PRIN GAUSS Project Kick off meeting
Università di Milano Bicocca, February 22, 2017

Automatic generation of (dynamic) formal models

Valeria Vittorini, Univ. Napoli Federico II

(valeria.vittorini@unina.it)

Stefano Marrone, Univ. della Campania Luigi Vanvitelli

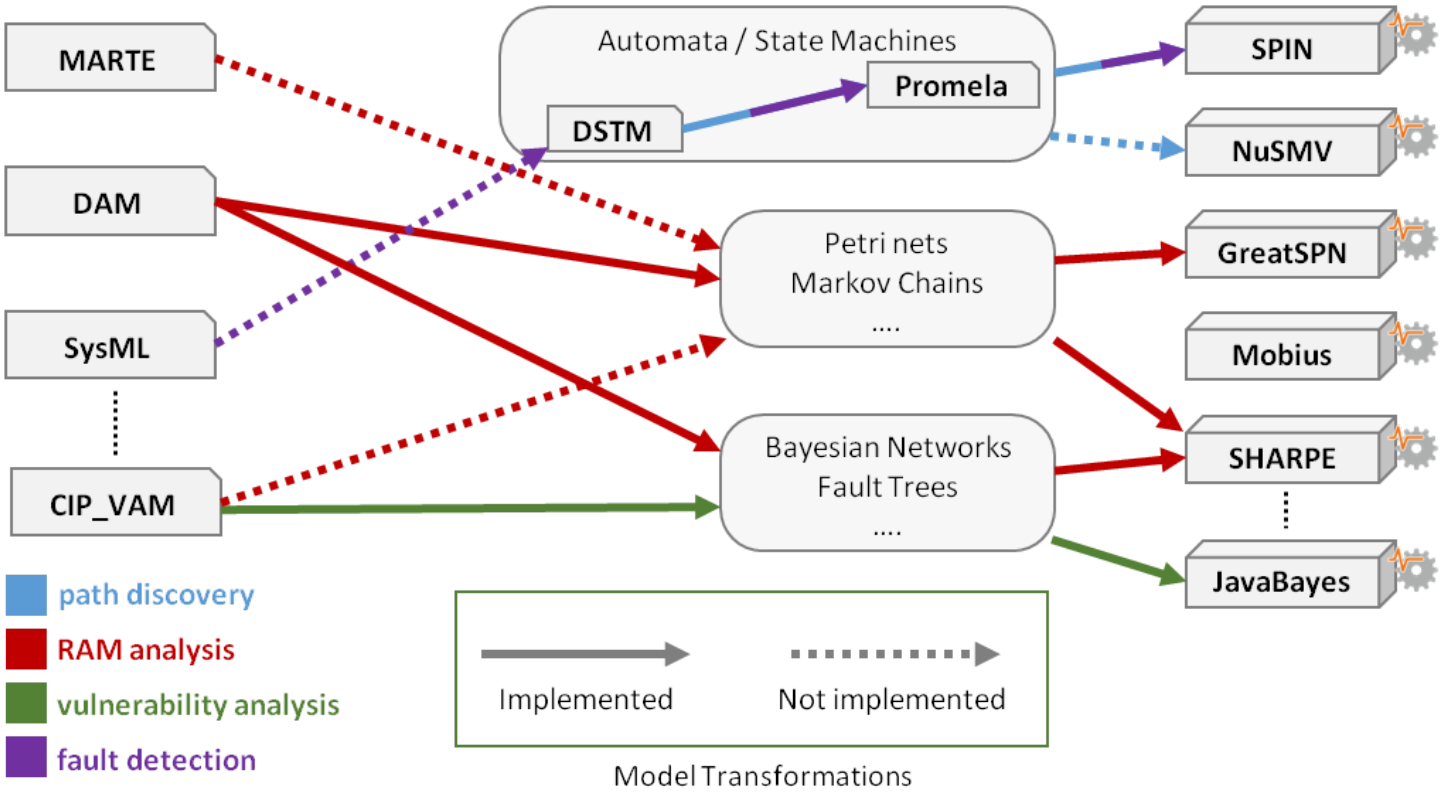
- Outline:
  - Approaches for the automatic generation of formal models
  - Dynamic State Machines (DSTMs)
  - Composition of heterogeneous parametric models
  - Possible contribution in GAUSS

