AdapID workshop
26 September 2006
KU Leuven

Model-based approaches for the design of secure e-ID card applications

Hans Vangheluwe

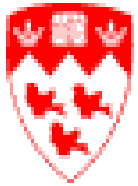
Mohamed Layouni, Ximeng Sun, Miriam Zia

Modelling, Simulation and Design Lab

McGill University

Stefan Brands, Credentica

MSDL
Modelling, Simulation and Design Lab



McGill

Belgian National electronic ID cards

- Functionalities of e-ID:
  - Visual and electronic identification of the cardholder;
  - Stores a single public key certificate linked to a citizen's national number → electronic authentication of the cardholder;
  - Digital signature;
  - ...
- Used in all transactions with government services.
- RISK: breaching **privacy** of citizen.

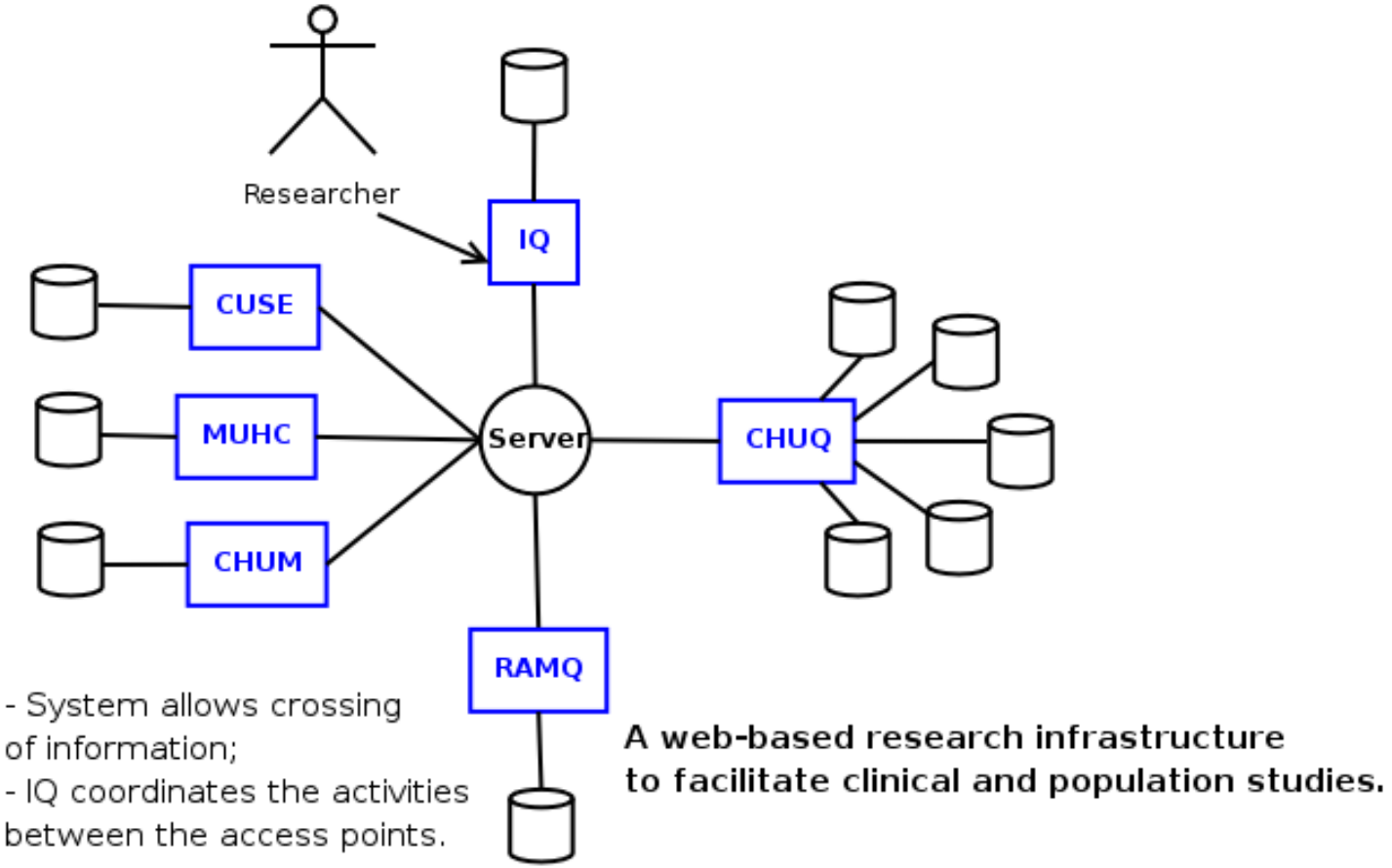
E-Health Applications

- **Motivation:**
  - **Improve the quality and efficiency of healthcare;**
  - **Reduce related costs;**
  - **Rely on the innovation of information and communication technology.**

- **Technology:**
  - **Associated with each patient is his/her Electronic Health Record (EHR) (patient-related information);**
  - **Electronic data warehouses: central information systems where EHRs are stored.**

- **Concerns:**
  - **Management of electronic health records;**
  - **Mining of electronic health data.**

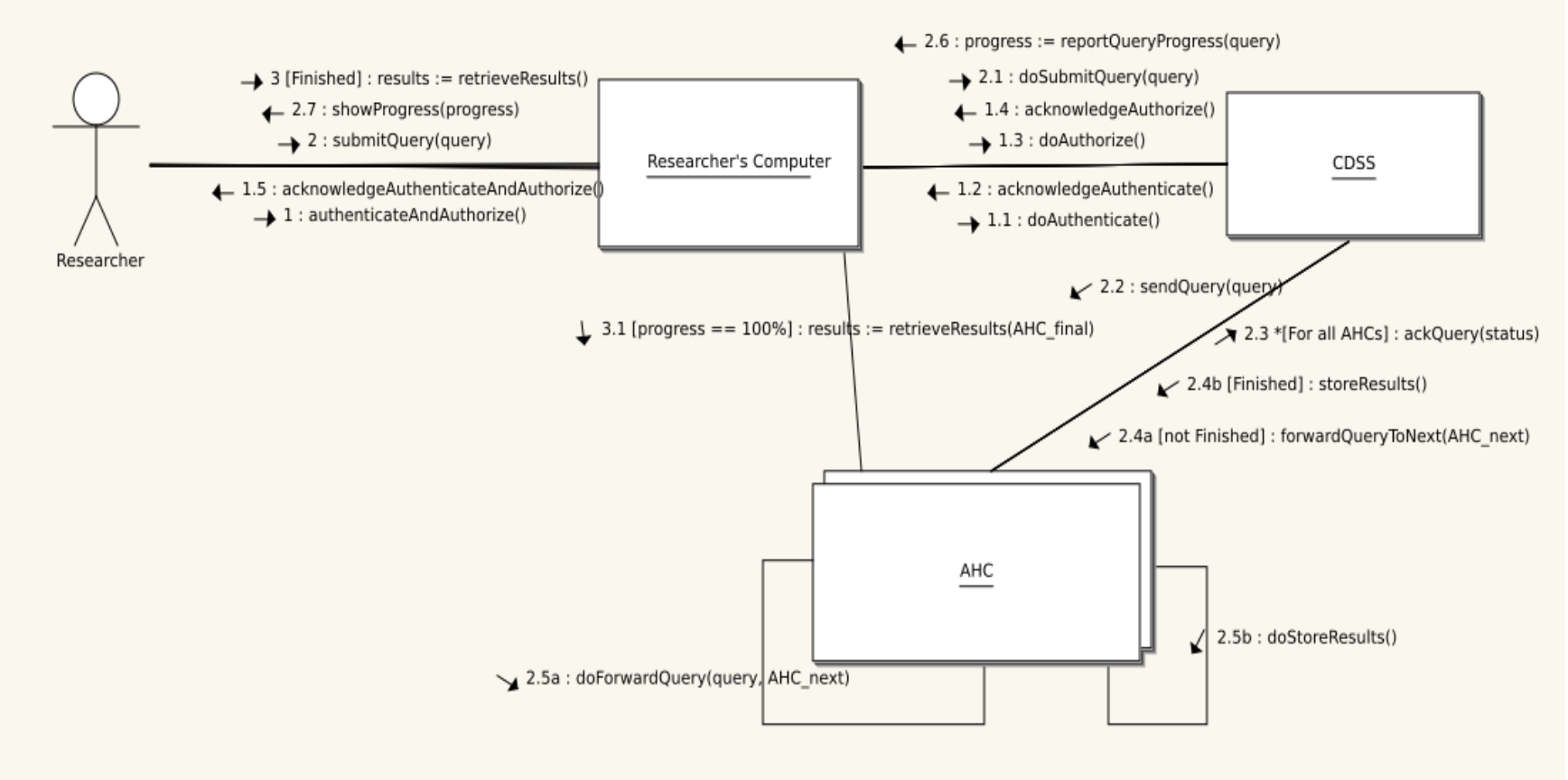
Existing Infrastructure for Mining of Electronic Health Records (EHR)



