Politecnico di Torino
Dipartimento di Automatica e Informatica
Torino, Italy

e-Lite
http://elite.polito.it

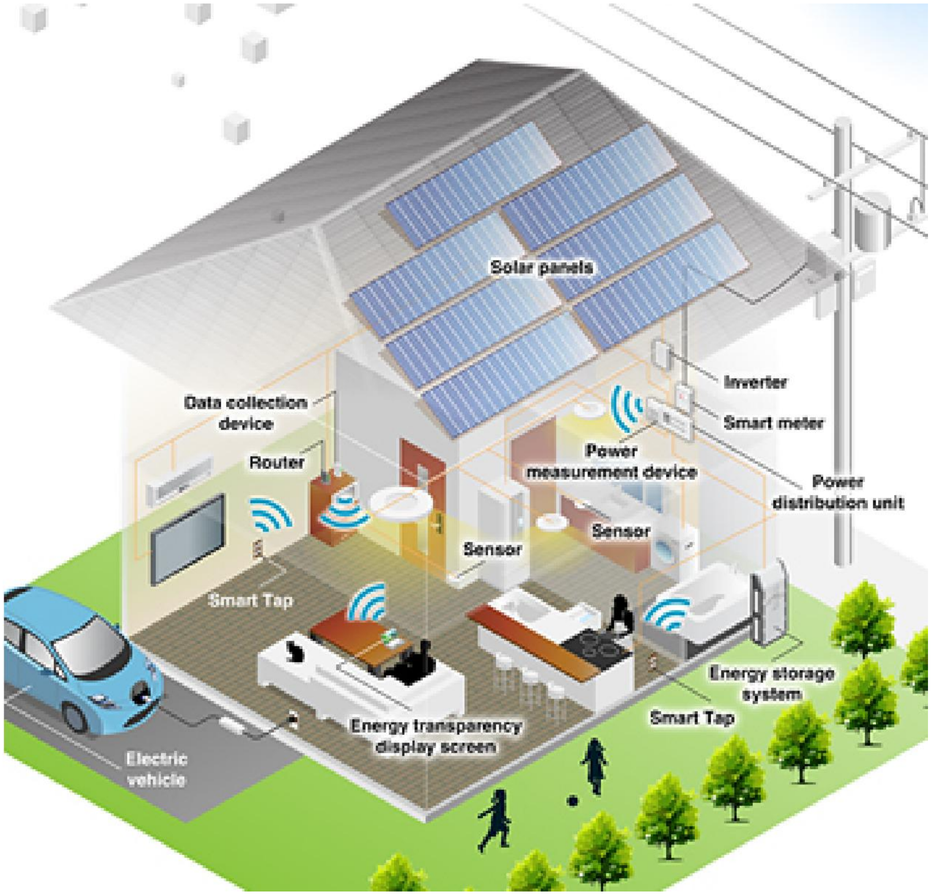
Design Time Methodology for the Formal Modeling and Verification of Smart Environments

Tutor: Prof. Fulvio Corno

Muhammad Sanaullah
4° year (25° Cycle)