Automatic generation of formal models

- Model driven engineering approaches based on:
  - UML profiling, or
  - DSML developed and supported by EMF technologies and tools (Ecore/Eclipse/ATL/Java….)
  - Development of model transformations from descriptive models (high-level models) to analysis models (low-level models)

Modeling railway control systems in promela (2015)
Using Bayesian Networks to evaluate the trustworthiness of '2 out of 3' decision fusion mechanisms in multi-sensor applications (2015)
Enabling the usage of UML in the verification of railway systems: The DAM-rail approach (2013)

Transformation chains

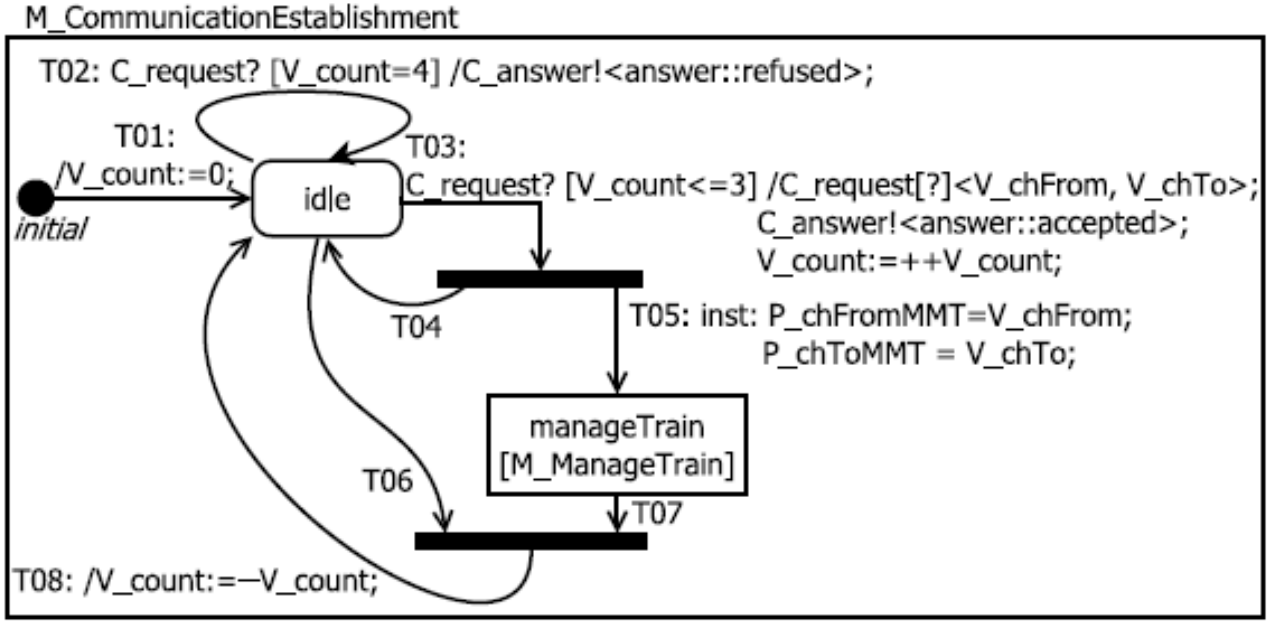


DSTM: Our extension of hierarchical state machine for embedded control systems

CIP_VAM: Our UML profile for vulnerability modeling (Critical Infrastructure Protection)

A proper DSML language or hierarchy of languages could be developed for deriving query-able formal models in GAUSS?