- **Inspired by the IRIS-Quebec implementation.**

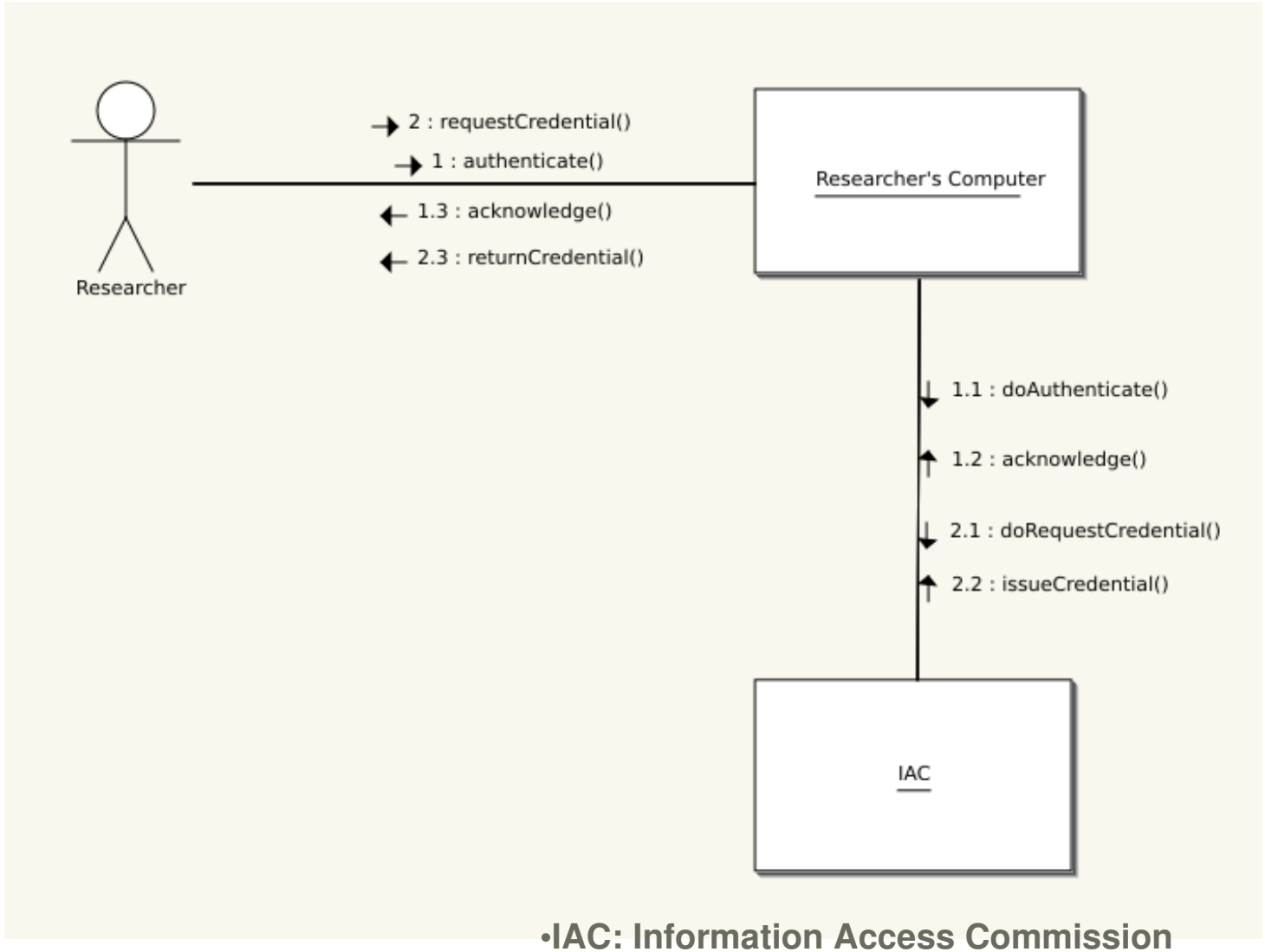
("Infrastructure de Recherche Intégrée en Santee du Québec")

Use Case: Mining EHR



- Queries are processed sequentially by a subset of the AHCs (Associated Hospital Centers) under the coordination of the CDSS (Clinical Data Sharing System).
- The CDSS first sends the query to *AHC_i1*. Once *AHC_i1* is done, the CDSS requests *AHC_i1* to forward the query along with the anonymized result to the next *AHC_i2*.
- When the cumulative result reaches *AHC_final*, the CDSS notifies the researcher that the query has been processed and provides the location where the result can be fetched.

Use Case: Issuing a Credential for EHR Mining



- IAC: Information Access Commission

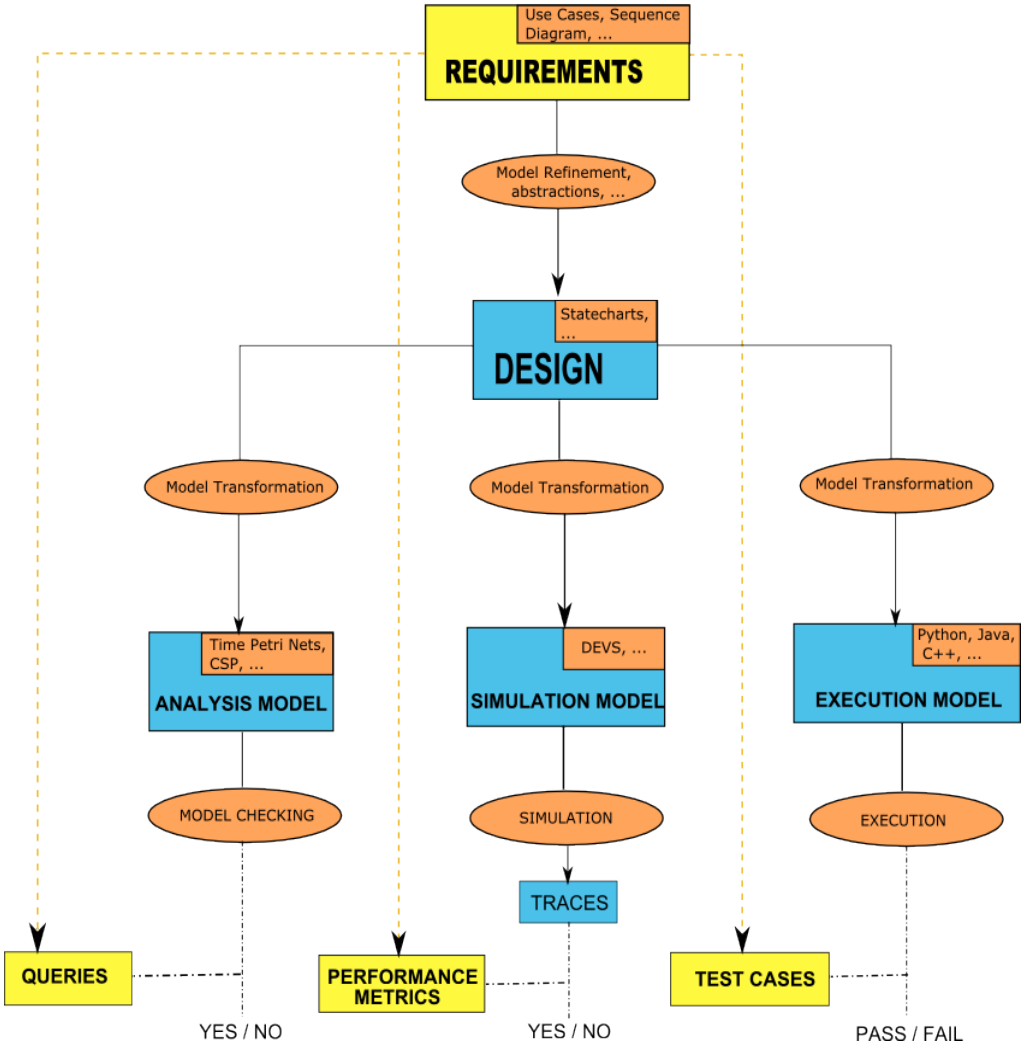
Concerns

- **We *only* require that communication channels between the AHCs, the CDSS, and the researcher guarantee the *integrity* of data. *Confidentiality* is not required because:**
    1. **AHCs exchange only anonymized EHRs when processing a query;**
    2. **The researcher retrieves the result of his/her query in an anonymized form (all person-identifying fields are removed);**
    3. **Authentication and query submission between the researcher and CDSS is likely to be done in Zero Knowledge thereby assuring confidentiality and preventing replay attacks.**

