SΦNX

A Co-Evolution Framework for Model Refactoring and Proof Adaptation in Cyber-Physical Systems

Overview

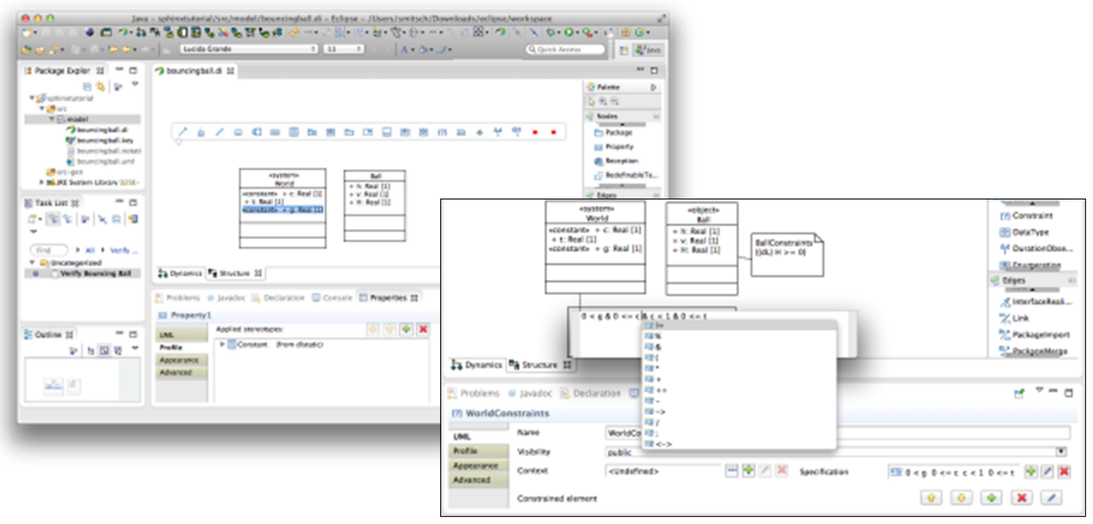
Hybrid systems with both discrete and continuous dynamics are an important model for real-world physical systems. The key challenge is how **to ensure their correct functioning w.r.t. safety requirements**. Promising techniques to ensure safety seem to be **model-driven engineering** to develop hybrid systems in a well-defined and traceable manner, **and formal verification** to prove their correctness. Their combination forms the vision of **verification-driven engineering**. It is not uncommon for **verification teams** to consist of many players with diverse expertise. We introduce a verification-driven engineering toolset that with tools for

(i) modeling hybrid systems,
(ii) exchanging and **comparing** models and proofs, and
(iii) managing verification tasks.

This toolset makes it easier to tackle **large-scale verification tasks**.

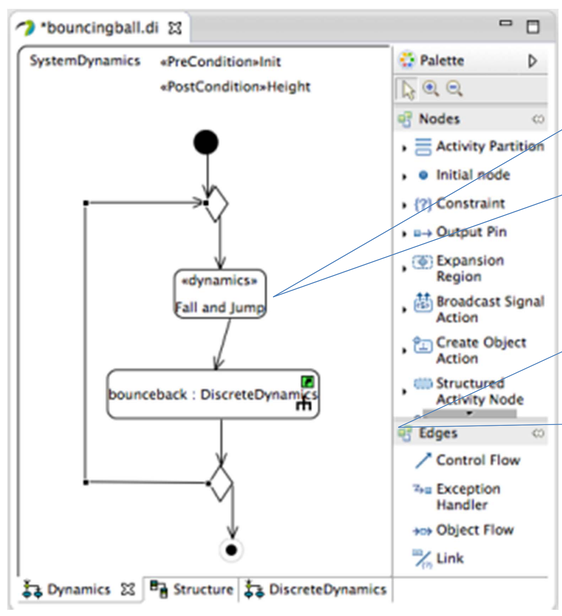
Graphical Modeling

Structure: UML Class Diagram

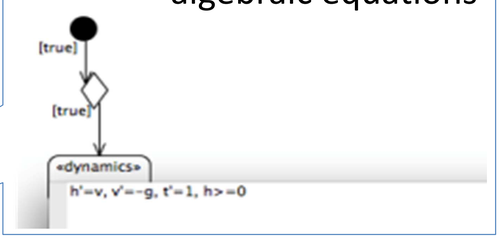


Constraint Popup Editor

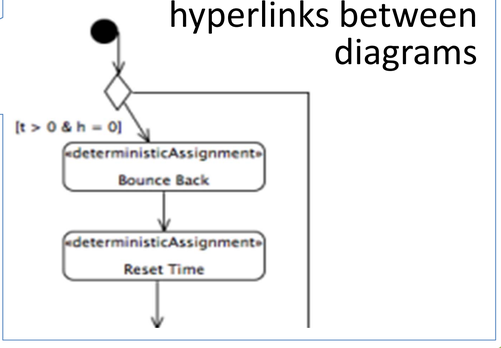
Dynamics: UML Activity Diagram



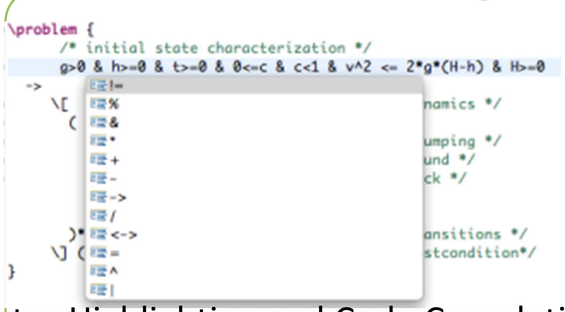
Popup editor for differential-algebraic equations