Dynamic State Machines (DSTMs)

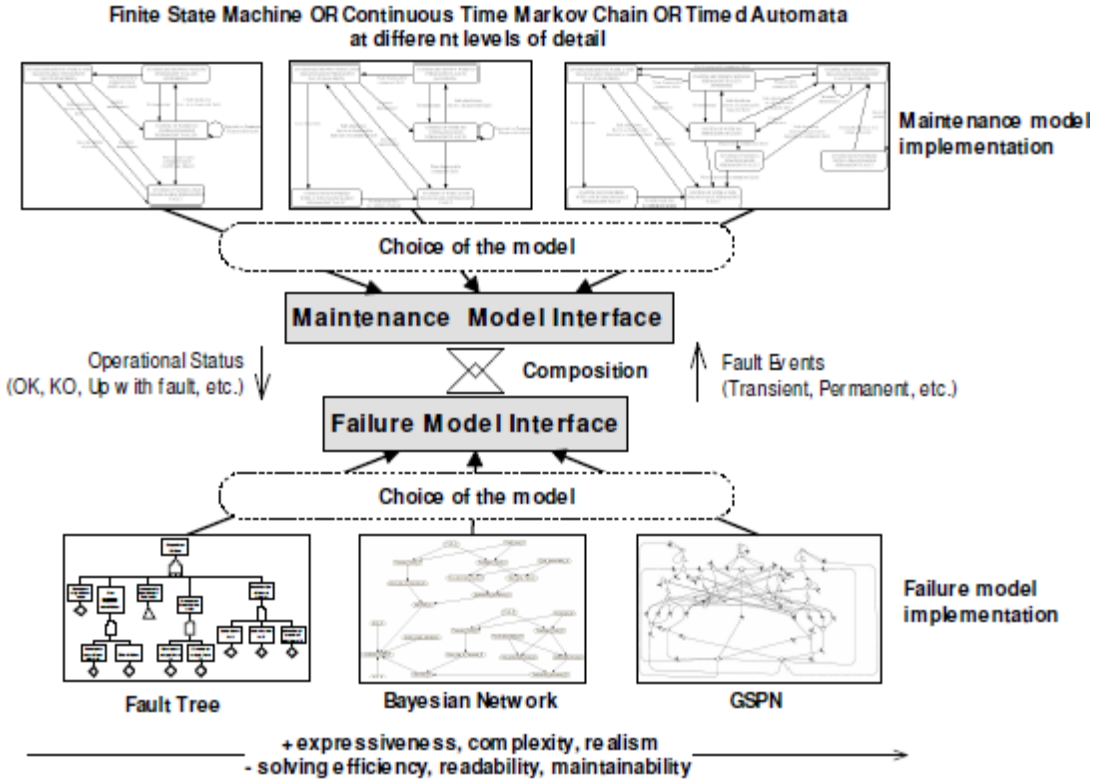


- DSTM is a formal specification language currently integrated into a EMF-based transformation chain in order *to derive Promela models* to be checked by Spin. A modeling GUI and a model verifier are available (the latter performs syntax and semantic s checks on DSTM models).
- Used (so far) for property verification or test case generation.
- It is possible to define backward processes in order to obtain DSTM models from traces /logs etc….
- *A relevant feature of DSTM in GAUSS* is that the state machines are instantiated dinamically (for example the manageTrain machine in the figure is instantiated if and when a request message arrives and it is accepted, in particular in the case shown in the figure the instantiated machines run concurrently with their caller)

Dynamic state machines for modelling railway control systems, Science of Computer Programming (2017)

Composition of heterogeneous parametric models

- Multiformalism
- Multi-level modeling
- Components and Interfaces
- Template models (parametric)



Fuzzy decision fusion and multiformalism modelling in physical security monitoring (2016)
A multiformalism modular approach to ertms/etcs failure modeling (2014)
Multiformalism and transformation inheritance for dependability analysis of critical systems (2010)
Multiformalism techniques for critical infrastructure modeling (2010)

Possible contribution in GAUSS

- WP1 – Modeling of functional and non functional properties
  - development of lightweight DSML (abstract, concrete and ontological)?
  - design of language hierarchies supporting ontology-based relationships between models?
  - Generation of complex models?
  - … ?
- WP5 – Online monitoring and data mining
  - generation of DSTM state machines from execution traces?
  - generation of test cases from DSTM state machines?
  - …?