Real-Time Animation for Formal Specification

Dominique Méry[1]
Neeraj Kumar Singh[1]

[1]Université Henri Poincaré Nancy 1
LORIA, BP 239, 54506 Vandoeuvre lès Nancy, France

October 25, 2010

Nancy-Université

CSD&M

Loria

Outline

1 **Motivation**
- Examples of failures
- Formal Methods

2 **Validation**

3 **Our Approach**

4 **Case Study : Pacemaker**
- One and Two-Electode Pacemaker
- Validation & Proof Statistics
- Real-time Animation : Pacemaker
- ECG Data and Features
- How Real-time Animation can help in real world?

5 **Conclusion**

6 **Future Work**

Examples of failures

- Therac-25
- Air-Traffic Control System in LA Airport
- Pacemakers reset to unsafe parameters due to external radiation sources (anti-theft devices, microwaves,...)
- Ariane 5 Explosion
- Infusion pumps delivering the wrong rate of medicine

Why Formal Methods?

The Analysis Problem:

- Is it complete ?
- Is it sound ?
- Have I really understood it ?
- Do different people say different things ?

What are Formal Methods?

Formal= Mathematical
Methods= Structured Approaches, Strategies
Using mathematics in a structured way to analyze and describe a problem.

Definition

Formal methods are a particular kind of mathematically-based techniques for the specification, development and verification of software and hardware systems.

Objective of Formal Method?

- To explain why formal specification techniques help discover problems in system requirements
- To describe the use of algebraic techniques for interface specification
- To describe the use of model-based techniques for behavioral specification

Use of formal methods

- The principal benefits of formal methods are in reducing the number of faults in systems.
- Consequently, their main area of applicability is in critical systems engineering. There have been several successful projects where formal methods have been used in this area.
- In this area, the use of formal methods is most likely to be cost-effective because high system failure costs must be avoided.

Verification

Demonstrating that a program meets its specifications by a formal argument based upon the structure of the program.

Validation

Demonstrating that a program meets its specifications by testing the program against a series of data sets.

Validation assumes an execution of the model; Verification generally does not.

What is Formal Model Animator?

- Visual representation of formal model

Why should we use Formal Model Animator?

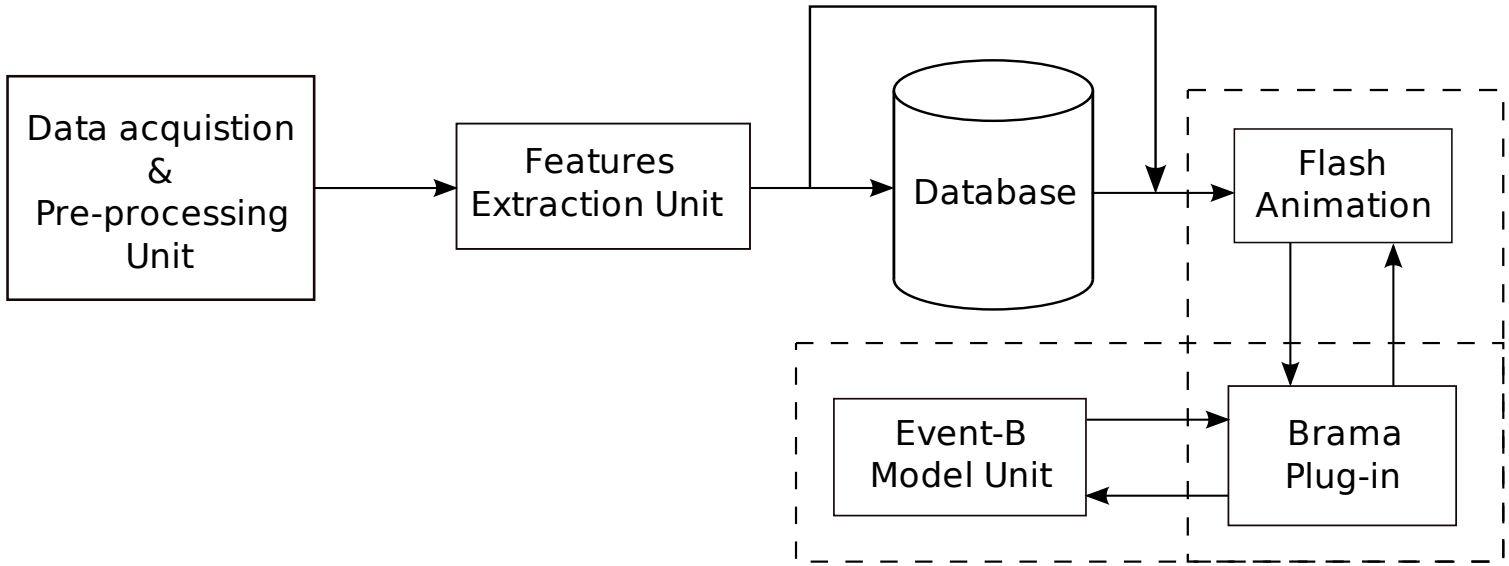
- To validate system behavior according domain experts
- To express formal model to non-mathematical domain experts
- To discover error in early stage of system development
- To provide confidence in system development
- Evidence based certification

