Verification of electronic ID-based E-Health Applications

Miriam Zia

August 28 2006

Modelling, Simulation and Design Lab – McGill University

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;
  - Generates a digital signature.
- Used in all transactions with government services.
- RISK: breaching privacy of citizen.

adapID Project (Flanders, Belgium)

- **AD**vanced **AP**plications for electronic **ID**entity Cards.

- **Aim of project:**
  - **– Design secure e-ID applications which protect the privacy of citizens;**
  - **– Designs will either function on top of current e-ID technology, or require design improvements in the e-ID architecture itself.**

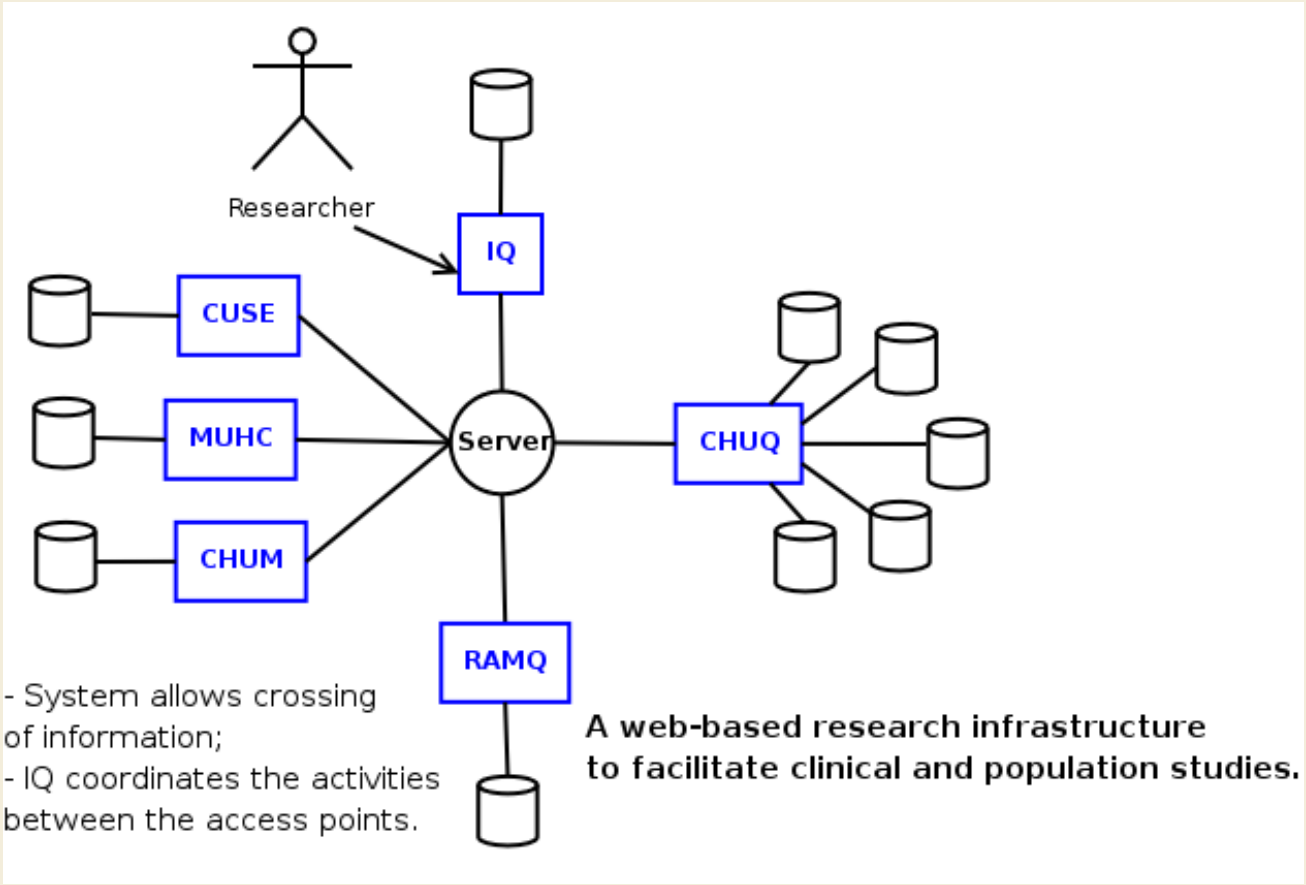
E-Health Applications

- **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.**

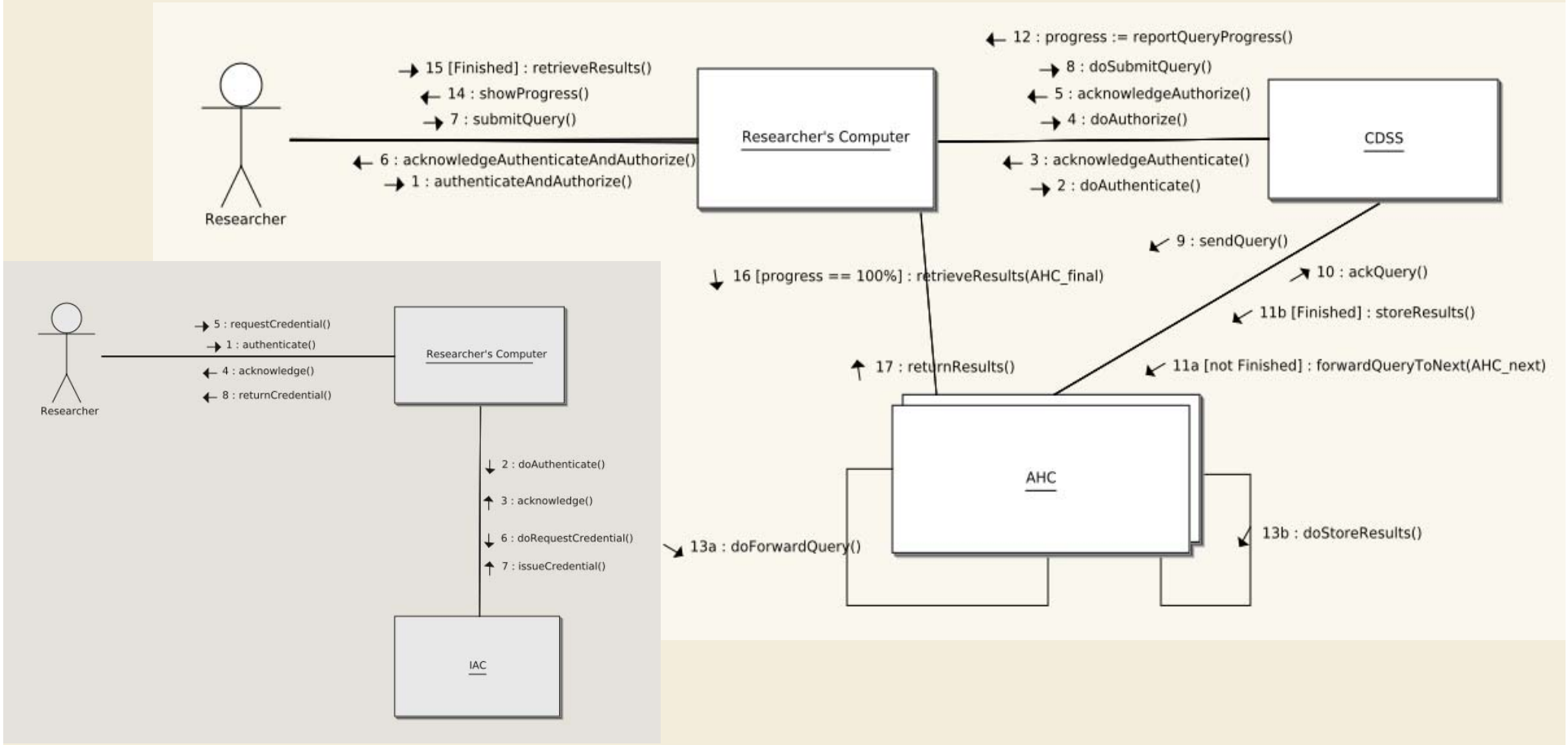
Existing Infrastructure for Mining of Electronic Health Data



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

(“Infrastructure de Recherche Intégrée en Santee du Québec”)

