FROM VERIFIED MODEL TO VERIFIED CODE
FOR MEDICAL CYBER-PHYSICAL SYSTEMS

Dr. Zhihao Jiang
Real-Time & Embedded Systems Lab
Dept. Electrical & Systems Engineering
University of Pennsylvania
zhihaoj@seas.upenn.edu
MEDICAL CYBER-PHYSICAL SYSTEMS

Implantable Pacemaker
1990-2000: **600,000** implantable pacemakers were recalled

**200,000** of these recalls were due to software issue

2008-12: **15% of all** the medical device recalls (Class I, II & III) due to software
Core Challenges for Safe Medical CPS

• Messy Plant:
  – Partially understood physiology

• Large Variability:
  – Every patient is different

• Limited Observability:
  – Losing physiological context
High-confidence Software Development for Life-critical Cyber-Physical Systems
“Let our heart models catch bugs before your heart does.”
THRUSt 1:
MAINTAIN PHYSIOLOGICAL CONTEXT
WITH HEART MODELING
Periodically generates electrical impulses to initialize heart beats

SA node
Atrial Contraction

- An impulse first triggers muscle contractions in the atria, pushing blood into the ventricles.
• Delay at AV node which allows the ventricles to fill fully
Ventricular Contraction

- Strong muscle contractions pump blood out of the heart
Bradycardia

- Delay in generation and/or conduction of the electrical impulses results in low heart rate
• Local electrical activations
ATRIAL SENSING (AS)

- Generate sensed event when signal above threshold

Pacemaker
VENTRICULAR SENSE (VS)

- Same for ventricular channel
Atrial Pacing (AP)

- Pace atrium when no AS within deadline
VENTRICULAR PACING (VP)

- Pace ventricle if no VS happen within deadline
• Maximum interval between two ventricular events \((\text{max}(V-A)+\text{max}(A-V))\)
• Unnecessary details
• Infeasible model identification

Cellular Electrophysiology

Whole heart Electrophysiology

Tong et. al 2014

Deng et. al 2016
Electrical Conduction System

Refractory Time

$V_{out}$

Rest ERP RRP Rest

Rest ERP RRP Rest

$V_{out}$

Time

Refractory

Electro-physiology of the Heart
TIMED AUTOMATA HEART MODEL

Node Automata

Path Automata

Marked Automata
Represent variety of heart conditions using different topologies and timing parameters

Normal Sinus Rhythm  Atrial Flutter  Ventricle Tachycardia  AV Nodal Reentry
Heart Model Simulation

Electrical System of the Heart

- Sinoatrial (SA) Node
- Bachmann's Bundle
- Anterior Internodal Tract
- Middle Internodal Tract
- Posterior Internodal Tract
- Atrioventricular (AV) Node
- Left Bundle Branch
- Right Bundle Branch
- Conduction Pathways

Electrograms

- HRA
- HRa
- HRd
- CST 1
- CST 2
- CST 3
- CST 4
- CSA 1
- CSA 2
- CSA 3
- CSA 4
- Hisa
- Hisa
- Hisa
- RVA
- RVA
- RVA
- RVA
HEART MODEL VALIDATION

• Condition-specific heart models
Penn Virtual Heart Model v2.0
Atrial flutter simulation
CLOSED-LOOP HEART – PACEMAKER
ILLUSTRATING PACEMAKER MEDIATED TACHYCARDIA
HEART ON A CHIP PLATFORM

Heart On a Chip

Commercial Pacemaker

Analog Interface
THRUST 2: CAPTURE PHYSIOLOGICAL VARIABILITY WITH CLOSED-LOOP MODEL CHECKING
Model Checking

- Explore the whole reachable state space of a model for property violations
- Widely used in semi-conductor industries for verifying chip design
Observable Behavior Space

