Institut
Mines-Telecom

Making Modeling Assumptions an Explicit Part of Real-Time Systems Models

Pierre de Saqui-Sannes - ISAE-SUPAERO
Ludovic Apvrille - Telecom ParisTech

ERTS 2016, Toulouse, France
January 27, 2016

Outline

TELECOM ParisTech

Rationale

- A model abstracts a system
  - Mastering the complexity of real-time systems
- A model is valid for a precise set of assumptions about the system and the system's environment
- A model should always be associated with the assumptions the designer has made to build up it
  - When the model evolves, the assumptions should evolve accordingly
  - And reciprocally

Our contribution

Making the modeling assumptions a full part of the model

Our Contribution

Objectives

- Solution not restricted to one modeling language
- Supports incremental modeling methods and versioning
- **Language**, **method**, **tool**

Our solution

- A new diagram: Modeling Assumption Diagram (MAD) added to SysML-Sec
- Assumptions attributes
- Relations between modeling assumptions
- Supported by a free and open-source tool (TTool)
  - http://ttool.telecom-paristech.fr
- Case study: a UAV

MAD: Assumption Stereotype

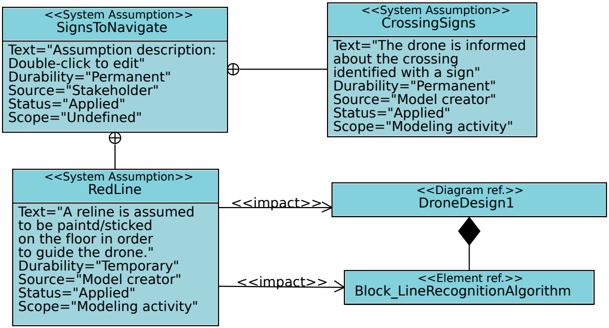
- **Stereotype** = system, environment
- **Durability** = temporary, permanent
- **Status** = applied, alleviated
- **Source** = end-user, stakeholder, creator of the model
- **Scope** = language, tool, modeling activity, verification

<<System Assumption>>
CrossingSigns

Text="The drone is informed about the crossing identified with a sign"
Durability="Permanent"
Source="Model creator"
Status="Applied"
Scope="Modeling activity"

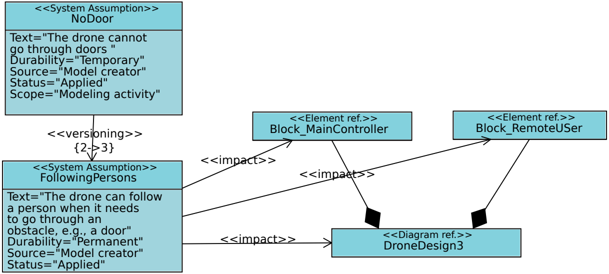
MAD: Relations

- **Containment**: a high-level assumption split up into elementary ones
- **Impact**: model elements impacted by a given assumption



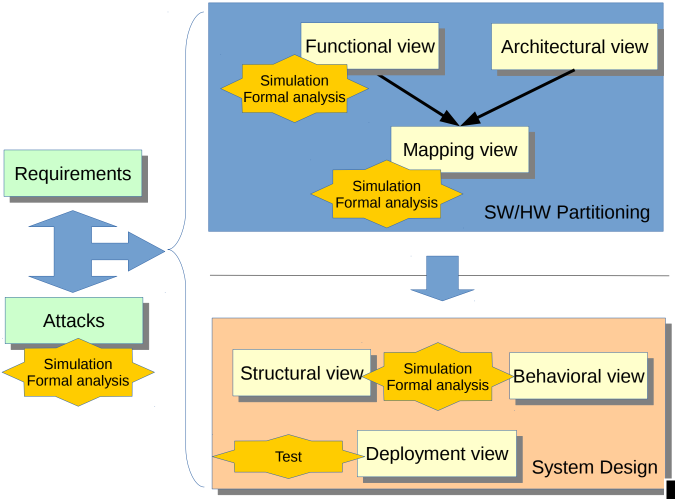
MAD: Relations (Cont.)

- Modification of assumptions → Modification of the system model
- Tracing (i) the versions of assumptions, and (ii) how the versions impact the system model
- **Versioning** relation: a applies until version x and becomes b at version y

