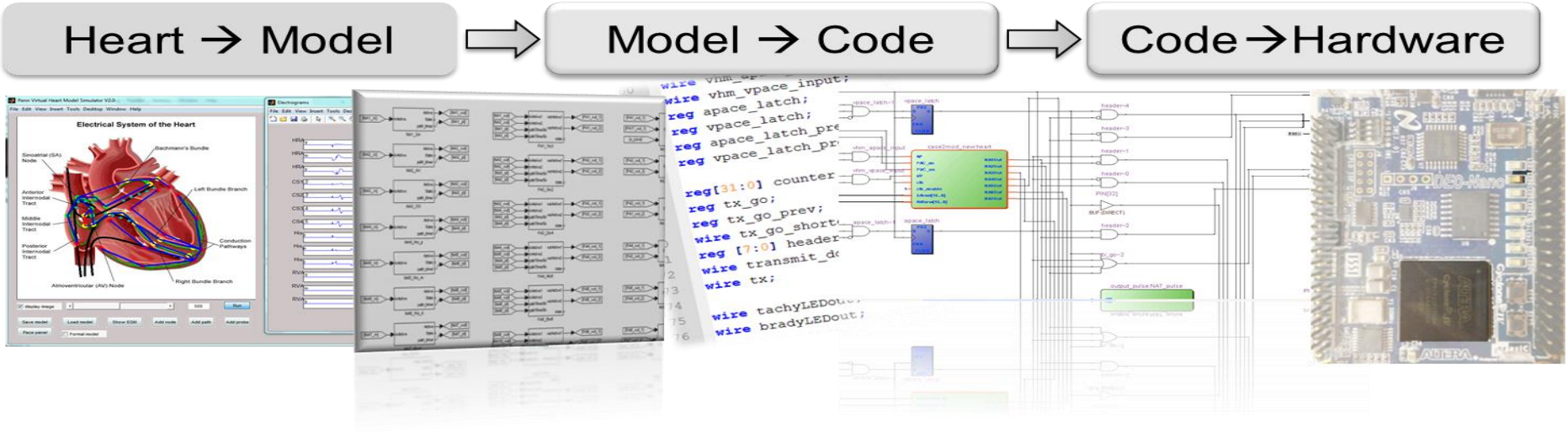


From Verified Models to Verified Code for Medical Devices

Miroslav Pajic and Rahul Mangharam

Dept. Electrical & Systems Engineering
University of Pennsylvania
{pajic, rahulm}@seas.upenn.edu

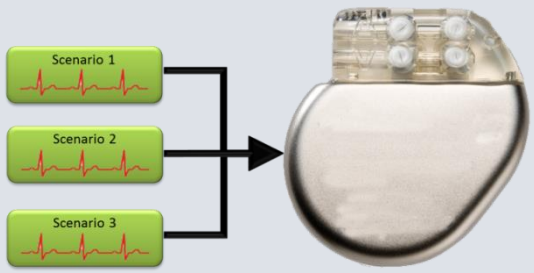
Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

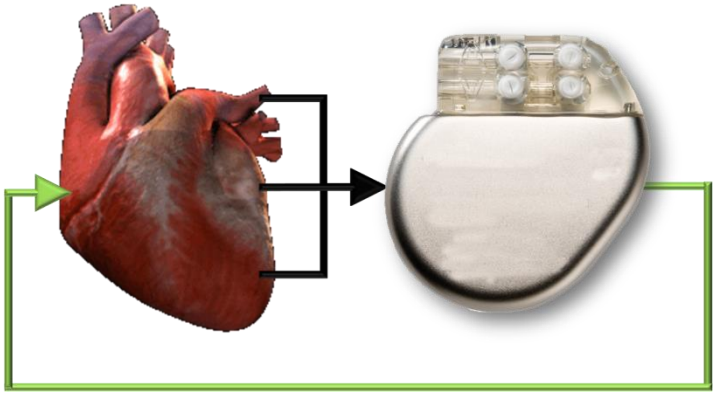
The Need for Closed-Loop Monitoring

- Software failures caused **24%** of all medical device recalls in 2011
- More than 1,500,000 ***software-based*** medical devices were recalled from 2002-2010

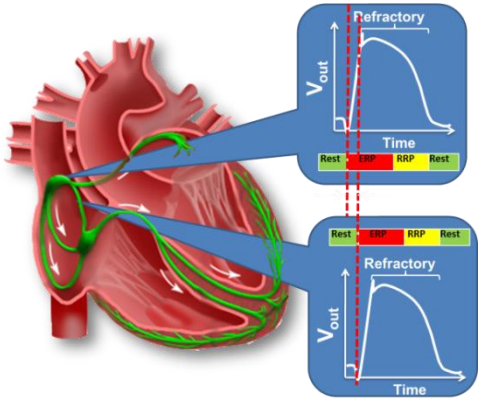
- **Problem**: No well-established standards for development of software for medical devices
  - Testing medical device software currently is ad-hoc, open-loop, and very expensive



- Our Approach: Verify and test the device software in ***closed-loop*** with its physical environment!
  - Model-Driven Development of pacemakers and PCA infusion pumps



