Design Time Methodology for the Formal Modeling and Verification of Smart Environments

**Tutor:** Prof. Fulvio Corno

Muhammad Sanaullah

4° year (25° Cycle)
Smart Environment (SmE)

- The **environment** which is richly integrated with multitude of **devices** and performs operations, in an **intelligent manner**, by considering the actions and presences of **users** is known as Smart Environment (SmE).

- The **major objective** is to enable the environment to **provide ease and comfort to the users**.
Basic Components of SmE

- Users
- Devices
- Decision Logic
- Environment

<table>
<thead>
<tr>
<th>Planning/Execution</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals</td>
<td>Users</td>
</tr>
<tr>
<td>Actions</td>
<td>Input/Sensing Devices</td>
</tr>
<tr>
<td>Decisions</td>
<td>Decision Logic</td>
</tr>
<tr>
<td>Operations</td>
<td>Operating Devices</td>
</tr>
</tbody>
</table>

Design Time Methodology for the Formal Modeling and Verification of Smart Environments
Research Challenges (Users)

- **Users interact** with the SmE in their own ways which, in turn, responds according to the specified and modeled behaviors.

- The **level of details** and sophistication varies from system to system, context to context and goals to goals.

- User identification (**UI**): the identification of the user through sensing and/or input devices;
- User actions history (**UH**): the stored history of previous user actions;
- User privileges – on the basis of their roles – (**UPr**): based on the role categorization, the system functionality provision granted to the user;
- User position – pre- and post-action execution – (**UP**): the geographical location of the user within the system boundaries with respect to a specific action;
- User’s possible actions (**UA**): the actions of the user which can be contemplated and facilitated by the system;
- User’s possible behaviors (**UB**): the behavior (related to movement and context-approved actions) of the user which can be contemplated and facilitated by the system
Research Challenges (Devices)

- Devices range from simple (e.g. lamp) to complex (e.g. TV)
- Heterogeneous nature by having some common and distinguish functionalities
- Allow specific **functionalities** by accepting relevant acceptable **commands** at some certain **states**
- Devices may have some inner constraints
  - (e.g. TV volume is can not be increased from 100%)
- Devices functionalities may be parallel in their behavior
- Interface Information
- Behavior Information
Research Challenges (Decision Logic & Environment)

- Control the interaction among the associated devices
- Imposed constraints, on the system (SmE), are considered
- Received Input commands, make decision about the output action
- Send commands to the relevant output devices for performing the specific functionality
- On the acceptance of any notification decides what to do next
- Firewall:
  - Filtered irrelevant commands
- Users location identification
- Devices current state identification
Motivation for the adoption of Formal Methods

- The **intricate communication** among the components along with **satisfaction of varied natured constraints** introduced a high degree of complexity, in-result the likelihood of error may increase.

- Due to their sensitive implementation scenarios (e.g. homes, hospitals, offices, industries, airports or railways) the **reliance** on these systems demands **consistent behavior**.

- The **reliable behavior** of such system can be **ensured** by using **modeling and verification** approaches, which help in **identifying and correcting the errors** in early design stages of the system.

- Of the many available modeling and verification techniques, **formal methods** appear to be the most promising.
Adopted Incremental Strategy

- Devices Verification
- IDE Verification
- SmE Verification
- A comprehensive compression with state-of-the-art
- Satisfaction of High-Level SmE Goals
Devices verification

- Consistency Verification
  - Ontology Modeling
  - Statechart Modeling

- Reliable Behavior Verification
  - Statechart Modeling

---

IDE & SmE Verification

- **Main Components**
  - Devices
  - Decision/Control Logic
  - Users
  - Environment/Context

- **A generic methodology**
  - modeling and verification of SmE

- **Verification**
  - Interaction
  - Control
  - Context
  - Safety
  - Security

- **Extended case study of Bank Door Security Booth System (BDSB)**


A comprehensive comparison with state-of-the-art

- Comparison by proposing
  - Parameter-Based Empirical Methodology

- Focusing on the adopted modeling and verification State-of-the-art
  - Covering Aspects
  - Uncovered Areas
  - Employed Tools

Satisfaction of High-Level SmE Goals

- Relate to acquiring the functionalities of a single device or a group of devices

\[ G \xrightarrow{\mathcal{E}(g)} G' \]

\[ \mathcal{E}(g) = \{e(d_1), e(d_2), \ldots e(d_m)\} \]

\[ \frac{\{c_i [g_i] / a_i\}}{s} \rightarrow \frac{\{c_{i+1} [g_{i+1}] / a_{i+1}\}}{s'} \rightarrow \frac{\{c_n [g_n] / a_n\}}{s''} \rightarrow \ldots \]

\[ \frac{\{c_n [g_n] / a_n\}}{d_s} \rightarrow \]

License

- This work is licensed under the Creative Commons Attribution- Noncommercial- Share Alike 3.0 Unported License.

- To view a copy of this license, visit [http://creativecommons.org/licenses/by-nc-sa/3.0/](http://creativecommons.org/licenses/by-nc-sa/3.0/) or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.
Thank you!