Use Case: Mining Electronic Health Data

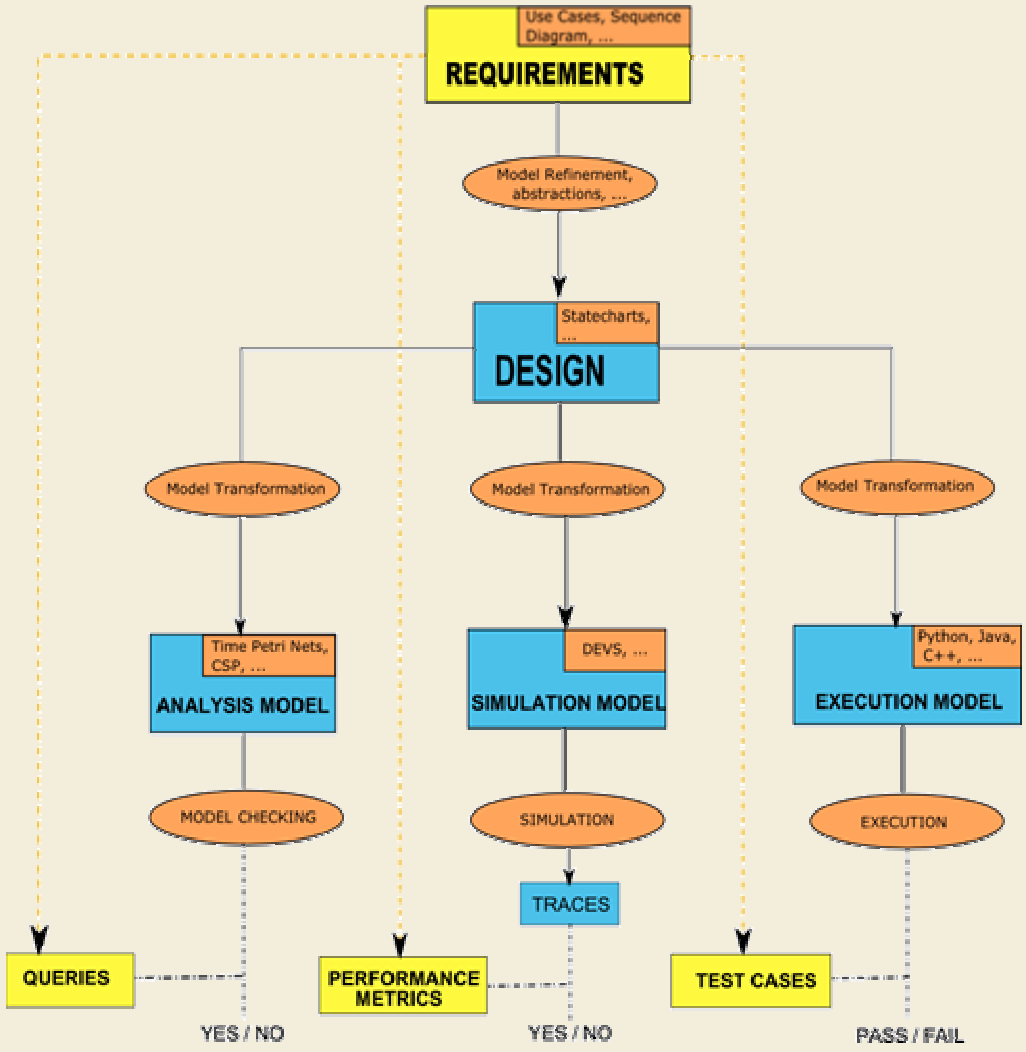


CONCERN: Communication channels between the AHCs, the CDSS, and the researcher must guarantee integrity and privacy of data.