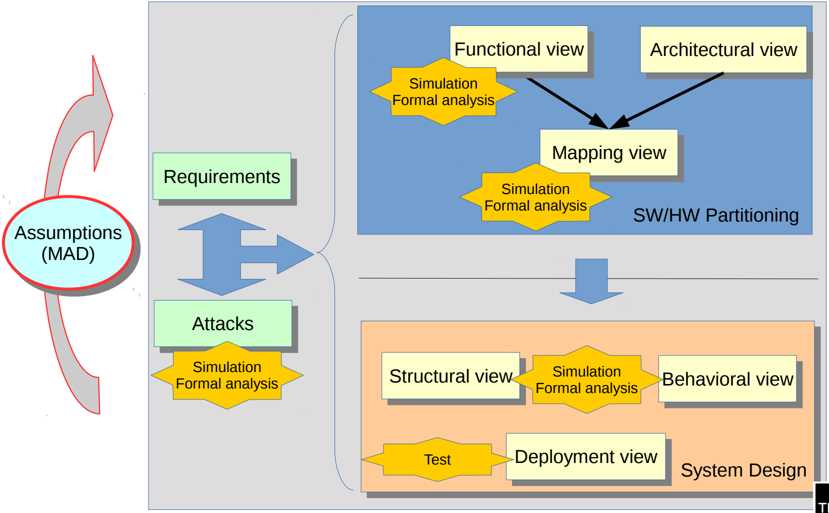


TELECOM ParisTech

Method


Functional view
Architectural view
Simulation
Formal analysis
Mapping view
Simulation
Formal analysis
SW/HW Partitioning
Requirements
Attacks
Simulation
Formal analysis
Structural view
Simulation
Formal analysis
Behavioral view
Test
Deployment view
System Design

Method


Assumptions (MAD)
Requirements
Attacks
Simulation Formal analysis
Functional view
Architectural view
Simulation Formal analysis
Mapping view
Simulation Formal analysis
SW/HW Partitioning
Structural view
Simulation Formal analysis
Behavioral view
Test
Deployment view
System Design

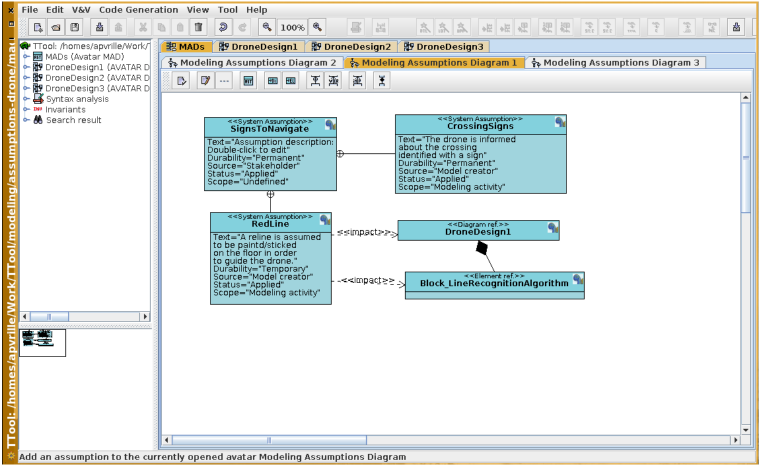
An Autonomous UAV

Autonomous drone navigation in harsh conditions, in particular inside buildings

3 scenarios (with different assumptions)

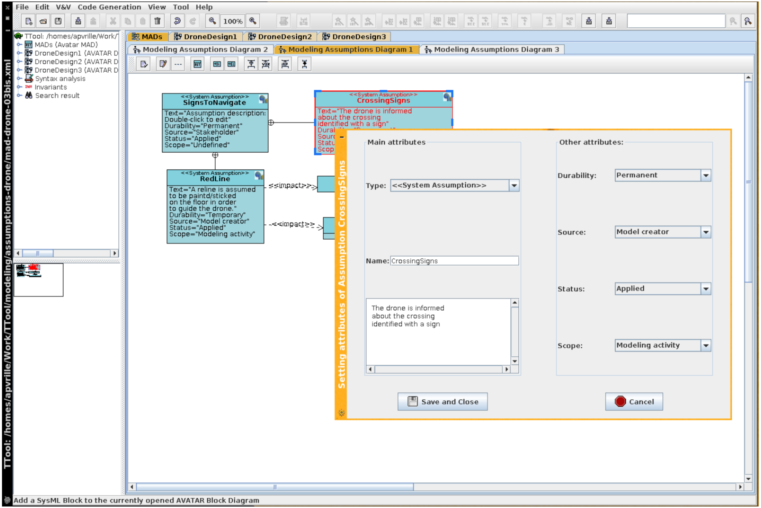
1. **Understanding marks**, e.g., a red line located on the floor
2. **Analyzing the environment** (obstacles, etc.) with image-based processing techniques (3D reconstruction).
3. **Going through obstacles with human assistance**
   - Entering in a room when the entrance door is closed.