Initial Heart Models

<table>
<thead>
<tr>
<th>Heart Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Sinus Rhythm</td>
</tr>
<tr>
<td>Bradycardia</td>
</tr>
<tr>
<td>AV Block</td>
</tr>
<tr>
<td>Bundle Branch Block</td>
</tr>
<tr>
<td>Sinus Tachycardia</td>
</tr>
<tr>
<td>Atrial Flutter</td>
</tr>
<tr>
<td>AVNRT</td>
</tr>
<tr>
<td>Atrial Fibrillation</td>
</tr>
<tr>
<td>Premature Ventricle Contraction</td>
</tr>
<tr>
<td>Ventricle Tachycardia</td>
</tr>
<tr>
<td>Ventricle Fibrillation</td>
</tr>
</tbody>
</table>
• Properties satisfied by M are also satisfied by P1, P2
• Behaviors not exist in P1, P2 may also be physiologically-valid
• Is this a valid counter-example?
• Need a framework to provide context for counter-examples

Counter-example
Multiple transitions are enabled
Relax guard conditions

if $t \in [1,5]$  
s=1
Simplify the model to increase non-determinism for more behavior coverage.
Combine models of different heart conditions for more behavior coverage
Initial Heart Models

Observable Behavior Space
ABSTRACTION TREE: HEART MODEL ABSTRACTION

Heart Conditions

- Normal Sinus Rhythm
- Bradycardia
- AV Block
- Bundle Branch Block
- Sinus Tachycardia
- Atrial Flutter
- AVNRT
- Atrial Fibrillation
- Premature Ventricle Contraction
- Ventricle Tachycardia
- Ventricle Fibrillation
Observable Behavior Space
ABSTRACTION TREE: HEART MODEL REFINEMENT

Heart Conditions

- Normal Sinus Rhythm
- Bradycardia
- AV Block
- Bundle Branch Block
- Sinus Tachycardia
- Atrial Flutter
- AVNRT
- Atrial Fibrillation
- Premature Ventricle Contraction
- Ventricle Tachycardia
- Ventricle Fibrillation

Variability

Observable Behavior Space

Physiological Context

39
• Basic Safety Properties
  – Heart rate never go too slow
  – Pacemaker never increase the heart rate too high

• Pacemaker Mediated Tachycardia
  – Can pacemaker increase heart rate inappropriately?
  – Are there multiple cases of them?
  – Can the algorithm terminate the behavior in time?
THRUST 3: VERIFIED MODEL TO VERIFIED CODE
FROM VERIFIED MODEL TO VERIFIED CODE

Heart

Model Checking
- Non-deterministic
- UPPAAL Model
- Refinement

Simulation
- Deterministic VHM
- Stateflow Chart
- HDL Coder

Platform Testing
- Heart-on-Chip
- C Code implementation

Pacemaker

Model Translation
- UPP2SF Model Translation

Simulink Coder

Research Impact

Model-based Design
- RTAS’12 (Best Paper Award)
- TECS’14
- FnEDA’16
- IEEE Computer’16

Formal Methods
- TACAS’12 (Best Paper Nominee)
- STTT’14
- MedCPS’16
- HSCC’16

Cyber-Physical Systems
- ICCPS’11
- ECRTS’11
- IEEE Proceedings’12

Biomedical Engineering
- EMBC’10
- EMBC’11
- EMBC’16
Research Summary & Plan

Development

Heart Modeling
Closed-loop Model Checking
Model Translation

Clinical

Quantitative Validation
Security Verification
in-silico Pre-clinical Trials
Data-driven Modeling

Providing Regulatory-grade Safety Evidence With Computer Models
Safety Evidence for Medical Devices

Today
- Animal
- Bench
- Computer

Future
- Animal
- Bench
- Human
- Computer
Research Summary & Plan

Development
- Heart Modeling
- Closed-loop Model Checking
- Model Translation

Clinical
- Quantitative Validation
- Security Verification
- in-silico Pre-clinical Trials
- Data-driven Modeling