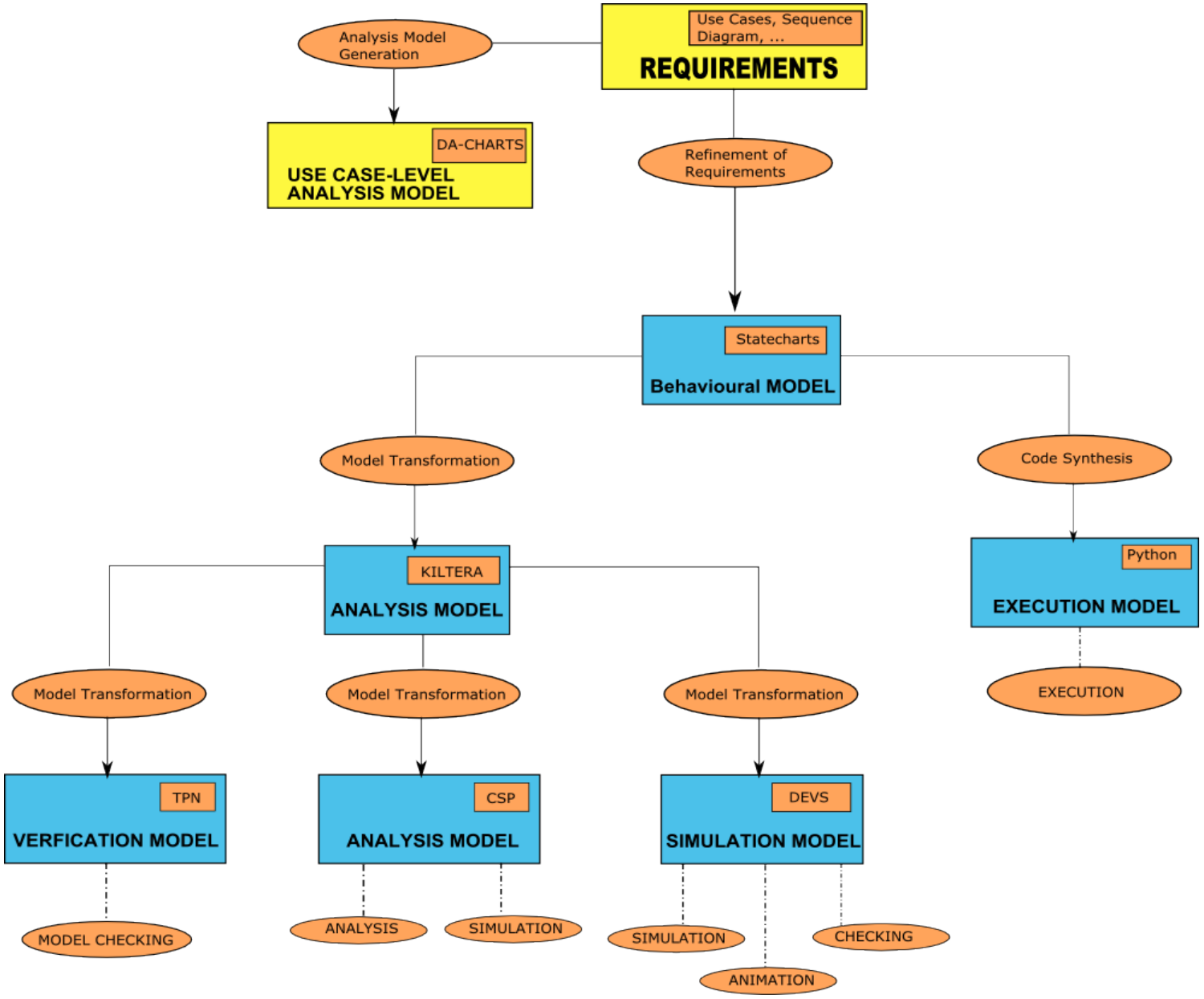
Modelling and Simulation Based Design of Complex Systems

- We now have:
  - A definition of eID;
  - A definition of e-health and related applications;
  - An example e-health use case, and requirements;
  - Something to check for (integrity of data).

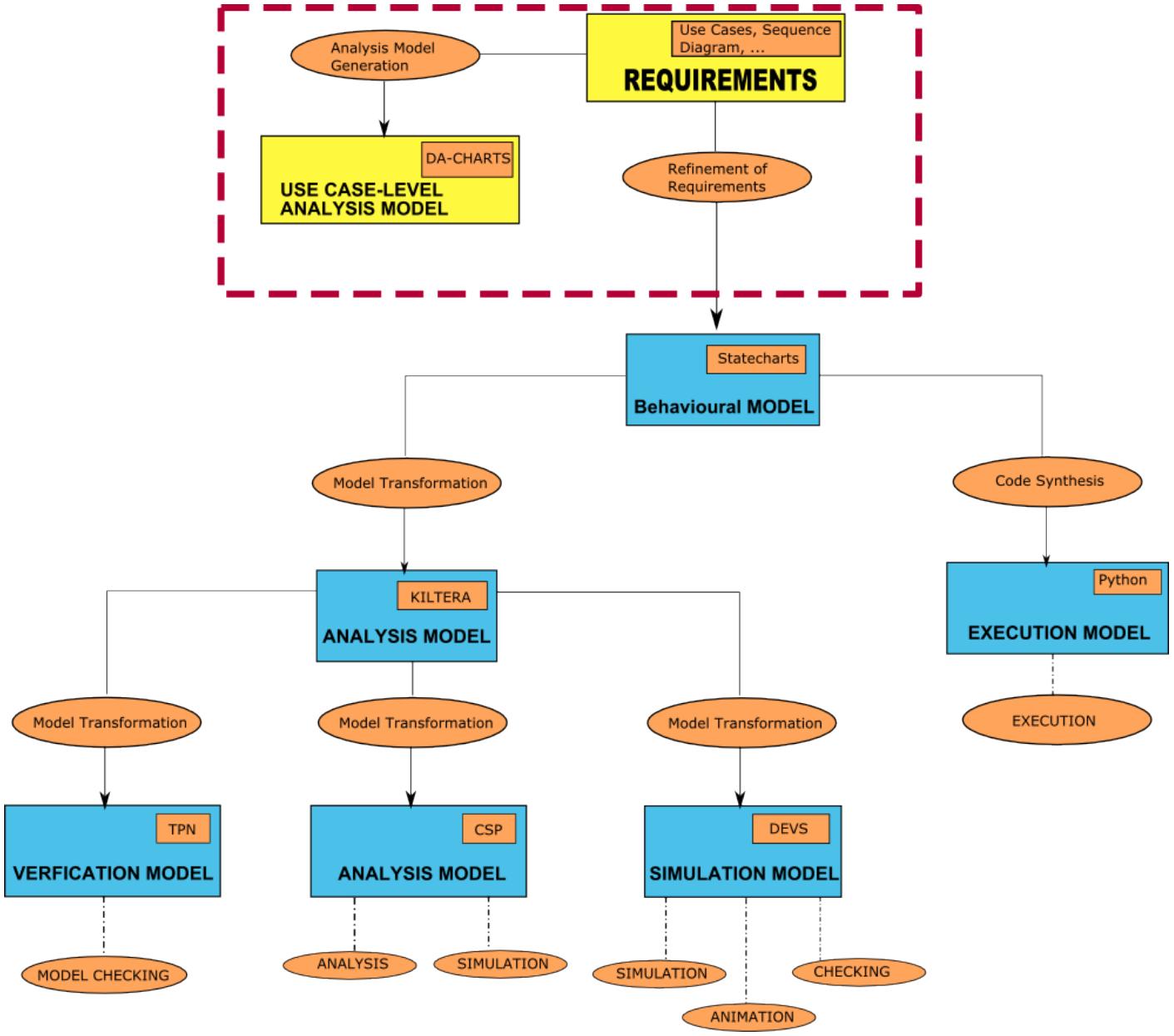
Where do we go from here?



Overview of the Process



Use Case-Level Analysis



Model-Driven Assessment of Use Cases for Dependable Systems

- Assessing and refining use cases to ensure that the specified functionality meets the dependability requirements of the system.

- Method:
  1. Mapping use cases to DA-Charts model;
  2. Perform probability analysis of the model using AToM^3.

Dependability and Fault Tolerance

- **Dependability:**

  Property of a computer system such that reliance can justifiably be placed on the service it delivers.

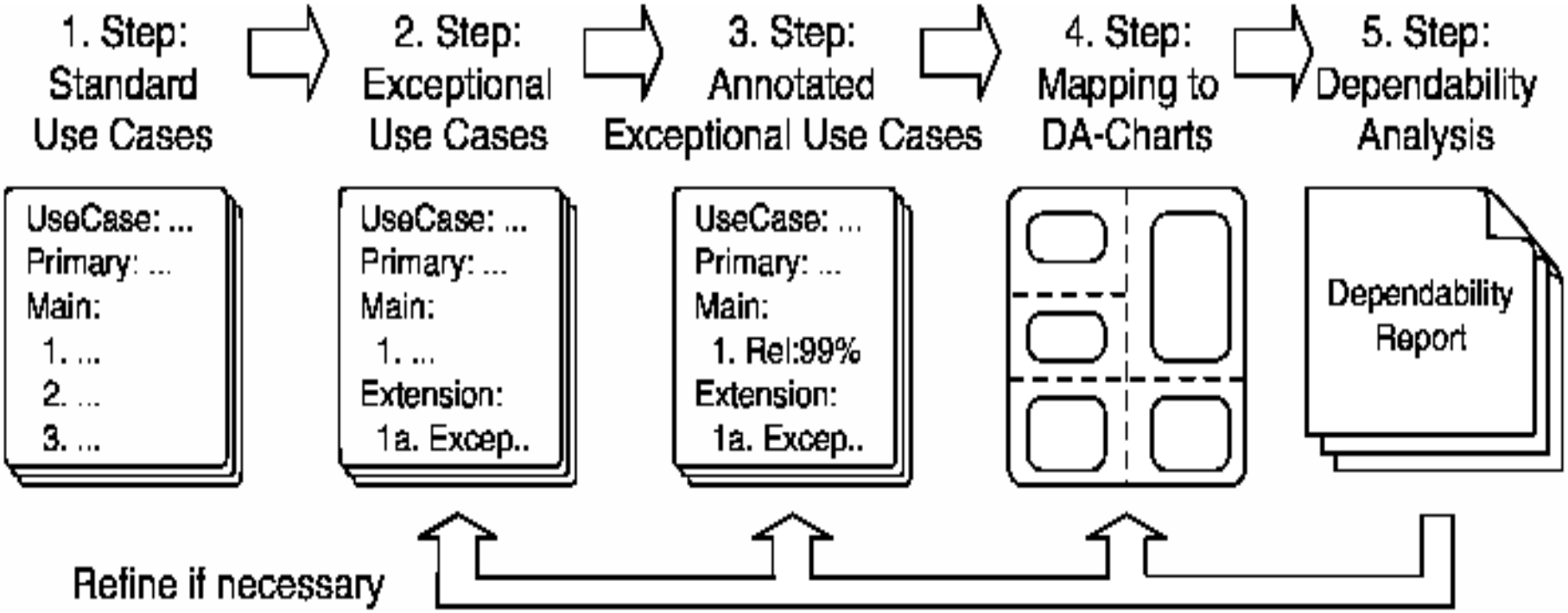
  - **Reliability: Measure a system's aptitude to provide service and remain operating as long as required.**
  - **Safety: Determined by the lack of catastrophic failures it undergoes.**

