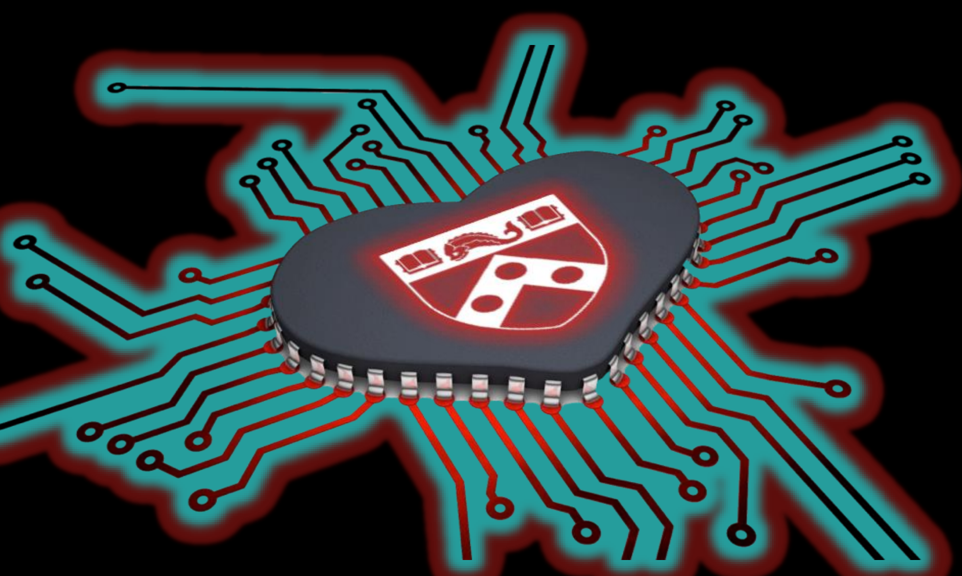
FROM VERIFIED MODEL TO VERIFIED CODE

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

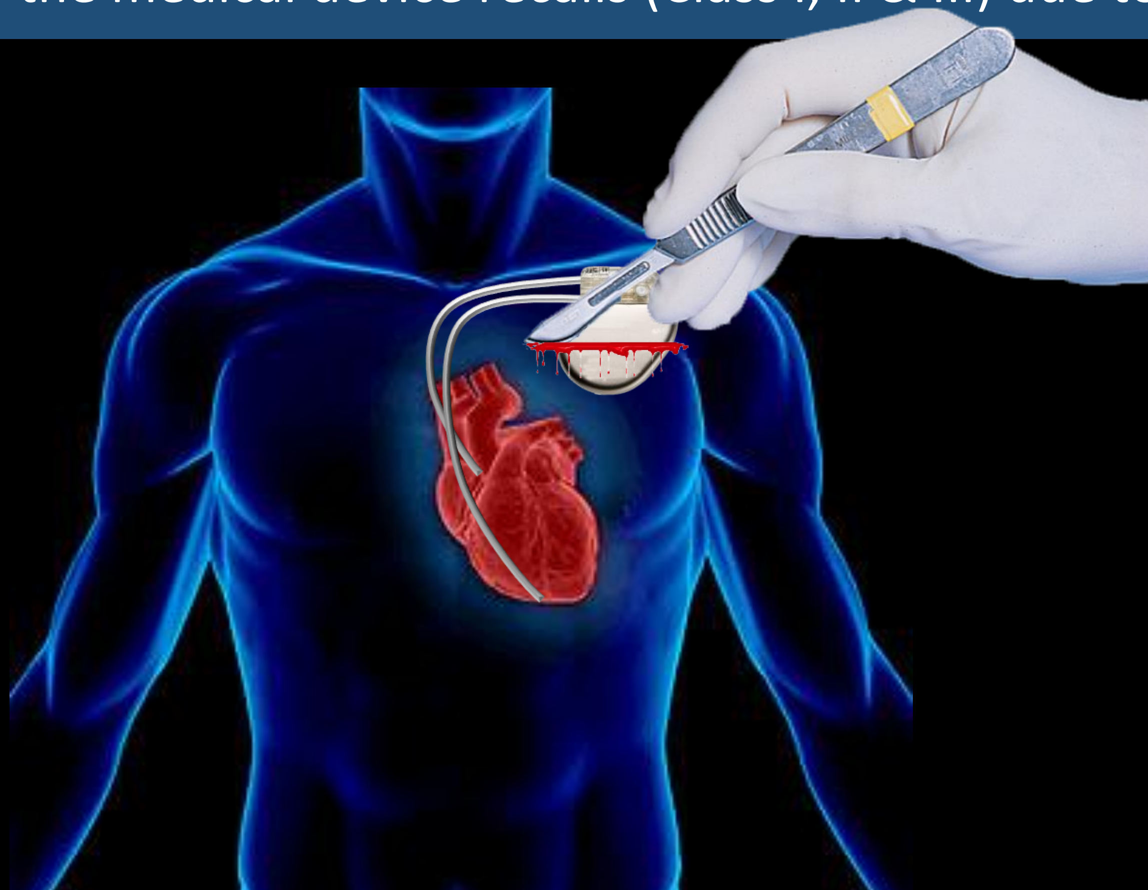
Implantable Pacemaker

The Problem –
Medical Device Recalls Due to Software

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

200,000 of these recalls were due to software issue