Providing Regulatory-grade Safety Evidence With Computer Models
The clinical trial

Animal testing

The ultimate closed-loop validation
Implantable Cardiac Defibrillator

- Shock Coils
- Right Ventricular Lead Tip & Ring
- Left Atrium
- Left Ventricle
- Right Atrium
- Right Ventricle
- ICD Can (Shock)
- Electrode
- Sense
- Therapy
- Atrial Signal
- Ventricular Signal
- Shock Signal

AS VS
AS VS
AS VS
RIGHT
The Rhythm ID Going Head to Head Trial*

Primary endpoint: occurrence of inappropriate therapy

~2,000 patients, 5 years

Select Medtronic ICDs (the control arm)

Vitality II ICD (Boston Sci.) (the treatment arm)

Assumed 25% less risk of inappropriate therapy with Vitality II relative to Medtronic ICDs

RIGHT Trial Results – Inappropriate Therapy

Gold et al. RIGHT of Inappropriate ICD Therapy

Table 2  Adjudication summary of spontaneous episodes where therapy was delivered

<table>
<thead>
<tr>
<th>Adjudicated rhythm</th>
<th>VITALITY 2</th>
<th>Selected Medtronic</th>
<th>Overall</th>
<th>P value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifact</td>
<td>23 (1.1)</td>
<td>90 (4.6)</td>
<td>113 (2.8)</td>
<td>.0094</td>
</tr>
<tr>
<td>Ventricular tachycardia</td>
<td>705 (34.9)</td>
<td>994 (51.0)</td>
<td>1699 (42.8)</td>
<td>.2490</td>
</tr>
<tr>
<td>Ventricular fibrillation</td>
<td>59 (2.9)</td>
<td>61 (3.1)</td>
<td>120 (3.0)</td>
<td>.4265</td>
</tr>
<tr>
<td>Sinus tachycardia</td>
<td>506 (25.0)</td>
<td>220 (11.3)</td>
<td>726 (18.3)</td>
<td>&lt;.0001</td>
</tr>
<tr>
<td>Atrial fibrillation</td>
<td>431 (21.3)</td>
<td>101 (5.2)</td>
<td>532 (13.4)</td>
<td>&lt;.0001</td>
</tr>
<tr>
<td>Atrial flutter</td>
<td>66 (3.3)</td>
<td>19 (1.0)</td>
<td>85 (2.1)</td>
<td>.0076</td>
</tr>
<tr>
<td>Atrial tachycardia</td>
<td>20 (1.0)</td>
<td>100 (5.1)</td>
<td>120 (3.0)</td>
<td>.0001</td>
</tr>
<tr>
<td>AVNRT</td>
<td>17 (0.8)</td>
<td>39 (2.0)</td>
<td>56 (1.4)</td>
<td>.5956</td>
</tr>
<tr>
<td>Other supraventricular tachycardia/unknown</td>
<td>178 (8.8)</td>
<td>325 (16.7)</td>
<td>503 (12.7)</td>
<td>.4436</td>
</tr>
<tr>
<td>Sinus rhythm with premature ventricular complexes</td>
<td>18 (0.9)</td>
<td>1 (0.1)</td>
<td>19 (0.5)</td>
<td>NE</td>
</tr>
<tr>
<td>Total events</td>
<td>2023</td>
<td>1950</td>
<td>3973</td>
<td></td>
</tr>
</tbody>
</table>

NE = nonestimable; AVNRT = Atrioventricular nodal re-entry tachycardia.