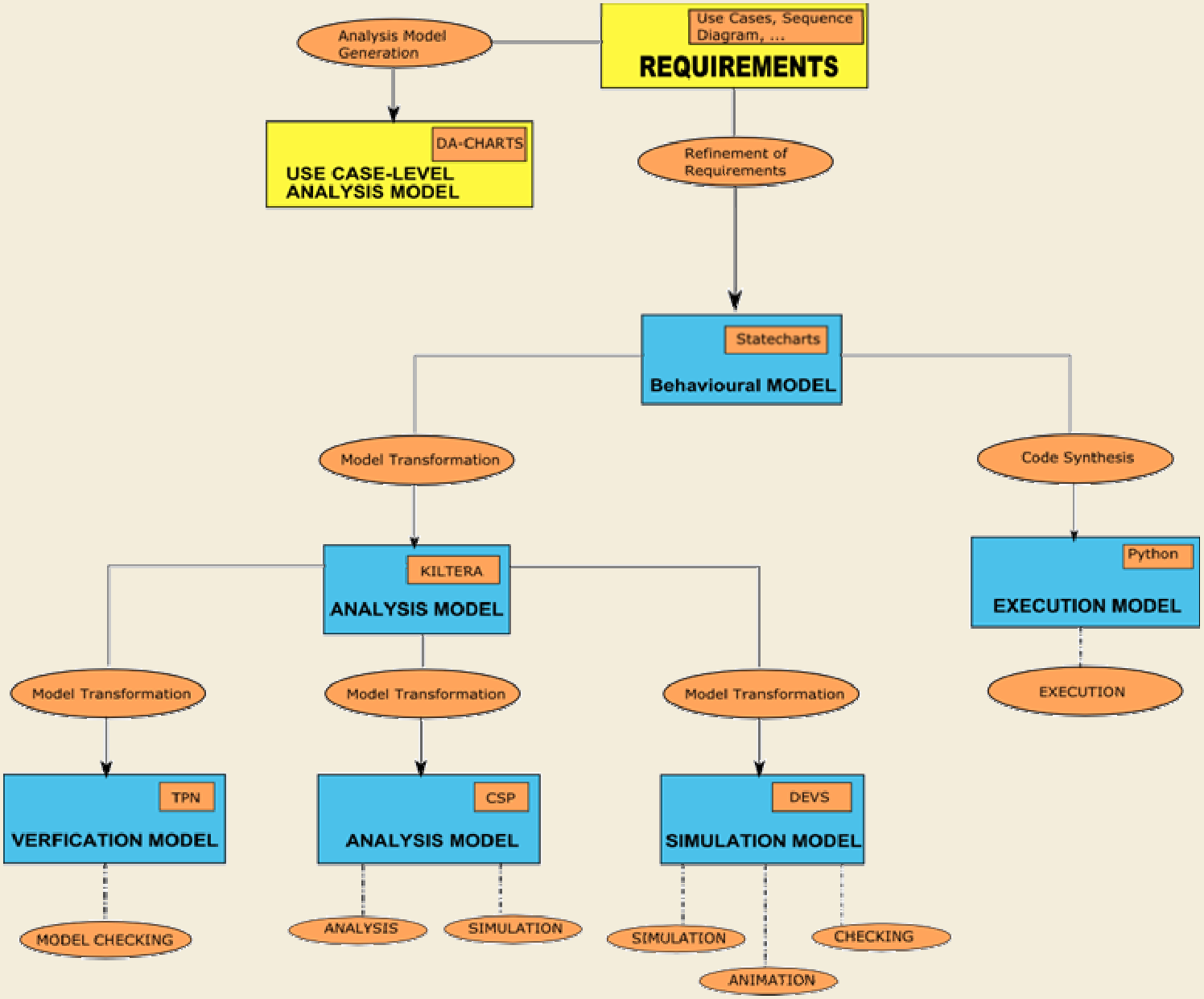
Recap: Modelling and Simulation Based Design of Complex Systems

- **We now have:**
  - **A definition of eID;**
  - **A definition of e-health and related applications;**
  - **An example e-health use case, and requirements.**