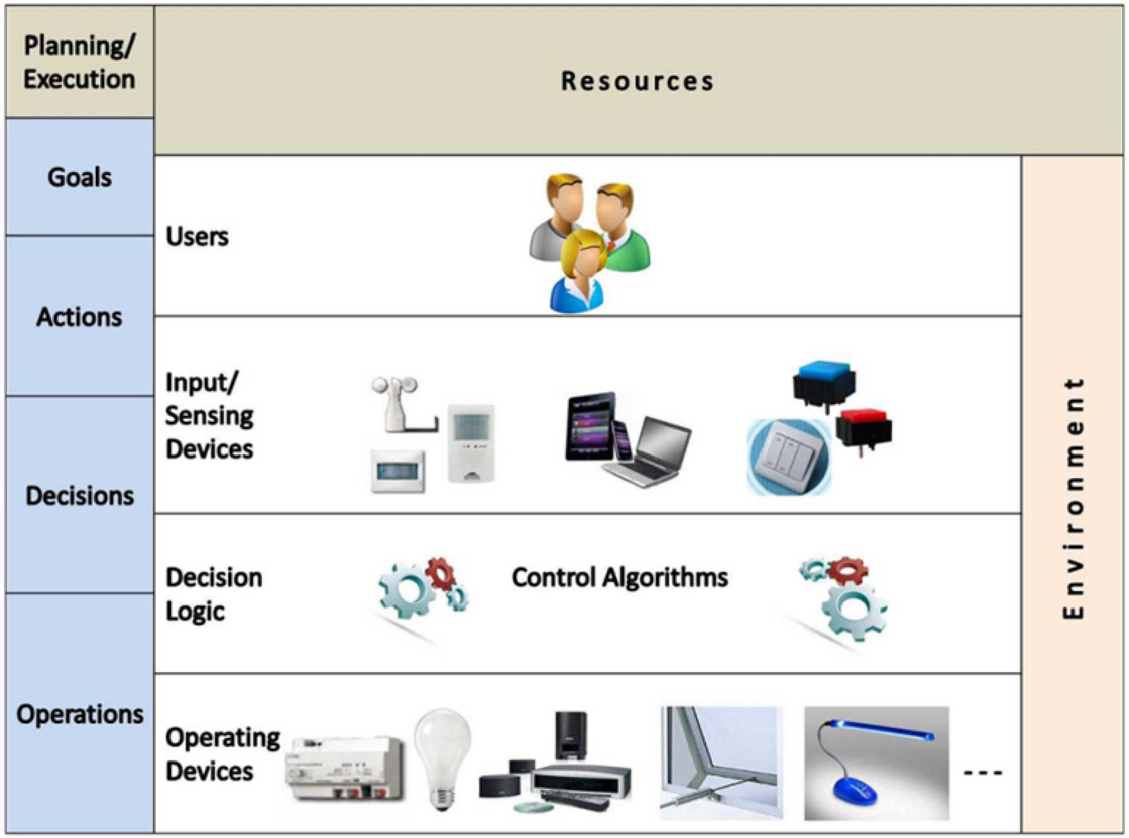
Smart Environment (SmE)