Existing approach for animation

- Toys data set
- Default data initialization
- Randomize data input

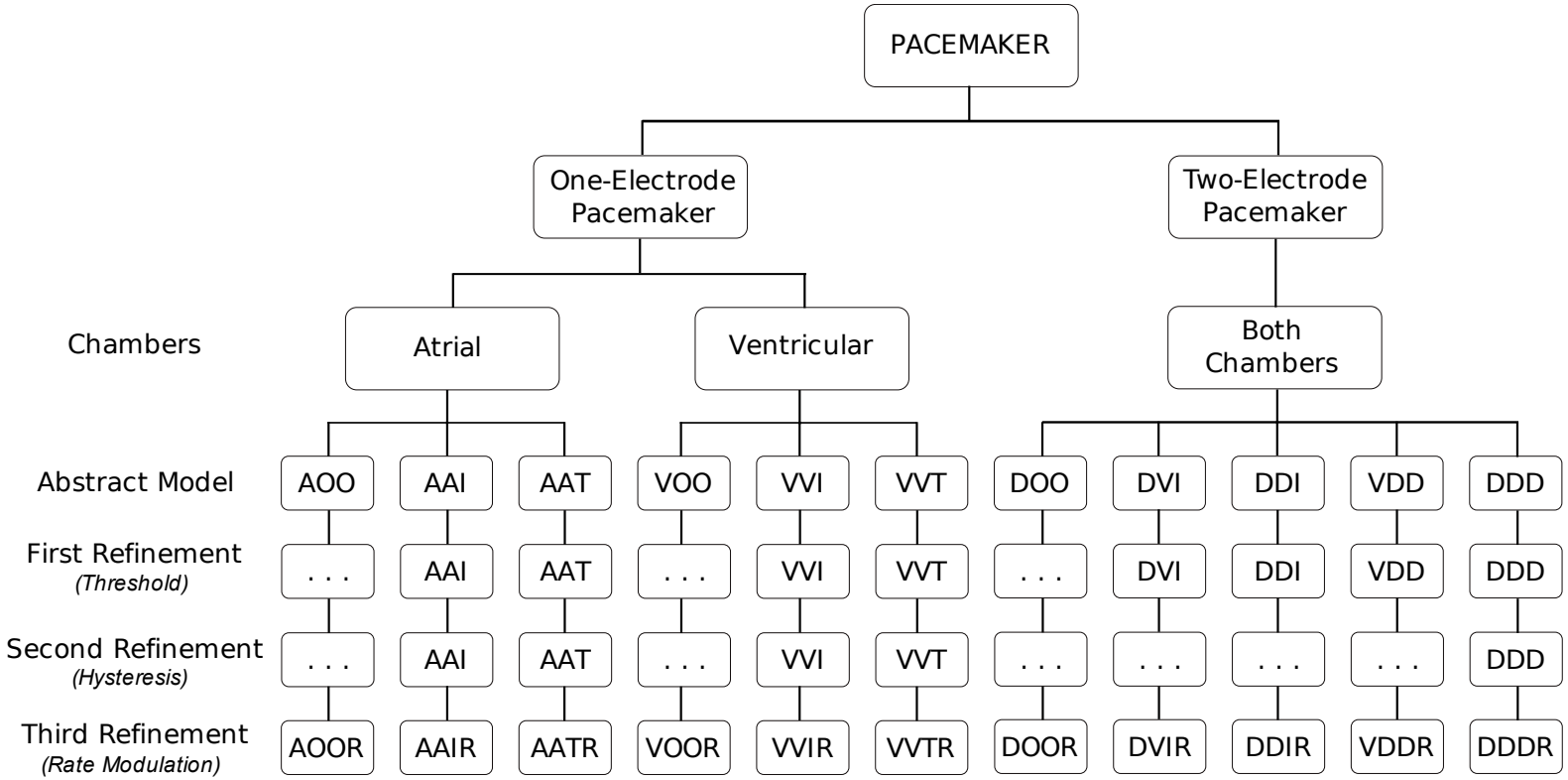
Hence, Model testing on *Toys data*.
Problem:No Real-time evidence based model testing.

An Architecture of Real-time Animator



1. Informal Requirements is available at McMaster University (SQRL).
2. One and Two-electrode pacemaker development using refinement-based incremental development.
3. Cover possible operating modes of pacemaker (i.e. Sensing threshold value, Hysteresis mode (ON and OFF) and Rate modulation)
4. Refinements relation among modes with different parameters.
5. Real-time animator help to analyze the current pacemaker challenges, to discover new operating modes and analyze the new behavior of the system.