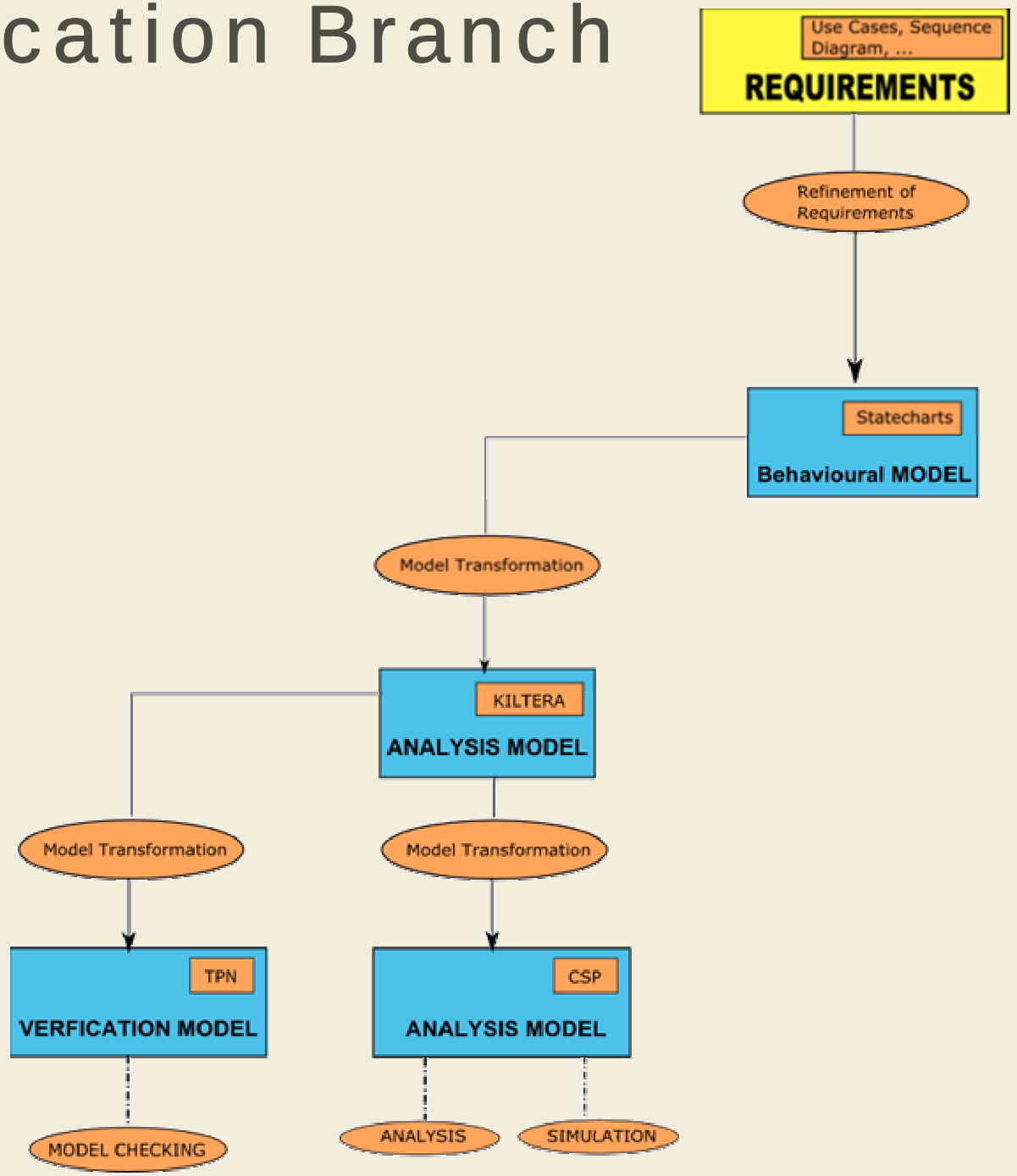
Where do we go from here?