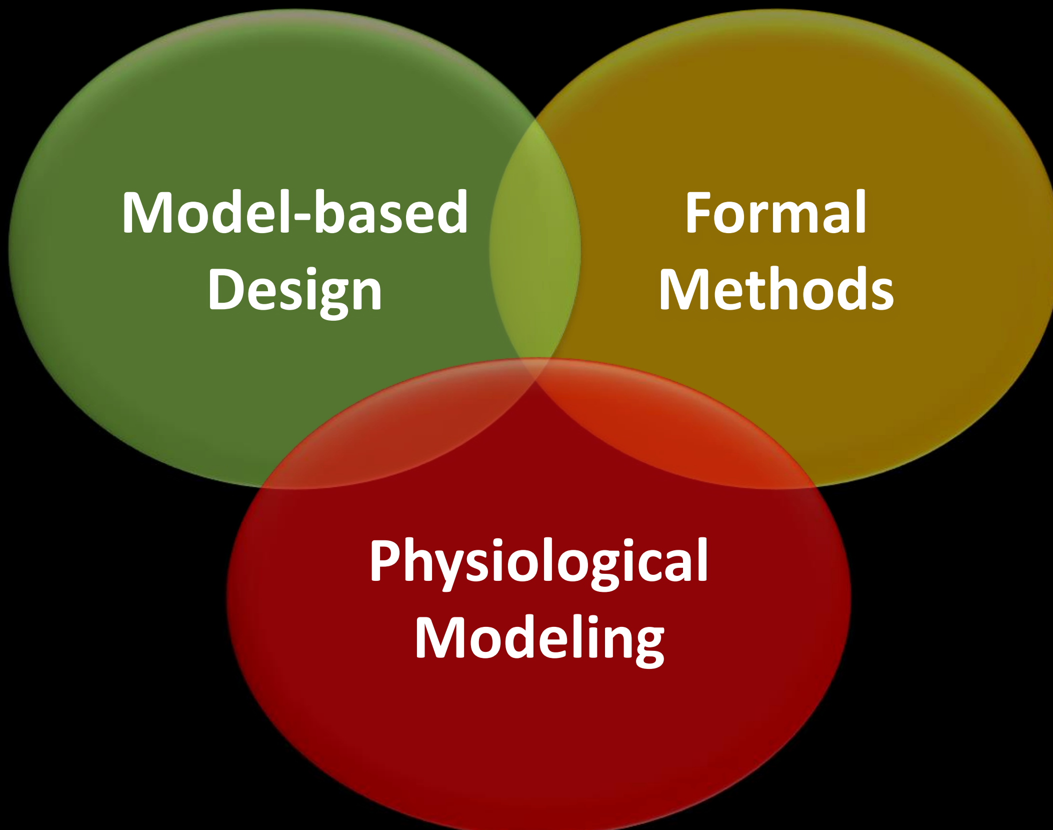
2008-12: **15% of *all*** the medical device recalls (Class I, II & III) due to software



Core Challenges for Safe Medical CPS

- **Messy Plant:**
  – Partially understood physiology
- **Large Variability:**
  – Every patient is different
- **Limited Observability:**
  – Losing physiological context