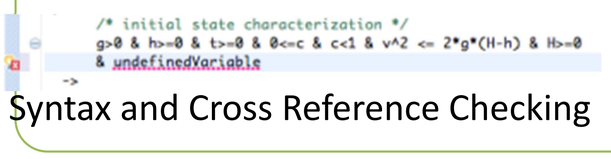
Hierarchical modeling and hyperlinks between diagrams



Textual Modeling

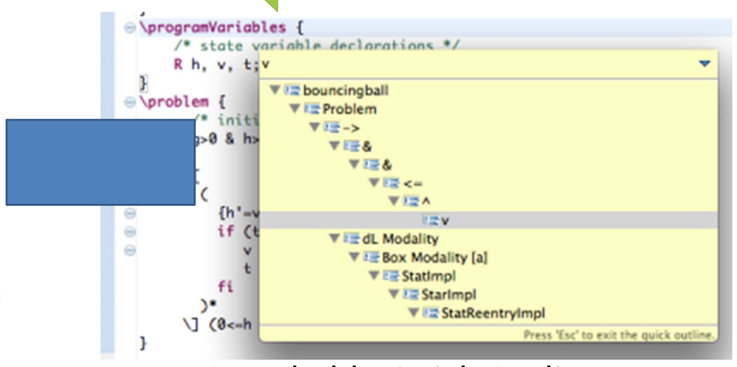


Syntax Highlighting and Code Completion



Syntax and Cross Reference Checking

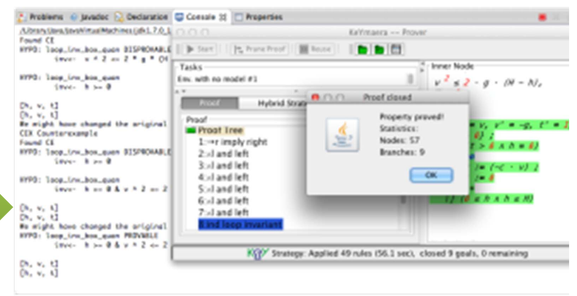
Transformation



Searchable Quick Outline for Navigation

Loading

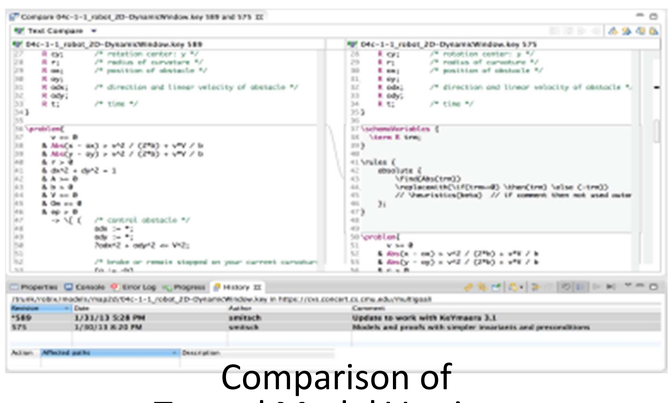
Verification



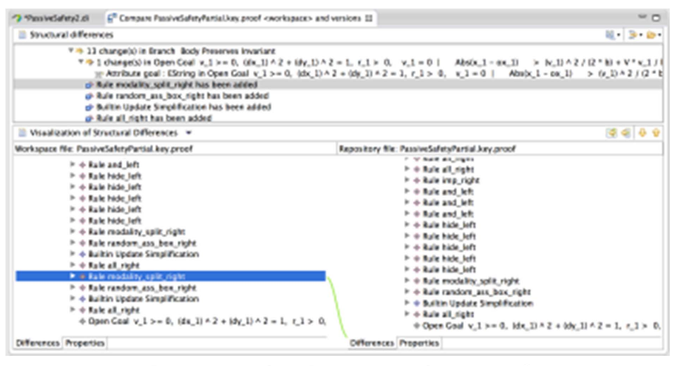
Hybrid System Verification in KeYmaera

Collaboration

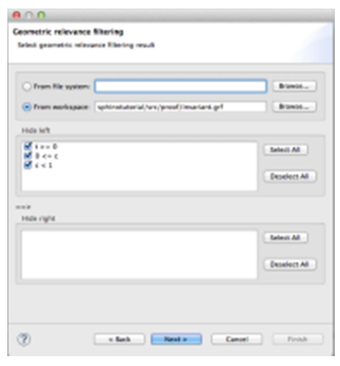
Proof Collaboration



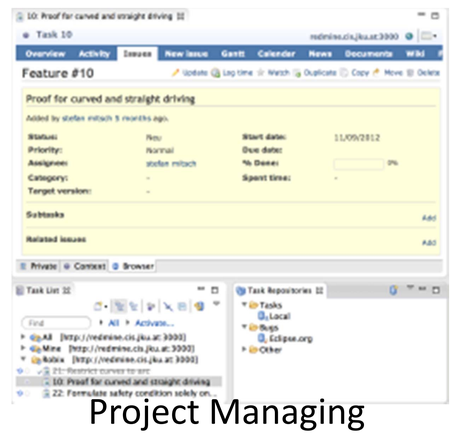
Comparison of Textual Model Versions



Semantic Comparison of Proof Versions



Import of External Proofs



Project Managing

Project Info

Funding: FP7 Marie Curie
Duration: NOV/2013 – OCT/2015
Partners: Carnegie Mellon University

cooperative cis.jku.at INFORMATION SYSTEMS

PEOPLE MARIE CURIE ACTIONS

Carnegie Mellon University