- **Fault tolerance:**

  Means of achieving system dependability.

  - **Error detection: Detection of exceptional situations**
  - **System recovery: Describing the interactions with the environment**

Model-Driven Process for Assessment and Refinement of Use Cases



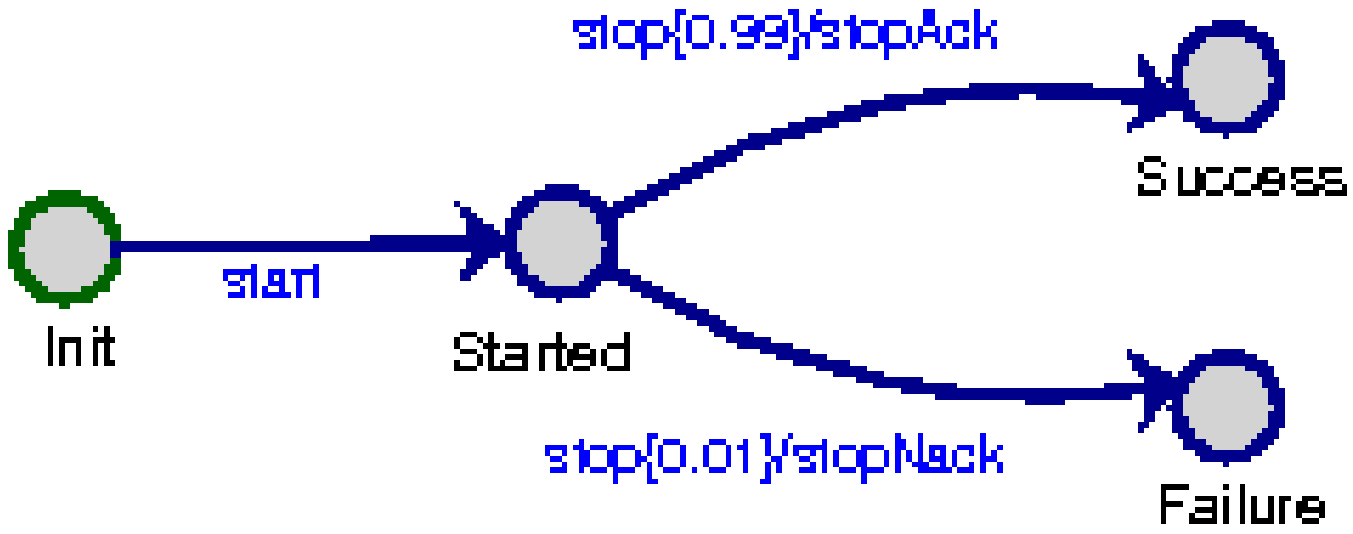
DA-Charts

• **D**ependability **A**ssessment **Charts**:

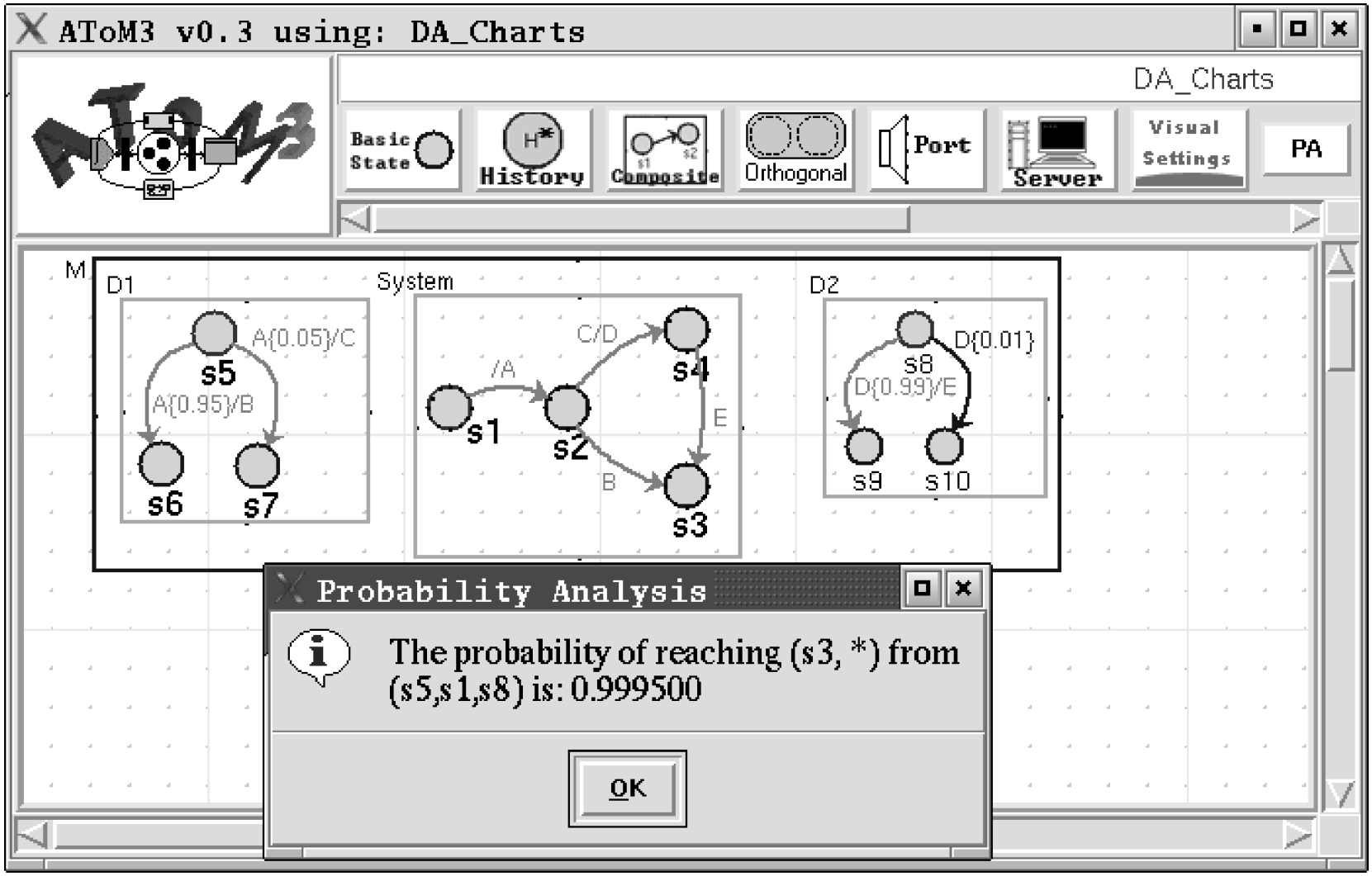
Probabilistic extension of the Statecharts formalism.

• A state can transition to one of two possible target states: a *success* state with probability *p* and a *failure* state with probability *1-p*.