Implantable Medical Devices – Cardiac Pacemakers



Heart | Pacemaker

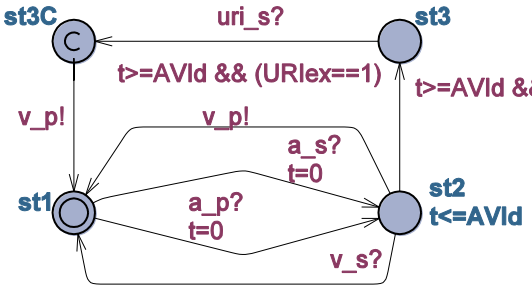
Verification: Random Heart Mode ⟺ UPPAAL Model

Interpolation | UPP2SF Model Translation

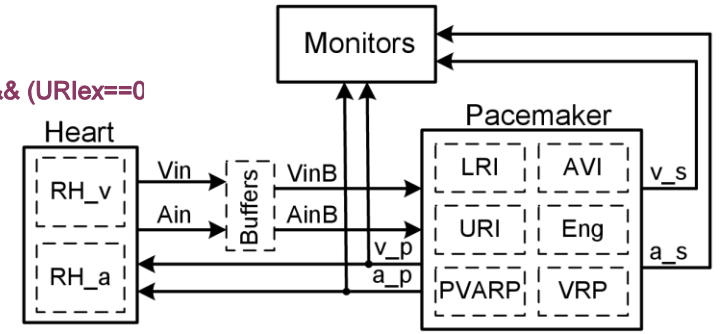
Simulation: Virtual Heart Model ⟺ Simulink Model

HDL Coder | Simulink Coder

Implementation: FPGA implementation ⟺ C Code implementation



AVI automaton

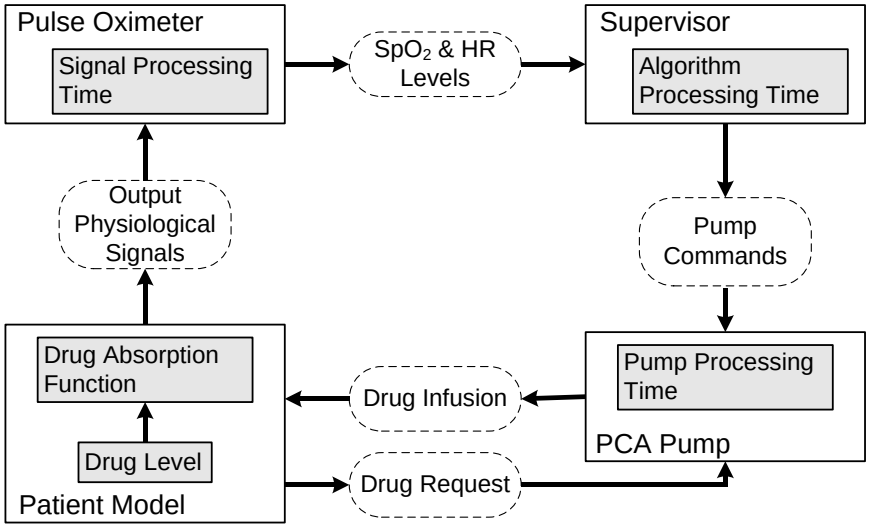


- Closed-loop safety properties are retained through the tool-chain
- Development of ***verified software from verified models***

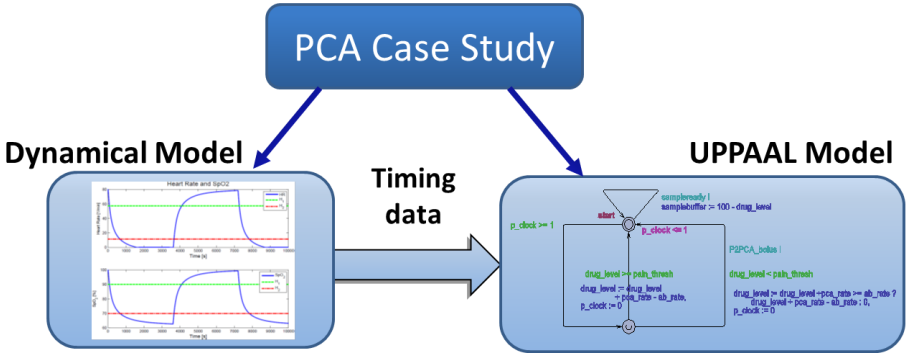
Patient Controlled Analgesia Case Study

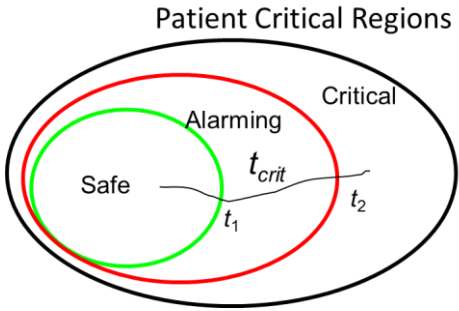
- A significant source of adverse events

Networked Physiological Control System



Modeling Approach





- Combining simulation-based analysis of a detailed system model with model checking of a timed-automata model
- The relationship between the two models preserves the crucial aspect of the timing behavior!

M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. Goldman, and I. Lee, "*Model-Driven Safety Analysis of Closed-Loop Medical Systems*", IEEE Transactions on Industrial Informatics, 2014

Thank You

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING