Automata for Real-time Systems

B. Srivathsan

Chennai Mathematical Institute

In this lecture

An **academic case-study** that investigates methods to build **more reliable** pacemakers

Lecture 10:
Towards reliable pacemakers

References

Modeling and verification of a dual chamber implantable pacemaker

Jiang, Pajic, Moarref, Alur, Mangharam. TACAS'12

Heart-on-a-chip: A closed-loop testing platform for implantable pacemakers

Jiang, Radhakrishnan, Sampath, Sarode, Mangharam. 2013

`mlab.seas.upenn.edu`

Heart and pacemaker basics

Presentation of Zhihao Jiang (U Penn)

Pacemaker software

In-built **algorithms** to **detect** and **terminate** various abnormal heart conditions

Pacemaker software

In-built **algorithms** to **detect** and **terminate** various abnormal heart conditions

At least **6** implanted medical devices were recalled in 2010 due to likely software defects

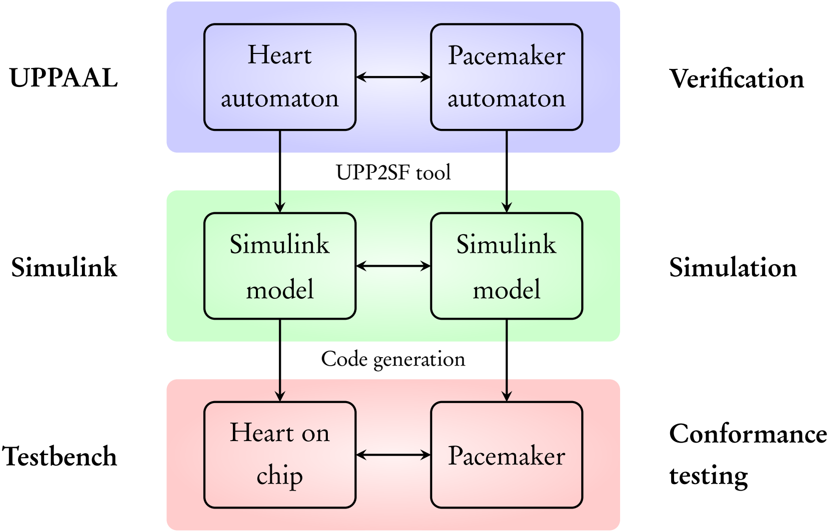
Killed by Code: Software Transparency in Implantable Medical Devices

Karen Sandler, Lysandra Ohrstrom, Laura Moy, Robert McVay

Two possible solutions for more reliable devices:

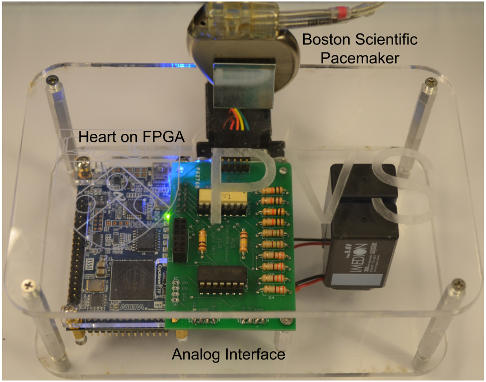
- **Model-based** system/software **design**
- **Closed-loop** testing

Model-based system/software design

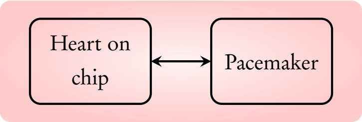


(Simulink is a commercial tool developed by Mathworks Inc.)

Closed-loop testing



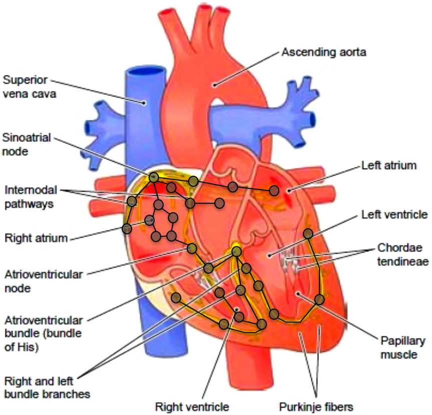
Testbench



Conformance testing

Coming next: Modeling and verification of heart and pacemaker

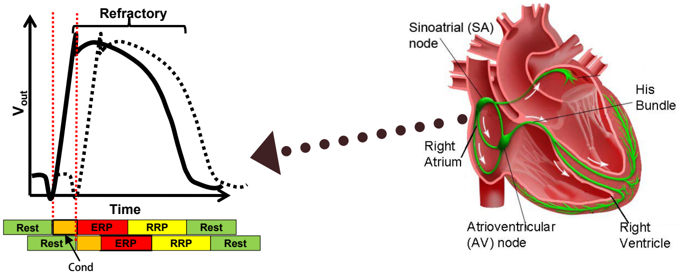
Heart as a timed automaton

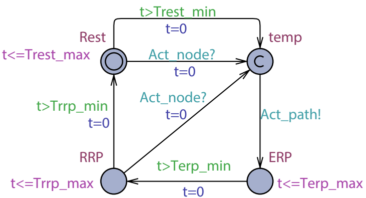


Abstract electrical conduction system of heart into **nodes** and **paths**

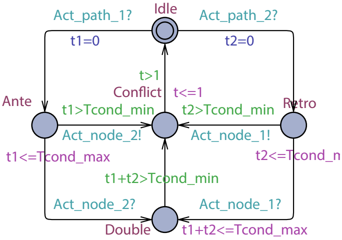
Picture credits: A Simulink hybrid heart model for quantitative verification of cardiac pacemakers