• Syntax: *event[condition]{probability}/action*

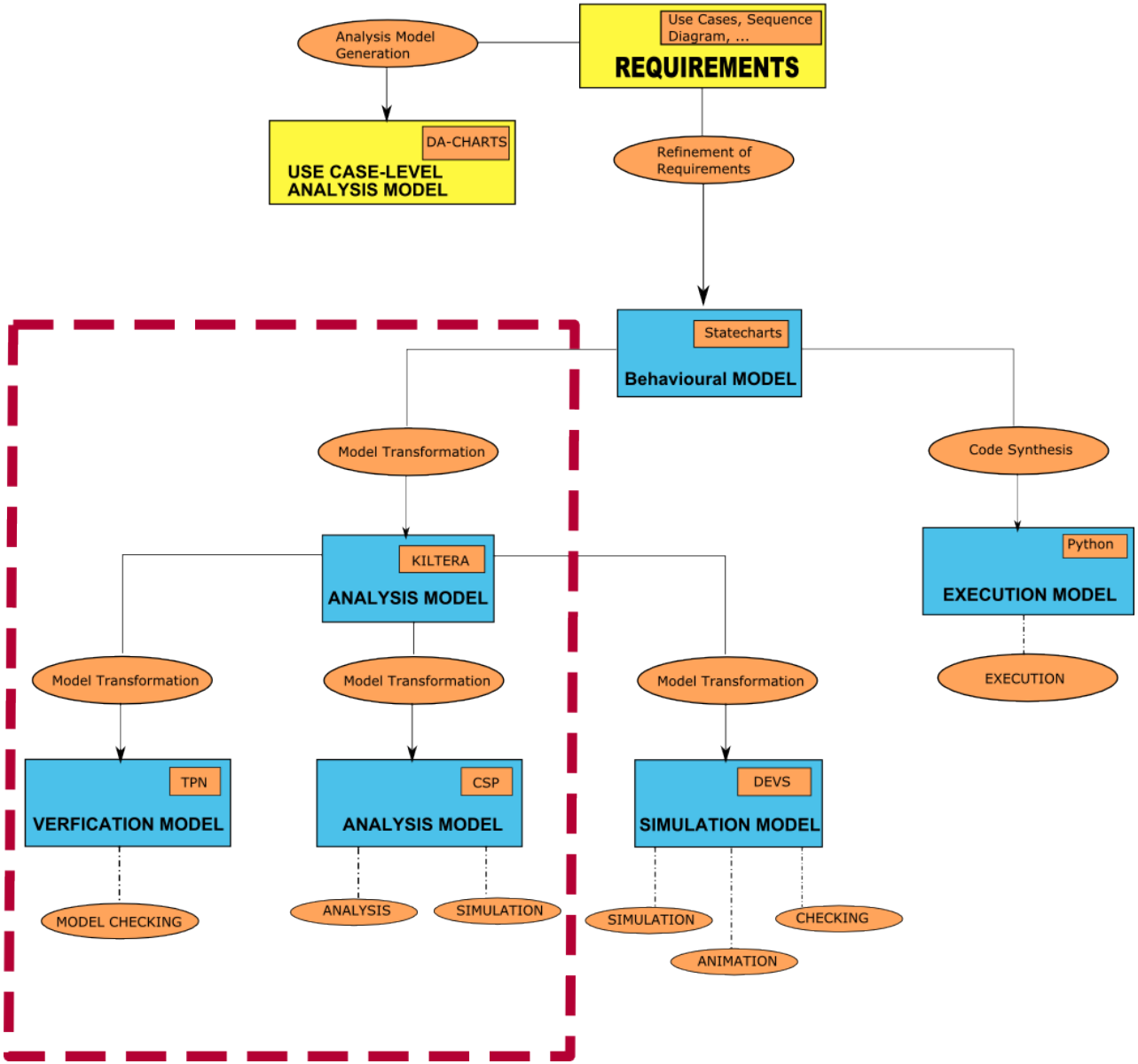


DA-Charts in AToM³

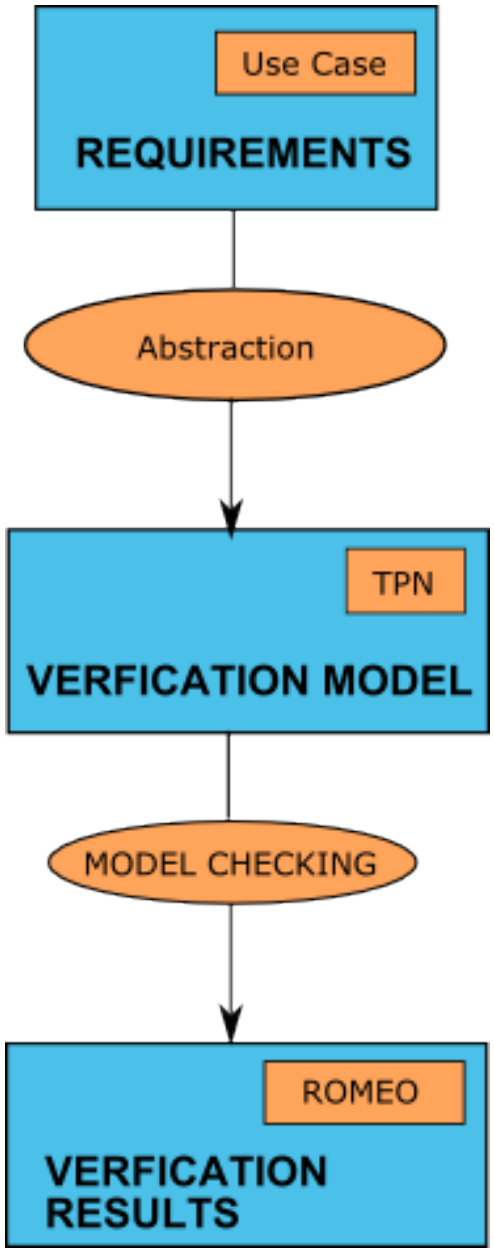


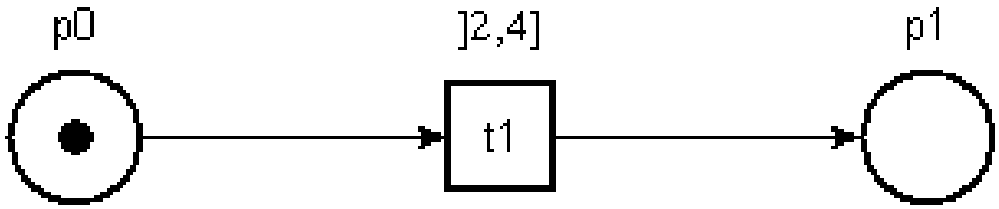
(note: concurrency)

Verification Branch



Model Verification with TPN and Romeo

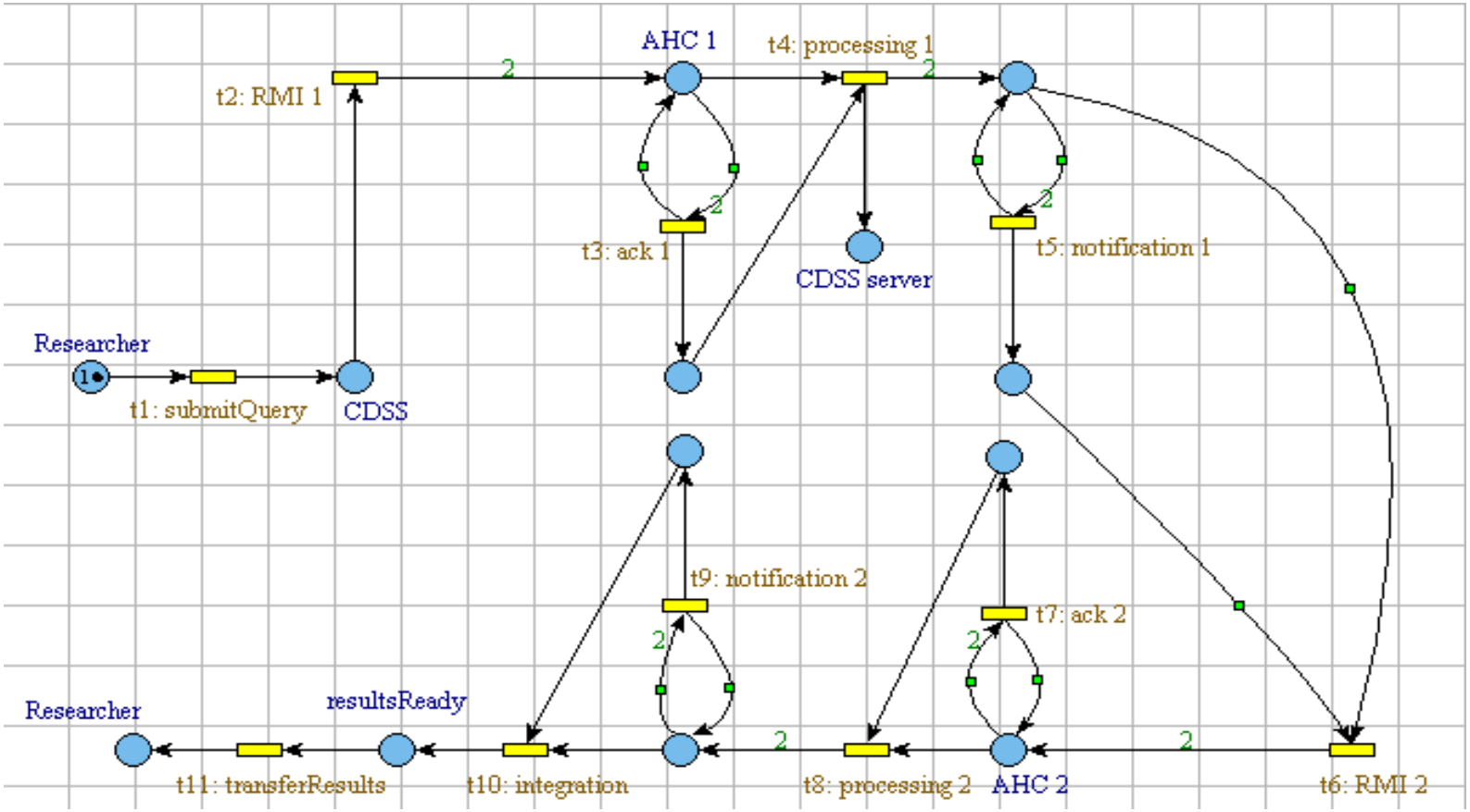




Example of TPN Model

- **ROMEO:**
  - **TPN Analyzer: translates TPN models into Timed Automata;**
  - **Performs state space computation and on-the-fly model checking of reachability properties expressed in RT-CTL (Real-Time Computation-Tree Logic).**