TTool: MAD Scenario #1



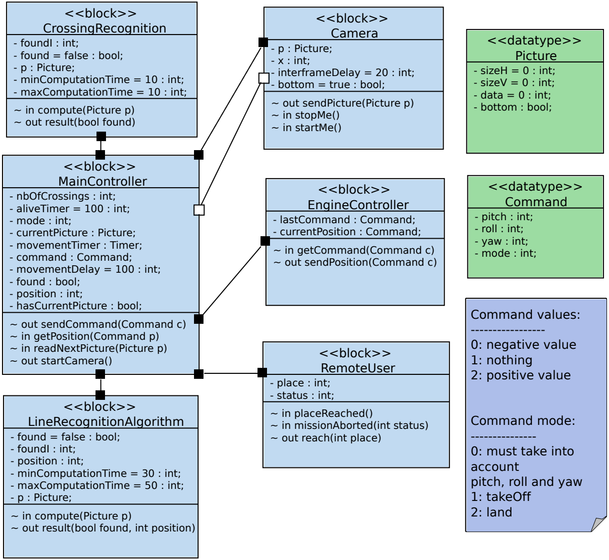
TELECOM ParisTech

TTool: Editing an assumption



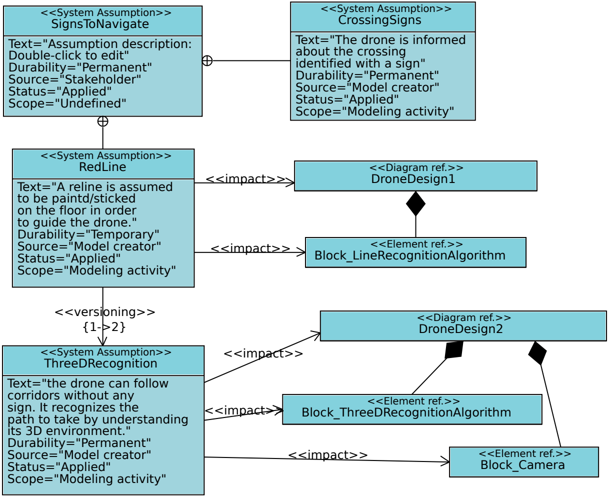
TELECOM ParisTech

TTool: Design #1

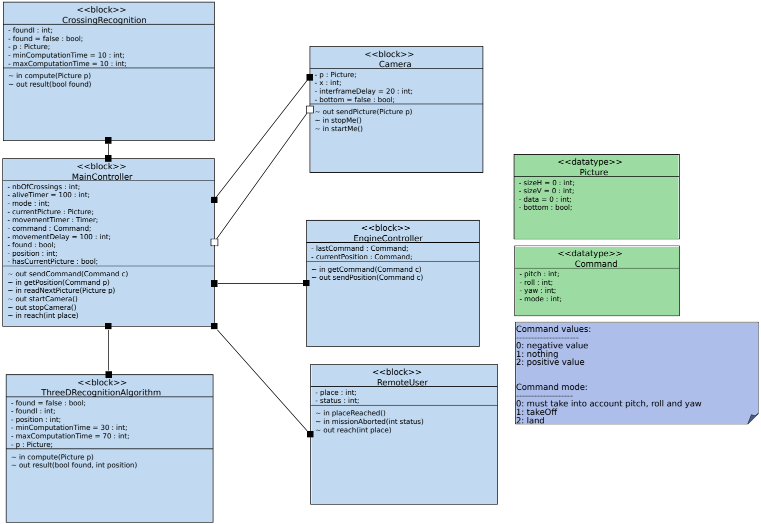


TELECOM ParisTech

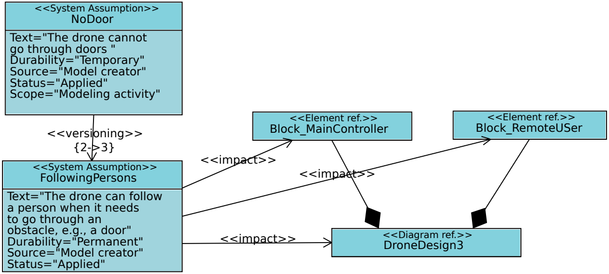
TTool: MAD Scenario #1 → #2



TTool: Design #2

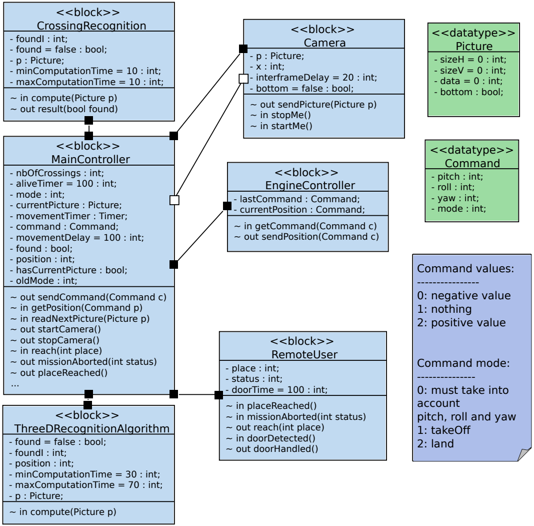


TTool: MAD Scenario #2 → #3



TELECOM ParisTech

TTool: Design #3



TELECOM ParisTech

Conclusion

Objective

Making modeling assumptions a part of every real-time system model

Contributions

- Model Assumption Diagram (MAD), attributes, relations
- Included into SysML-Sec, supported by TTool

Future work

- Optimizing simulation and verification with regards to versioning

To Go Further ...

- **TTool**: http://ttool.telecom-paristech.fr
- **SysML-Sec**: http://sysml-sec.telecom-paristech.fr

- **Drone4u** project: http://drone4u.telecom-paristech.fr
  - Several videos of the UAV in action!