Research Scope



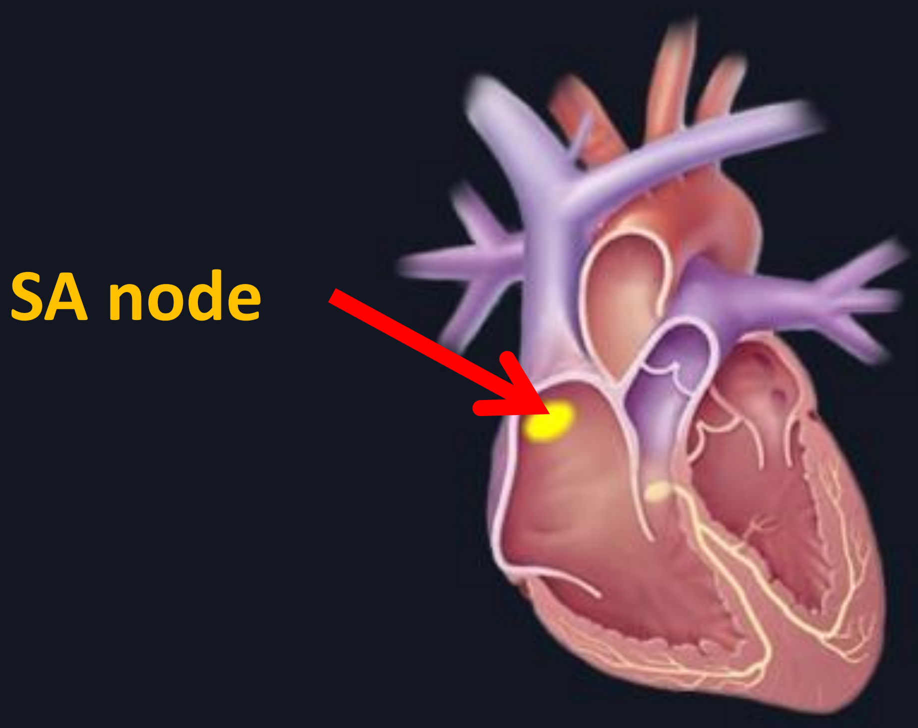
High-confidence Software Development for Life-critical Cyber-Physical Systems

"Let our heart models catch bugs before your heart does."