TPN Model of the CDSS

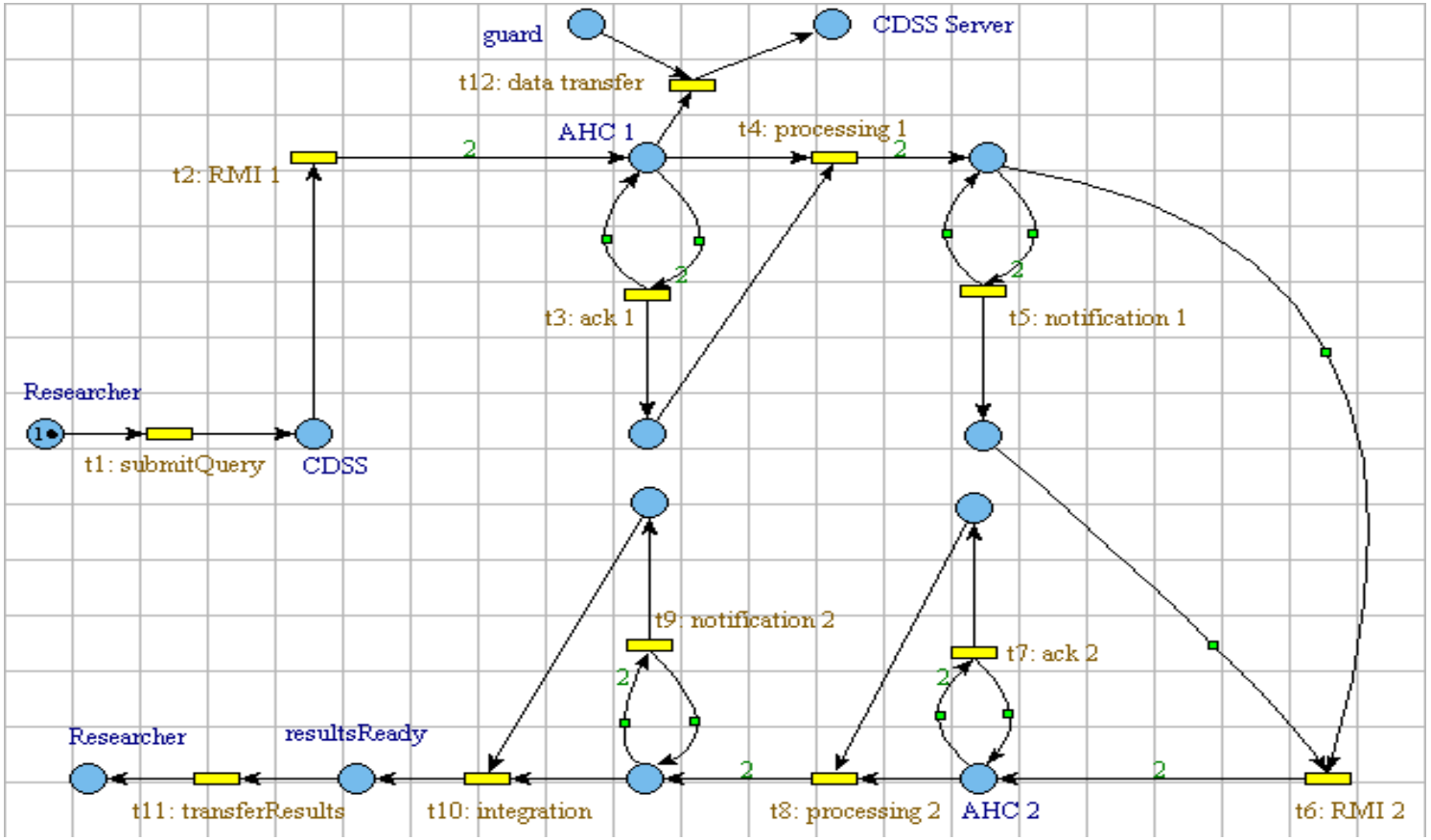


- **Check : AG[0,inf](M(CDSS server)<1)**
  - **Assumption that the "CDSS server" place could hold 2 tokens if there was some breach of privacy of data (results were stored on the server).**
- **Output:**

  false *(property does not hold)*

  Trace: t1: submitQuery, t2: RMI 1, t3: ack 1, t4: processing 1

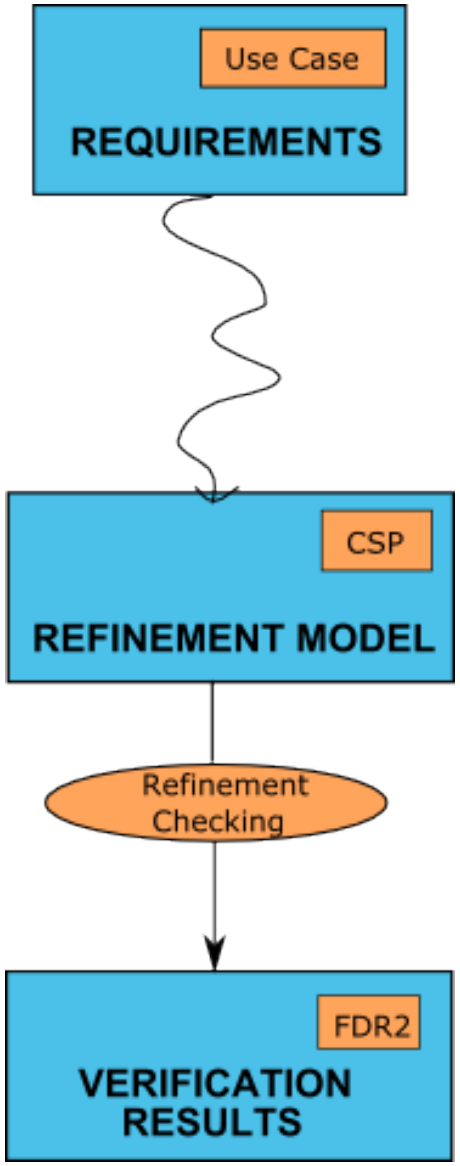
Privacy-respecting TPN Model of the CDSS



- Check : AG[0,inf](M(CDSS server)<1)
- Output:

