td>
<td>UML Statecharts</td>
</tr>
<tr>
<td>Middleware</td>
<td>Device categories</td>
<td>Ontology</td>
<td>DogOnt classes</td>
</tr>
<tr>
<td></td>
<td>System configuration</td>
<td>Ontology</td>
<td>DogOnt instances</td>
</tr>
<tr>
<td>Devices</td>
<td>Device models</td>
<td>State machines</td>
<td>UML Statecharts</td>
</tr>
<tr>
<td></td>
<td>Whole system behavior</td>
<td>Parallel state</td>
<td>UML Statecharts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machines</td>
<td></td>
</tr>
</tbody>
</table>
The DogOnt ontology

Formalism
- UCTL
- UML Statecharts
- DogOnt classes
- DogOnt instances
- UML Statecharts
DogOnt instances: DimmerLamp

Formalism
- UCTL
- UML Statecharts
- DogOnt classes
- DogOnt instances
- UML Statecharts
Overall system components

...to be continued...
Device modeling

- Ontologies are declarative formalisms: device properties
- For device behavior we need an operational formalism
  - Statecharts (Harel, 1987, now in UML 2.0)
Use cases

- Ontologies are declarative formalisms: device properties
- For device behavior we need an operational formalism
  - Statecharts (Harel, 1987, now in UML 2.0)
- We use Statecharts for
  - Modeling the behavior of each device type
  - Implementing the **Intelligent Algorithms** within the gateway
  - Building a **whole-system model** allowing simulation and emulation
- Statecharts have a formal semantics: formal verification is possible
Overall system components

Formal Verification

IE'2011, Nottingham UK
Overall system components

...to be continued...
Temporal logic

- **UCTL logic**
  - Branching-time
  - State-based and action-based
- **Operators**
  - Next (X,N)
  - Future (F)
  - Globally (G)
  - All (A)
  - Exists (E)
  - Until (U)

**Examples**

\[ AG[\text{openRequest}(T1)] \]
\[ A \left[ T \{ \neg \text{openRequest}(T1) \} U \{ tsDone(T1) \} \right] \]

\[ AG[\text{daDoorOpen}(DAExt)] \]
\[ A \left[ T \{ \neg \text{daDoorOpen}(DAInner) \} U \{ \text{extDoorClosed}() \} \right] \]

**Formalism**

- UCTL
- UML Statecharts
- DogOnt classes
- DogOnt instances
- UML Statecharts
- UML Statecharts
Overall system components

System requirements

DogOnt

Device Statechart

Whole Environment Model

Composition

Whole System Model

Emulation

Composition

Load model

System Configuration

Gateway

Sense & Control

Real devices

Intelligent Algorithms

Run

Formal Verification Simulation
But… (goal of this paper)

- Formal verification relies on the composition of device state charts
- Environment control relies on information in DogOnt device properties
- How to ensure their consistency?
- Solution: use formal verification, too
The problem
The problem

- Naming consistency for **states**
- Naming consistency for **commands**
- Naming consistency for **notifications**
- Acceptance of commands
- **Reachability** of declared states
- **Generation** of declared notification
- Range of numeric status variables
Approach

- From DogOnt, extract UCTL properties
- From DogOnt, build a synthetic environment for the device
- Integrate Device State Chart in the synthetic environment
- For every property
  - Run Model checker
Approach

- From DogOnt, extract UCTL properties
- From DogOnt, build a synthetic environment for the device
- Integrate Device State Chart in the synthetic environment
- For every property
  - Run Model checker

Building a closed system model, ready for verification

Device Statechart

Closed system model

Model Checking

OK

ERR

Environment

Device

Environment Generate Commands (EGC)

Environment Receive Notifications (ERN)
Approach

Example: DimmerLamp generated & verified properties

--- Action Properties
  --- the acceptance of all the commands in DSC
    EF {sending(stepDown)} true
    EF {sending(stepUp)} true
    EF {sending(set)} true
    EF {sending(off)} true
    EF {sending(on)} true

  --- the generation of all the notifications in DSC
    EF {sending(stateChanged)} true
    EF {accepting(stateChanged)} true

--- State Properties
  --- the reachability of all the states in DSC
    EF (offState)
    EF (onState)
    EF (LightIntensityState)
Experimental Results

- UCTL Model Checker
- Dog2.1 standard device classes
- Device classes verified: 11
- Number of verifies properties: 114
  - Some design errors found and corrected
- CPU time: < 1 sec / property

- Formally validated device statechart library in Dog2.1
Conclusions

- Engineering the Design Process for Intelligent Environments
- Formalisms and tools are needed
- Ontologies, Statecharts, Temporal Logics

http://elite.polito.it
http://domoticdog.sourceforge.net
fulvio.corno@polito.it