Thrust 1: Maintain Physiological Context with Heart Modeling

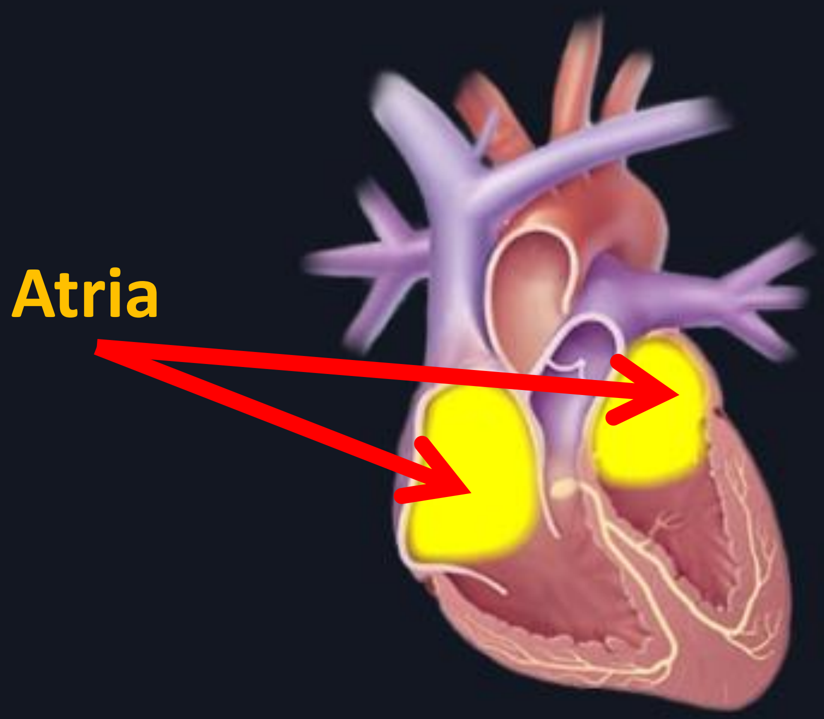
Natural Pacemaker

- Periodically generates electrical impulses to initialize heart beats



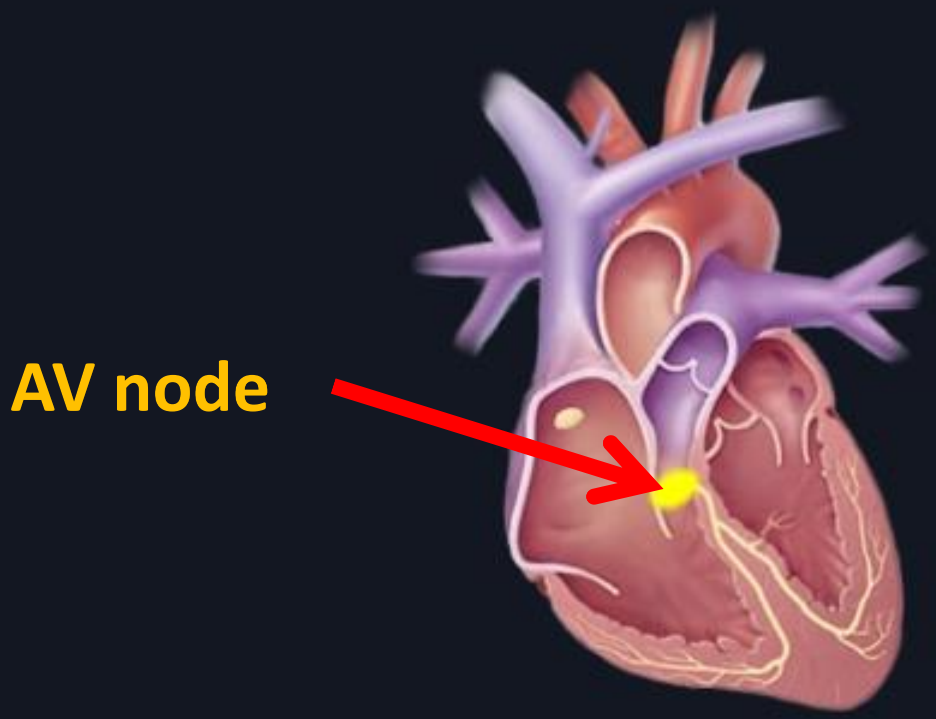
Atrial Contraction

- An impulse first triggers muscle contractions in the atria, pushing blood into the ventricles