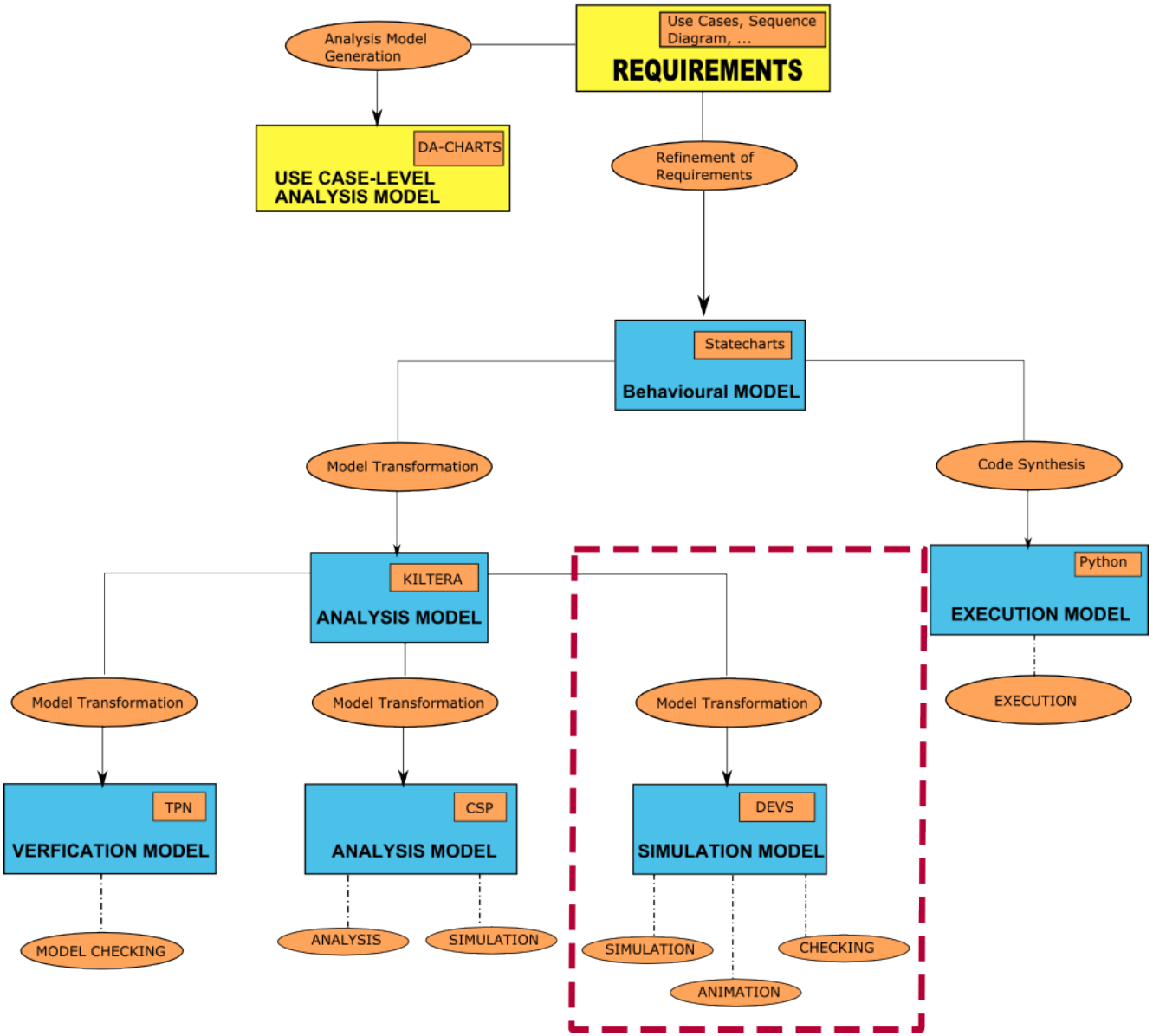
  true

Use Case Analysis with CSP and FDR2

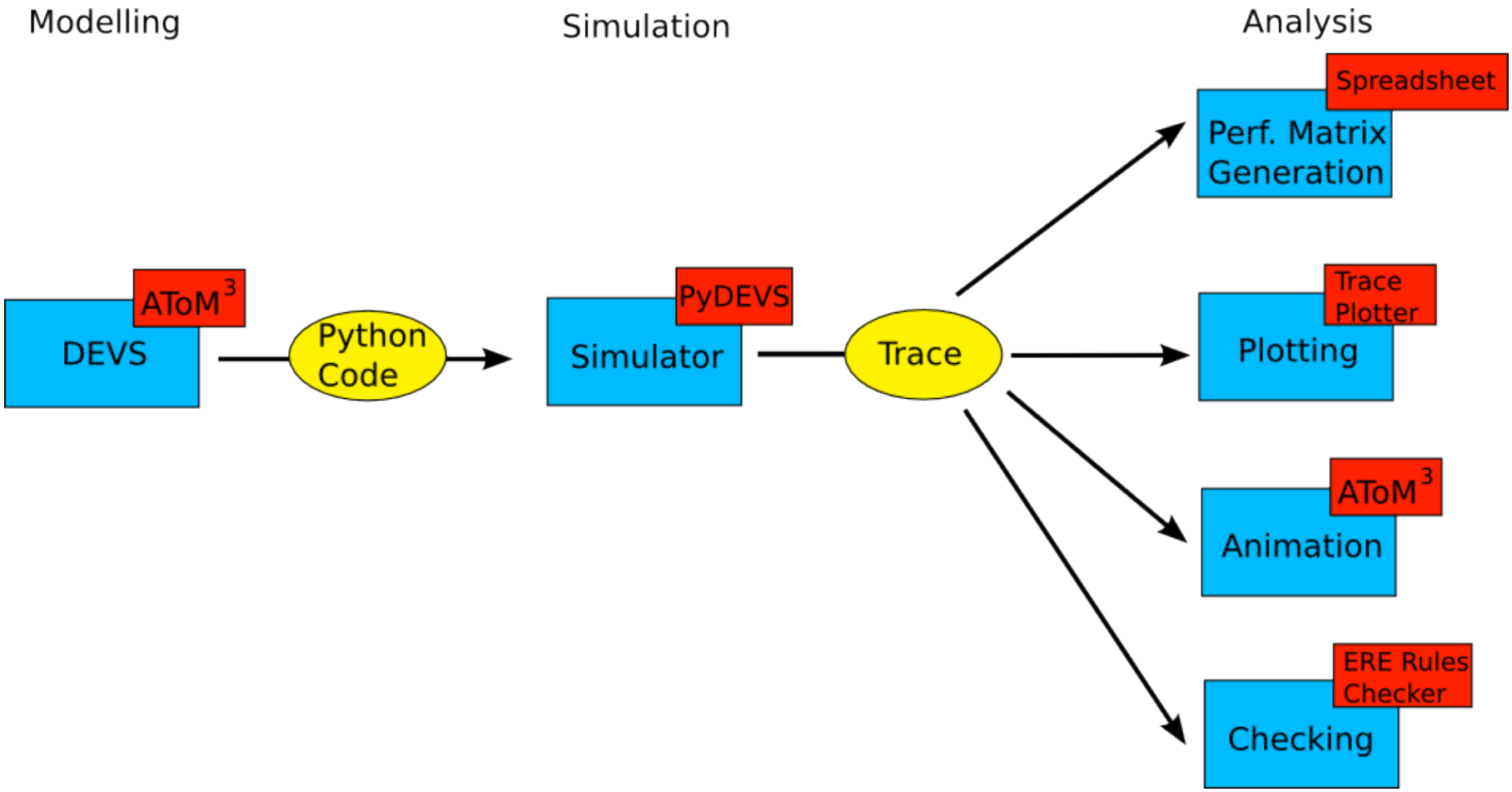


- CSP *(Communicating Sequential Processes)*:
  - Language for describing patterns of interaction.
- FDR2 *(Failures/Divergence Refinement 2)*:
  - Model checker for systems described in CSP;
  - Converts two CSP process expressions into labelled transition systems, and then determines whether one of the processes is a refinement of the other.

Simulation Branch



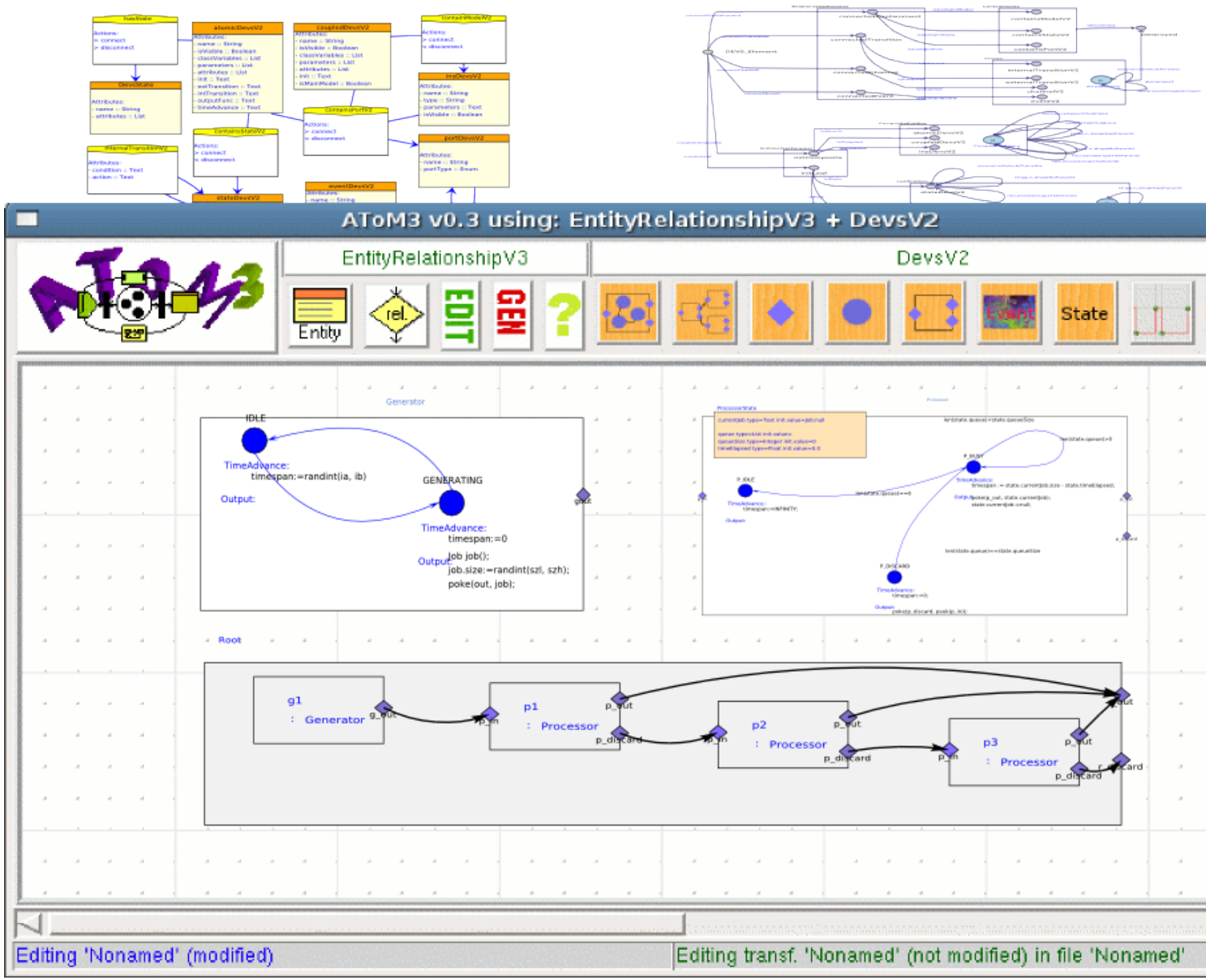
Approach


Modelling
Simulation
Analysis
DEVS
AToM3
Python Code
Simulator
PyDEVS
Trace
Perf. Matrix Generation
Spreadsheet
Plotting
Trace Plotter
Animation
AToM3
Checking
ERE Rules Checker