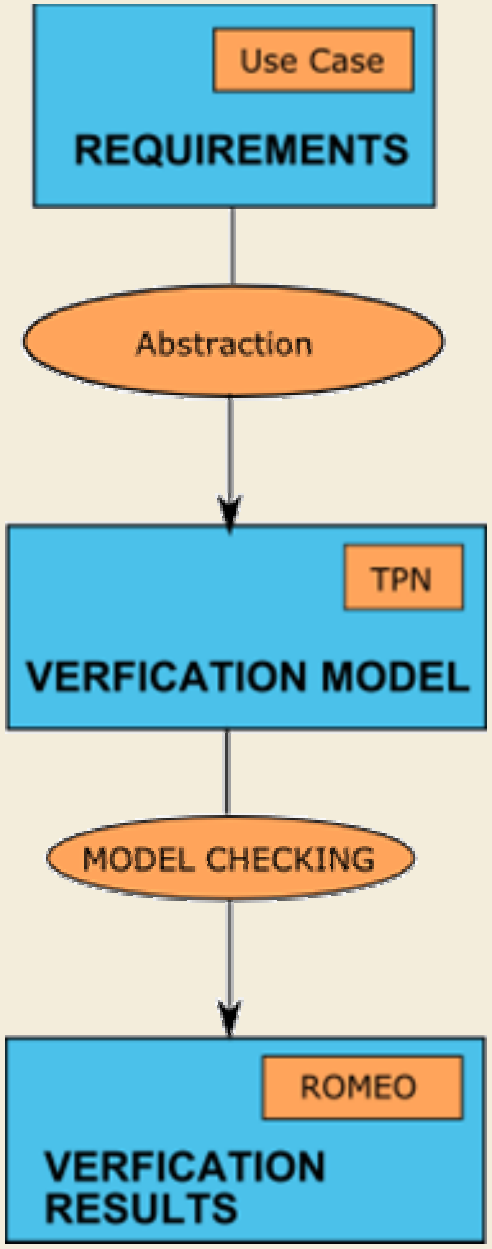
Overview of Process

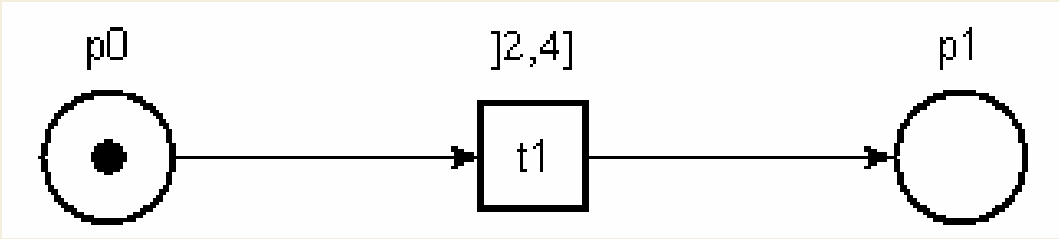


Verification Branch



Model Verification with TPN and Romeo

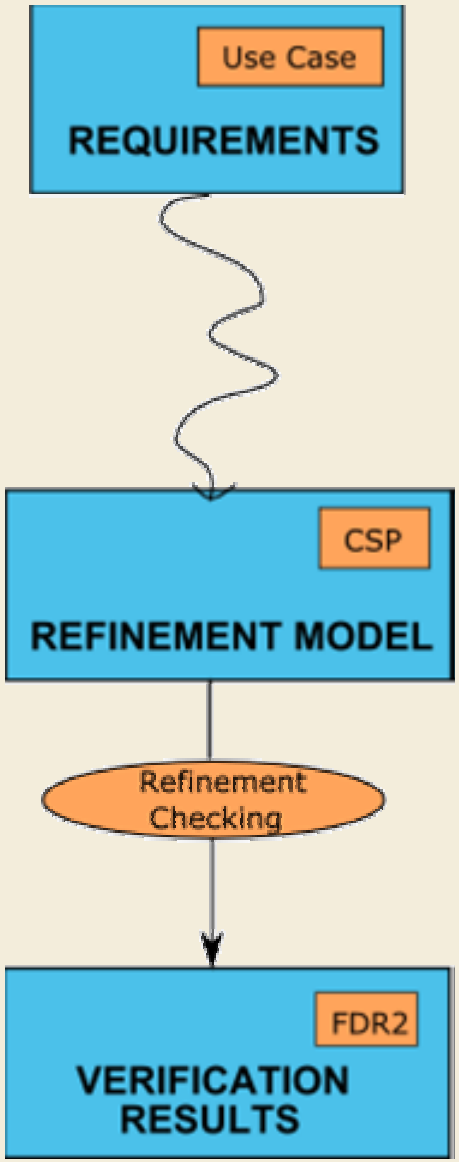




Example of TPN Model

- **ROMEO:**
  - **– TPN Analyzer: translates TPN models into Timed Automata;**
  - **– Performs state space computation and on-the-fly model checking of reachability properties.**

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;**
  - **– It converts two CSP process expressions into labelled transition systems, and then determines whether one of the processes is a refinement of the other.**

References

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

[adapID] **https://www.cosic.esat.kuleuven.be/twiki/adapid/bin/view.cgi/Public/WebHome**

[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.**