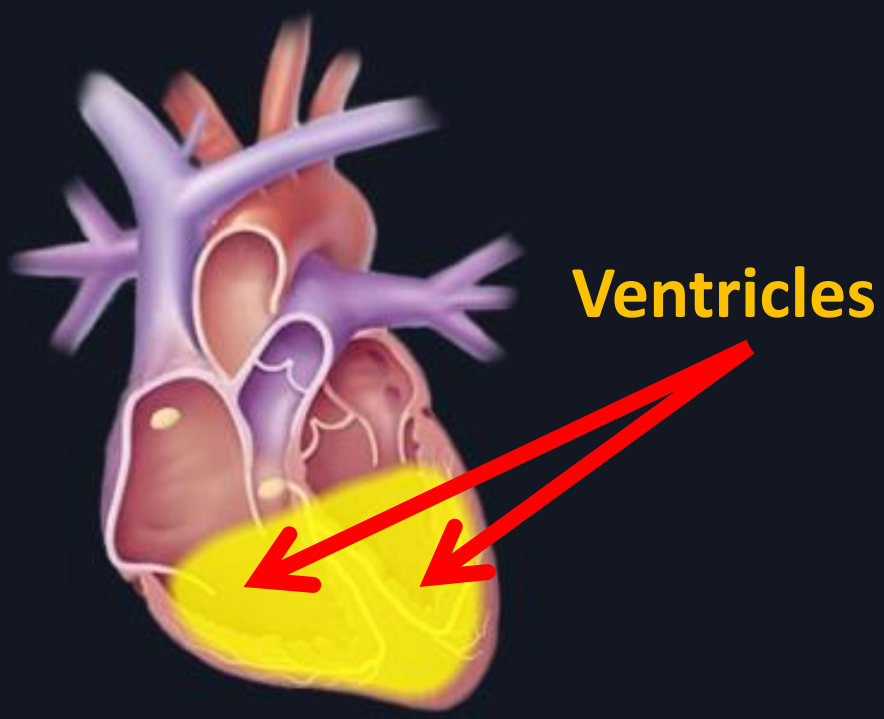
Delay At AV Node

- Delay at AV node which allows the ventricles to fill fully



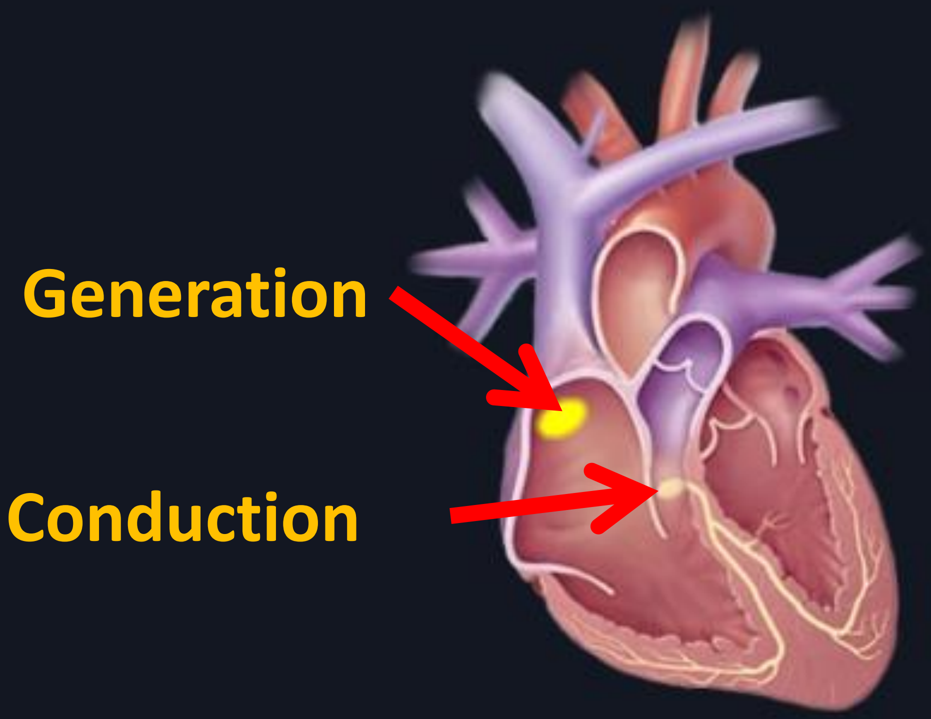
Ventricular Contraction

- Strong muscle contractions pump blood out of the heart