One and Two-Electode Pacemaker



ProB

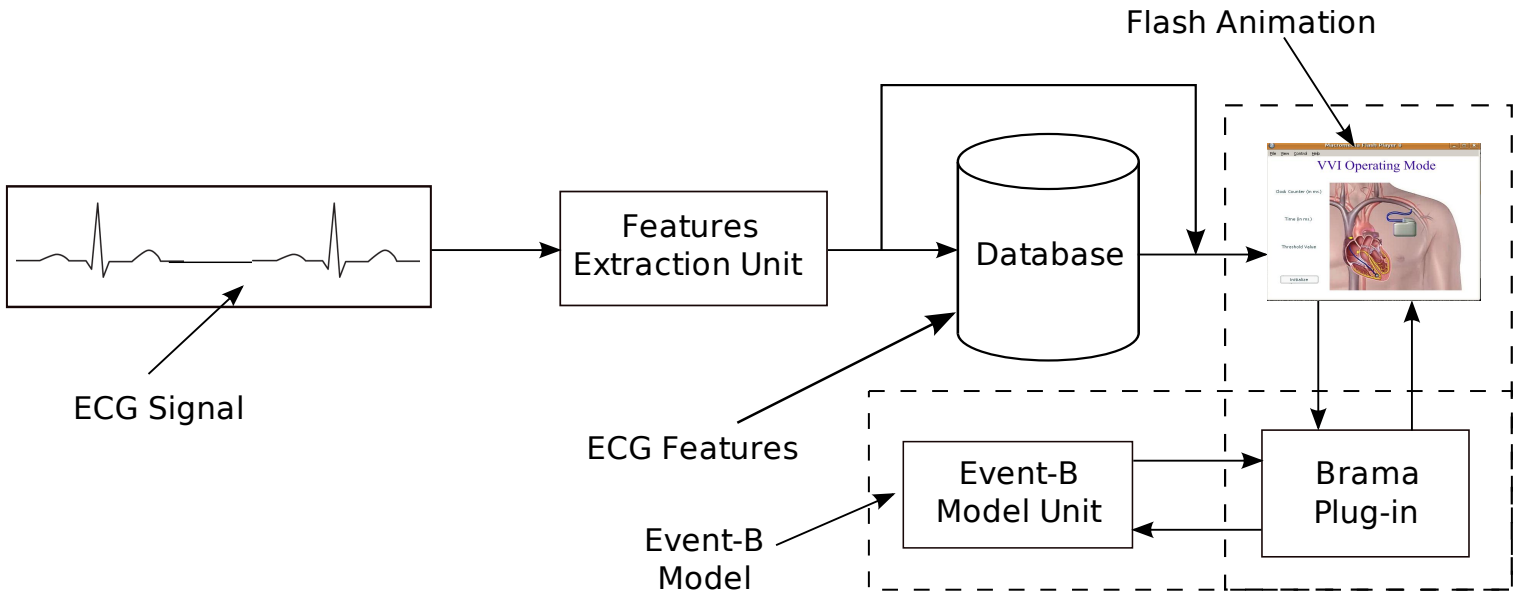
Model Checker used to verify the Event-B model and correctness of operating modes.

Proof Statistics

Model	Total number of POs	Automatic Proof	Interactive Proof
One-electrode pacemaker			
Abstract Model	159	134(84%)	25(16%)
First Refinement	44	40(91%)	4(9%)
Second Refinement	36	24(66%)	12(34%)
Third Refinement	80	80(100%)	0(0%)
Two-electrode pacemaker			
Abstract Model	166	125(76%)	41(24%)
First Refinement	211	190(90%)	21(10%)
Second Refinement	18	15(90%)	3(10%)
Third Refinement	67	66(99%)	1(1%)
Total	781	674(86%)	107(14%)

Table: Proof statistics

Real-time Animation : Pacemaker



- MIT-BIH Database Distribution
- Algorithms to calculate ECG Features *(http://ecg.mit.edu/index.html)*

How Real-time Animation can help in certification?

- Easy to explain model behavior to domain experts.
- Real-time evidence-based testing of system specification.
- Helps to domain experts to analyze work process guidelines (such as medical protocols or guidelines).
- Last but not least - System testing early stage of development without generating the source code.
- Simulation assists to regulatory agencies.
- Helps to meet ISO/IEC and IEEE standards.
- Improving Requirements using simulation
- Improving Error Detection

- Our approach places great emphasis on certification from requirements handling within lifecycle
  - Requirements Review
  - Traceability of Tests to Requirements
  - French-Italienne based pacemaker company and Medical Experts are agree on this prototype tool and real time results.
- This methodology encourages a view separate from the main 'development' lifecycle (a 'reaction' to the evolving design)
- The pacemaker case study indicates using our approach to find the critical conditions of operating modes (i.e. failure to sense).
- Real-time animator using pacemaker case study help to analyze the current pacemaker challenges, to discover new operating modes and analyze the new behavior of the system.

Limitation

- Data acquisition support
- Real-time Algorithm

Future Work

1. Apply our approach on more case studies.
2. Live demo for model animation using Data acquisition hardware.
3. To write API for interfacing hardware and formal model.
4. To support multiple formal modeling languages(TLA$^+$, Alloy, Z, CSP, VDM etc.).

Thank You!