Inappropriate Therapy

VITALITY 2: 62.2%
Medtronic: 45.9%

Majority of the therapy episodes were inappropriate

*Michael R. Gold, Primary results of the Rhythm ID Going Head to Head Trial, Heart Rhythm, Vol 9, No 3, March 2012
in-silico Pre-Clinical Trials

1. Real Patient Data for Adjudication & Extraction
   - Adjudicated EGM Database
     - Patient A
     - Patient B
     - Patient C
     - N Patient Records
     - M Episodes

2. Synthetic Heart Model Generation
   - Generating synthetic heart models

3. Cohort Generation
   - Complete Generated Population

4. Device Testing & Evaluation
   -Boston Scientific ICD
   - Medtronic ICD
   - Diagnosis Sensitivity and Specificity

Learn Parameter distribution
Sampling parameters from distribution
10,000's Condition-specific Model Generation
10,000's Condition-specific electrograms
Closed-loop evaluation

Result 1: Specificity across populations

Atrial fibrillation  Atrial flutter  PVC  Non-sustained VT  Other SVT  Double Tachycardia  Ventricular Fibrillation  Ventricular Tachycardia
Result 1: Specificity across populations
Result 2: Patient Condition-level Analysis

Table 1: Specificity for SVTs and sensitivity for VTs.

<table>
<thead>
<tr>
<th>Arrhythmia</th>
<th>Boston Sci. ICD</th>
<th>Medtronic ICDs</th>
<th>P value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specificity (%)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Atrial Fibrillation</td>
<td>99.8</td>
<td>99.6</td>
<td>0.3167</td>
</tr>
<tr>
<td>Atrial flutter</td>
<td>58.3</td>
<td>79.33</td>
<td>&lt;0.0001</td>
</tr>
<tr>
<td>Premature ventricular complexes</td>
<td>100</td>
<td>100</td>
<td>1</td>
</tr>
<tr>
<td>Nonsustained ventricular tachycardia</td>
<td>100</td>
<td>99.8</td>
<td>0.3171</td>
</tr>
<tr>
<td>Other Supraventricular tachycardia</td>
<td>96.3</td>
<td>99.7</td>
<td>&lt;0.0001</td>
</tr>
<tr>
<td>Brady-Tachy</td>
<td>100</td>
<td>98.83</td>
<td>0.0079</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensitivity (%)</th>
<th>P value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ventricular fibrillation</td>
<td>100</td>
</tr>
<tr>
<td>Ventricular tachycardia</td>
<td>100</td>
</tr>
</tbody>
</table>
In-Silico Pre-Clinical Trials Toolchain

**Patient Data Management**
- Virtual Cohort Generation
- Simulated Trial
- Device in the Loop
- Trial Results

**Patient Data Management**
- Patient Data Management
- Virtual Cohort Generation
- Simulated Trial
- Device in the Loop
- Trial Results

**Virtual Cohort Generation**
- Unlabeled patient data is annotated
- Timing and morphology information is extracted
- Virtual cohort is generated from extracted information
- Software simulation using virtual cohort
- Hardware validation with actual physical device
- Analysis of results

**Patient Information**
- File: AAE198A.xls
  - Name: 198
  - Age: 85
  - Sex: Male
  - Diagnosis: CAD

**Patient EGM Data**
- EGM Record
  - Filter
  - Annotated
  - Signatures

**Analysis of results**
Device-in-the-loop Testing
Understanding the Application Domain
Medical Collaborators

Heart model development and validation, Device algorithm, De-identified Patient data

Director, Cardiac Electrophysiology, Philadelphia VA Medical Center

Developing clinical assist system for atrial fibrillation

Director, Electrophysiology Laboratories, Penn Cardiology, Penn Presbyterian Medical Center

Heart Model development and validation, ICD discrimination algorithm development, in silico Pre-clinical trials

Electrophysiology Fellow, Hospital of the University of Pennsylvania
Industrial Collaborations

- Provided algorithm descriptions, sample devices, programmers, testing platform
- Provided algorithm descriptions, sample devices, programmers, test cases
- Provided model-based design toolbox
- Provided software and hardware
CyberCardia
NSF CPS Frontier

5 Computer Scientists, 2 Cardiologists, 1 Physicist, 1 BioMed Engineer, 2 Mathematicians, 1 Electrical Engineer
Thanks!

Questions?