Chen *et. al*. HSCC'13





Node



Path

Parameters Trest_max, Trrp_min, etc. chosen acc. to node placement and patient history

Heart automaton H: $N_1 \mid\mid P_1 \mid\mid N_2 \mid\mid P_2 \mid\mid \ldots \mid\mid N_k$

N_i Node automaton

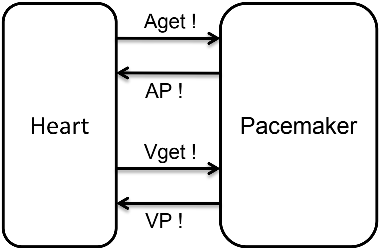
P_i Path automaton

k Number of nodes to which heart is abstracted

$\mid\mid$ Parallel composition (asynchronous product construction)

Pacemaker as a timed automaton

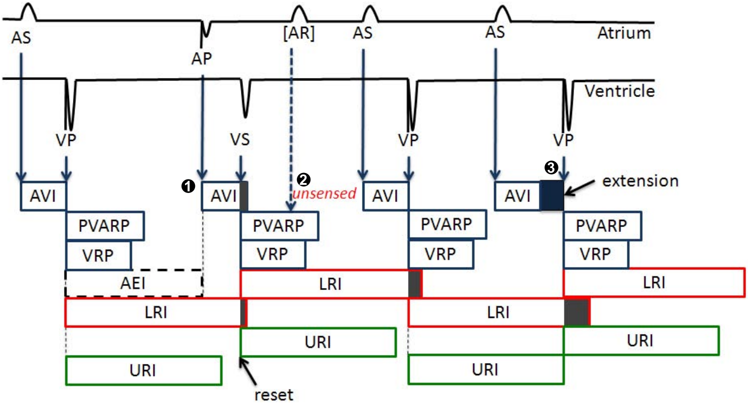
Heart-pacemaker interaction

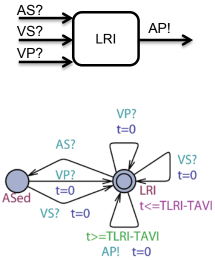


$$N^1.\ Act\_Path! \rightarrow\ Aget!$$
$$N^2.\ Act\_Path! \rightarrow\ Vget$$

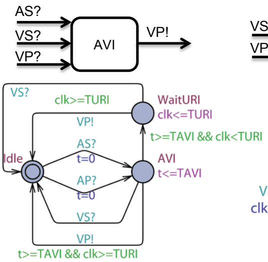
N^1 node at atrial lead
N^2 node at ventricular lead

Pacemaker timing cycles

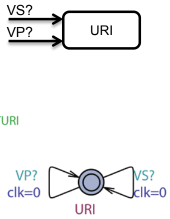




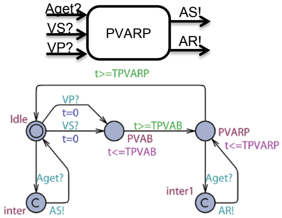
(a) LRI component



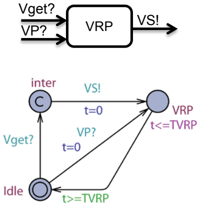
(b) AVI component



(c) URI component



(d) PVARP component



(e) VRP component

Pacemaker automaton P: *LRI* || *AVI* || *URI* || *PVARP* || *VRP*

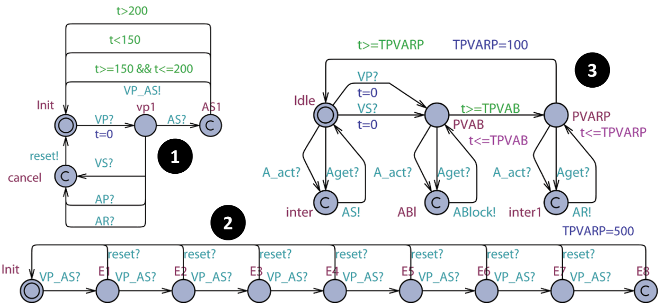
Heart-pacemaker automaton: $H \parallel P$

An algorithm for Endless Loop Tachycardia

Endless Loop Tachycardia (ELT)

Slides of Zhihao Jiang

- **ELT-detection:** If **VP-AS pattern** within 500ms for at least 8 times
- **ELT-termination:** **Increase** PVARP to 500ms **once**

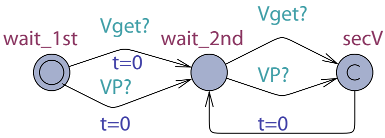


1 VPAS 2 ELTct 3 PVARP'

Pacemaker P_1: $LRI \mid\mid AVI \mid\mid URI \mid\mid PVARP' \mid\mid VRP \mid\mid ELTct \mid\mid VPAS$

Is the modified pacemaker safe?

Question 1: Are 2 ventricular events within time?



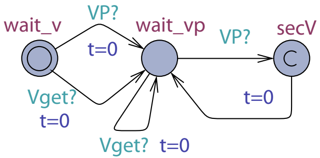
(a) Monitor PLRI_test

Check in UPPAAL if in $H \parallel P_1 \parallel PLRItest$, all paths satisfy

$$PLRItest.t \leq TLRI$$

Is the modified pacemaker safe?

Question 2: Are 2 ventricular events very fast?



(b) Monitor PURI_test

Check in UPPAAL if in $H \mid\mid P_1 \mid\mid PURItest$, all paths satisfy

$$PURItest.t \geq TURI$$

Each time new algorithm is added, **model** it and **check** if basic safety properties are satisfied

Take-home

- Model-based system/software design
- Closed-loop testing