DEVS Formalism

- *D*iscrete-*EV*ent system *S*pecifications
- To develop a rigourous basis for the compositional modelling and simulation of discrete event systems

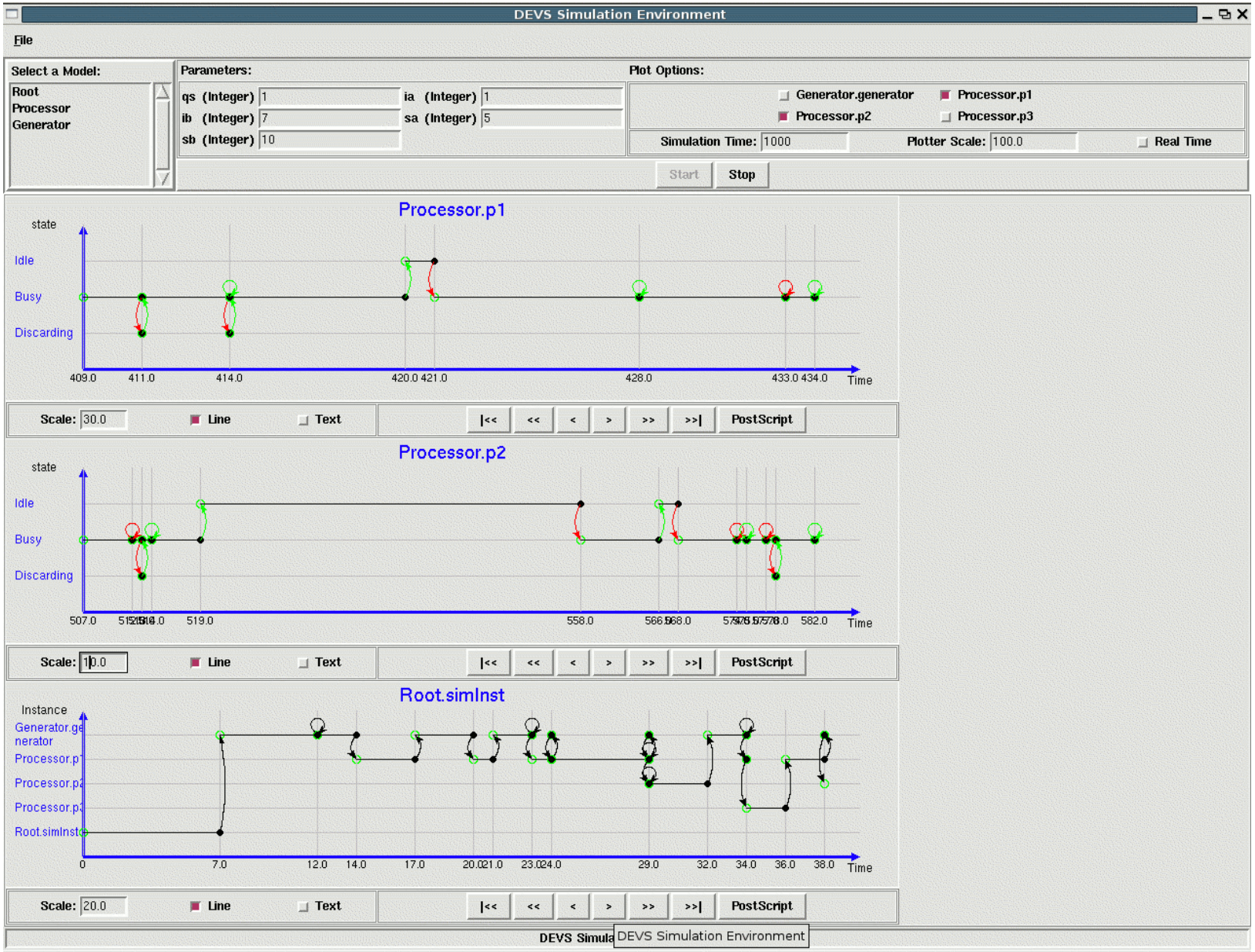
DEVS in AToM³



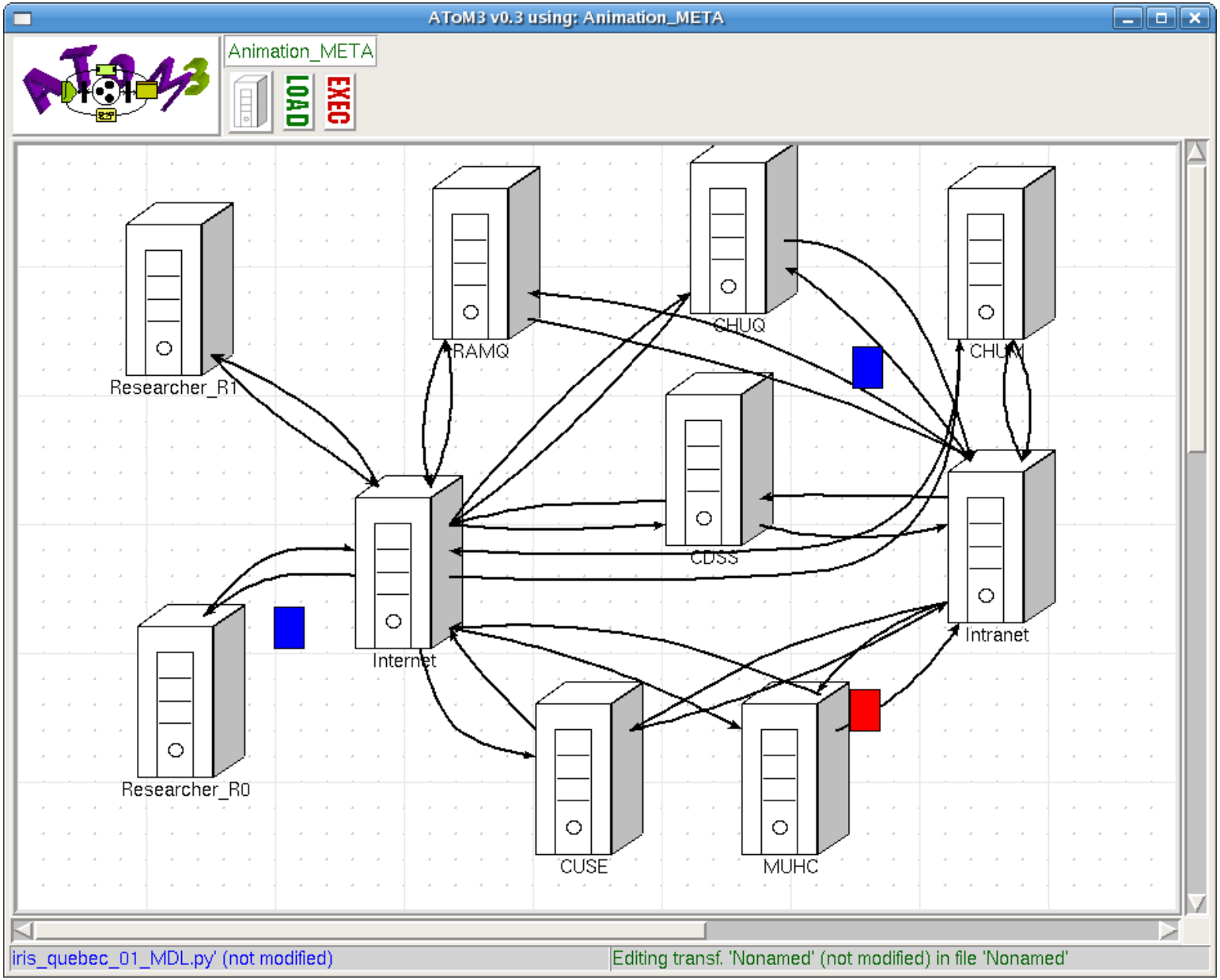
Modelling & Simulation using PyDEVS

- PyDEVS (aka PythonDEVS):
  - A prototype DEVS modelling language with simulator

Simulation Results Analysis with DEVS Trace Plotter



Animation in AToM^3



Conclusions

- Gave overview of first experiments in modelling and simulation based design of e-Health applications
- Next phase:
  - Elaborate use case(s)
  - Down to synthesis of code ?
  - Use Credentica SDK

References

[IRIS-Quebec] **http://www.iris-quebec.ca/**

[BH01-1] **Andrea Bobbio and András Horváth, "Model Checking Time Petri Nets Using NuSMV", PMCCS 5, 2001.**

[Hoa78] **C.A.R Hoare, "Communicating Sequential Processes", Communications of the ACM 21, 1978.**

[Ros94] **A.W. Roscoe, "Model-Checking CSP", in A *Classical Mind: essays in Honour of C.A.R. Hoare*, Prentice Hall, 1994.**

[MSKV06] **S. Mustafiz, X. Sun, J. Kienzle, and H. Vangheluwe. "Model-Driven Assessment of Use Cases for Dependable Systems", ACM/IEEE 9th International Conference on Model Driven Engineering Languages and Systems, 2006.**