- 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



Planning/ Execution

Resources

Goals

Actions

Decisions

Operations

Users

Input/ Sensing Devices

Decision Logic

Control Algorithms

Operating Devices

Environment

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

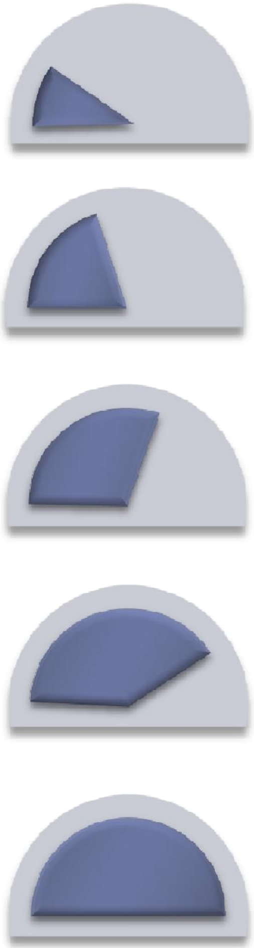
Devices Verification

IDE Verification

SmE Verification

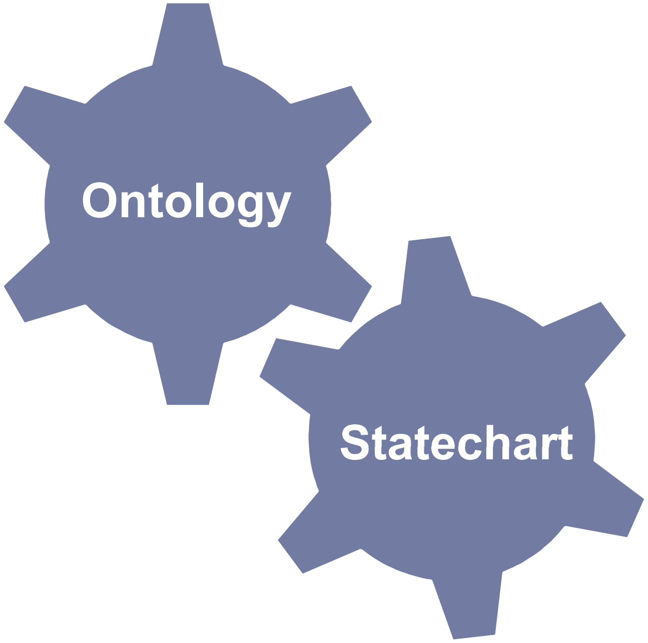
A comprehensive compression with state-of-the- art

Satisfaction of High-Level SmE Goals



Devices verification

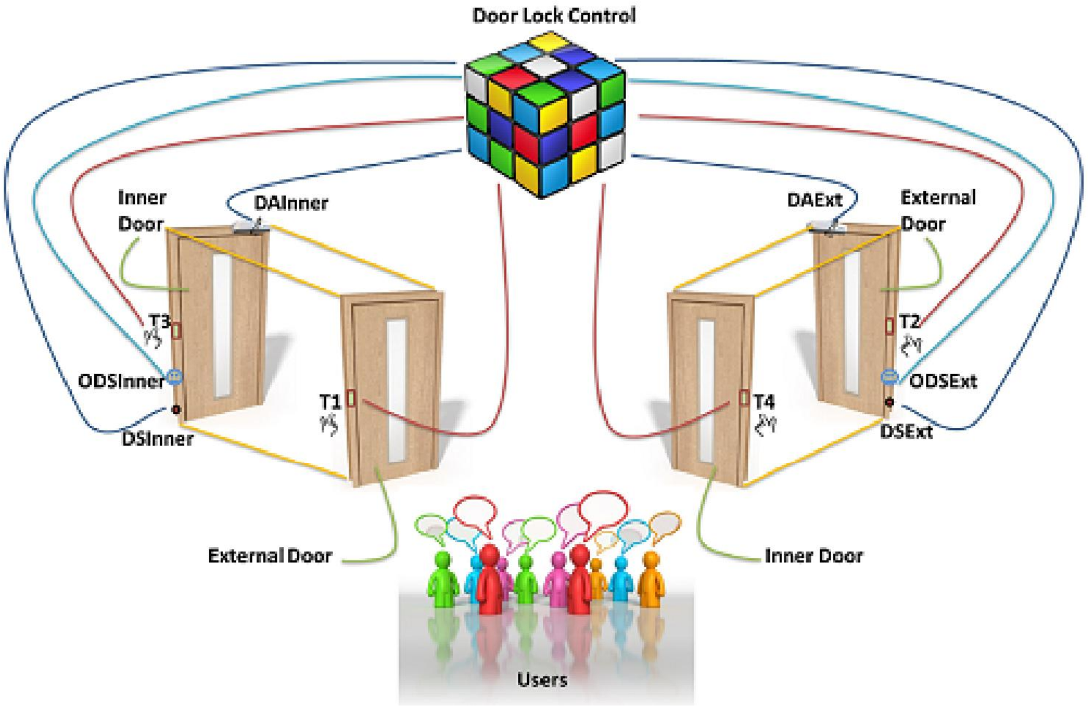
- Consistency Verification
  - Ontology Modeling
  - Statechart Modeling
- Reliable Behavior Verification
  - Statechart Modeling



1. Fulvio Corno, **Muhammad Sanaullah**, "*Formal Verification of Device State Chart Models*", IEEE Computer Society (USA), The 7th International Conference on Intelligent Environments, Nottingham (UK) 25-28 July 2011, page no. 66 to 73, ISBN: 9780769544526, DOI:10.1109/IE.2011.36

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)

2. Fulvio Corno, **Muhammad Sanaullah**, "*Design time Methodology for the Formal Verification of Intelligent Domotic Environments*", In: Ambient Intelligence- Software and Applications, Springer Berlin (DEU), International Symposium on Ambient Intelligence, Salamanca (ES) 6 - 8 April 2011, pp. 8, 2011, Vol. 92, page no. 9 to 16, ISBN: 9783642199363, DOI:10.1007/978-3-642-19937-0_2

3. Fulvio Corno, **Muhammad Sanaullah**, "*Modeling and Formal Verification of Smart Environments*", In: Hangbae C, Lee D, Overill R (ed) Special Issue: **Human-centric Security Service and Its Application** in Smart Space, **Security and Communication Networks**, 2013, pages 17, DOI: 10.1002/sec.794.

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

4. Fulvio Corno, **Muhammad Sanaullah**, "*Design-Time Formal Verification for Smart Environments: An Exploratory Perspective*", Journal of Ambient Intelligence and Humanized Computing, 2013, pages22, DOI: 10.1007/s12652-013-0209-4

Satisfaction of High-Level SmE Goals

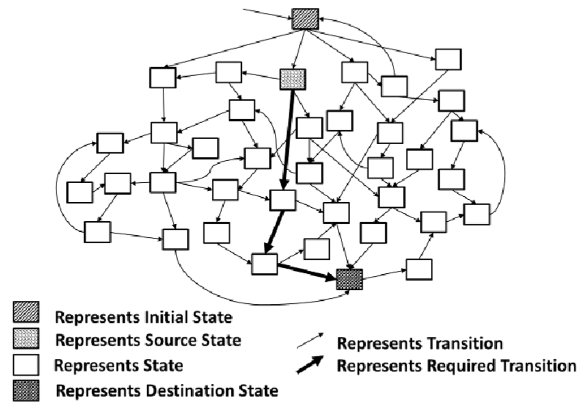
- Relate to acquiring the functionalities of a single device or a group of devices

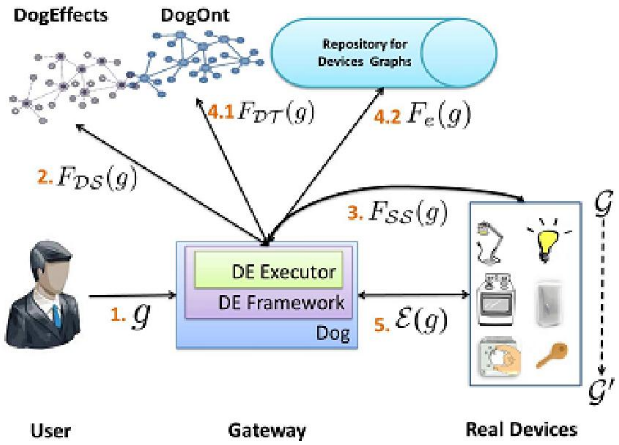
$$\mathcal{G} \xrightarrow{\mathcal{E}(g)} \mathcal{G}'$$

$$\mathcal{E}(g) = \{e(d_1), e(d_2) \dots e(d_m)\}$$

$$ss \xrightarrow{\{c_i[g_i]/a_i\}} s' \xrightarrow{\{c_{i+1}[g_{i+1}]/a_{i+1}\}} s'' \dots$$

$$\xrightarrow{\{c_n[g_n]/a_n\}} ds$$


▨ Represents Initial State
▨ Represents Source State
□ Represents State
▨ Represents Destination State
Represents Transition
Represents Required Transition



5. **Muhammad Sanaullah**, Fulvio Corno, Faisal Razzak, "*Automatic Device Activation Regarding High-Level Goals in Smart Environments*", Journal of Ambient Intelligence and Smart Environments, 2013, pages 23 (Accepted).

License

Thank You!