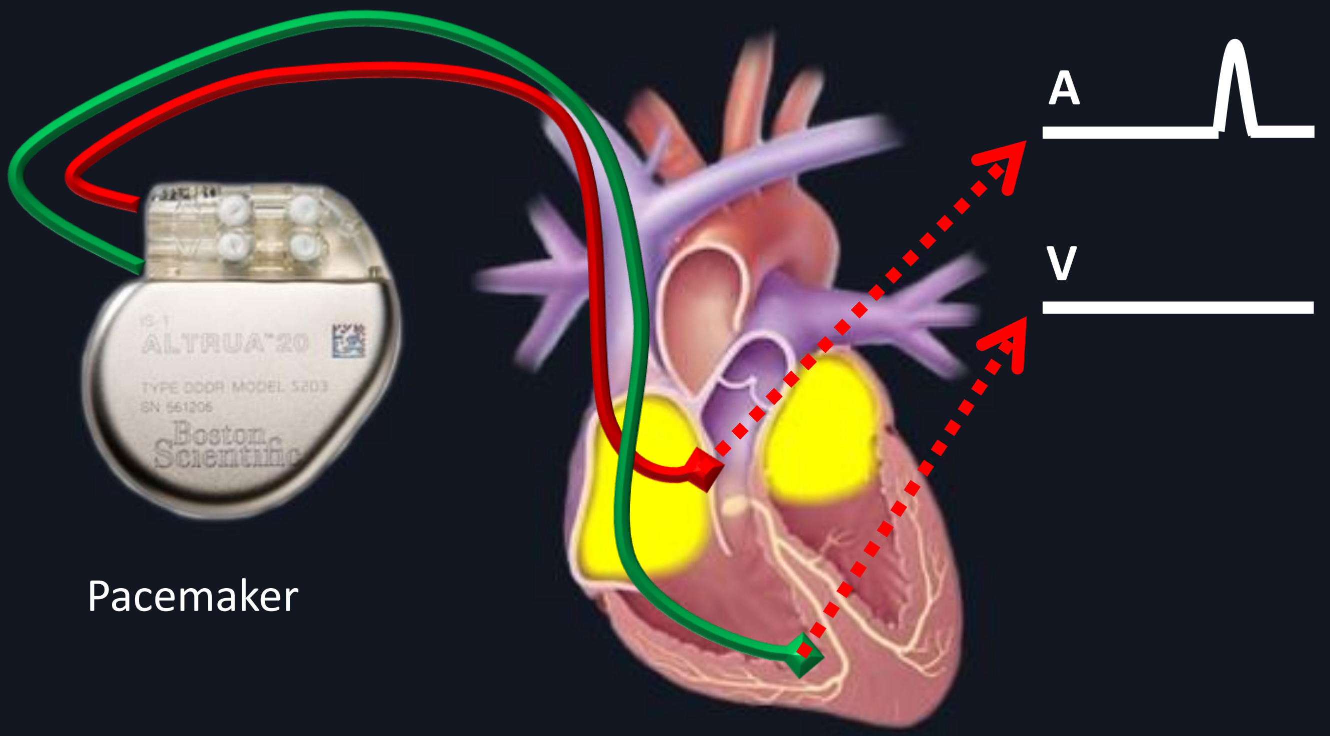
BRADYCARDIA

- Delay in generation and/or conduction of the electrical impulses results in low heart rate



Pacemaker Sensing

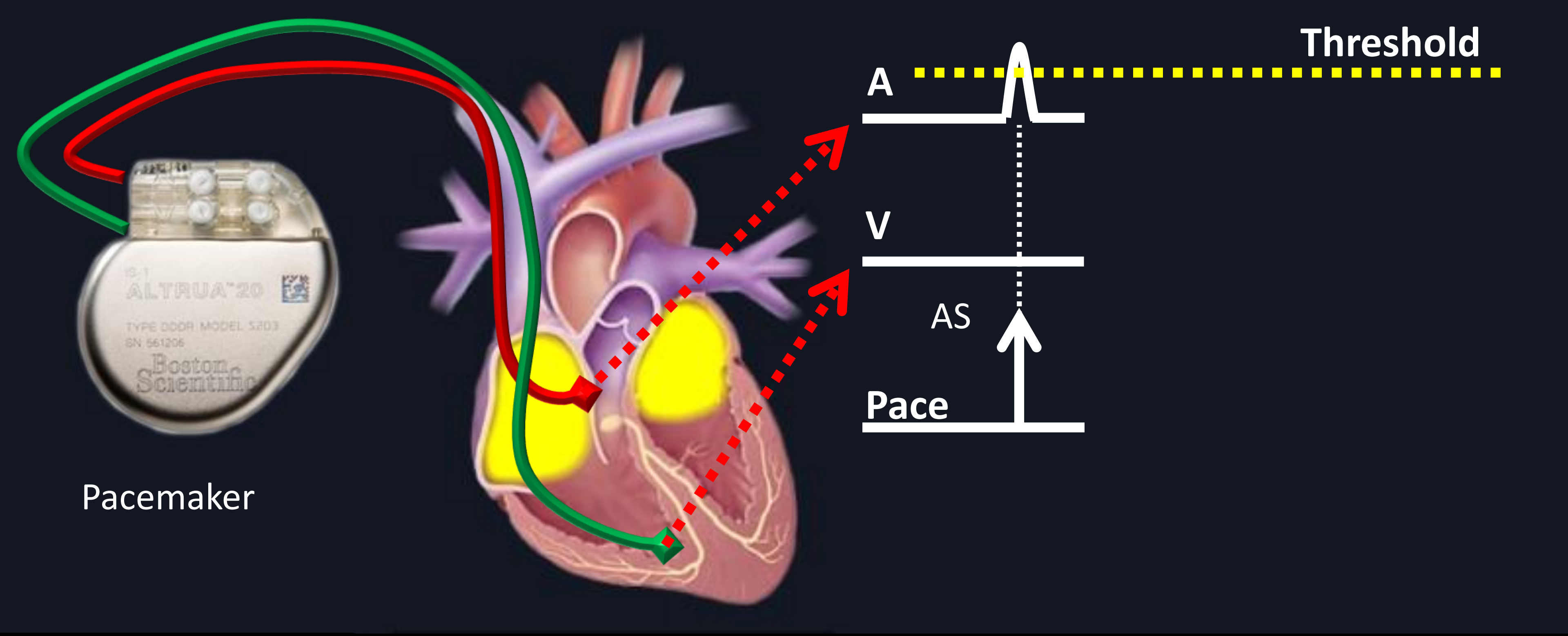
- Local electrical activations



Pacemaker

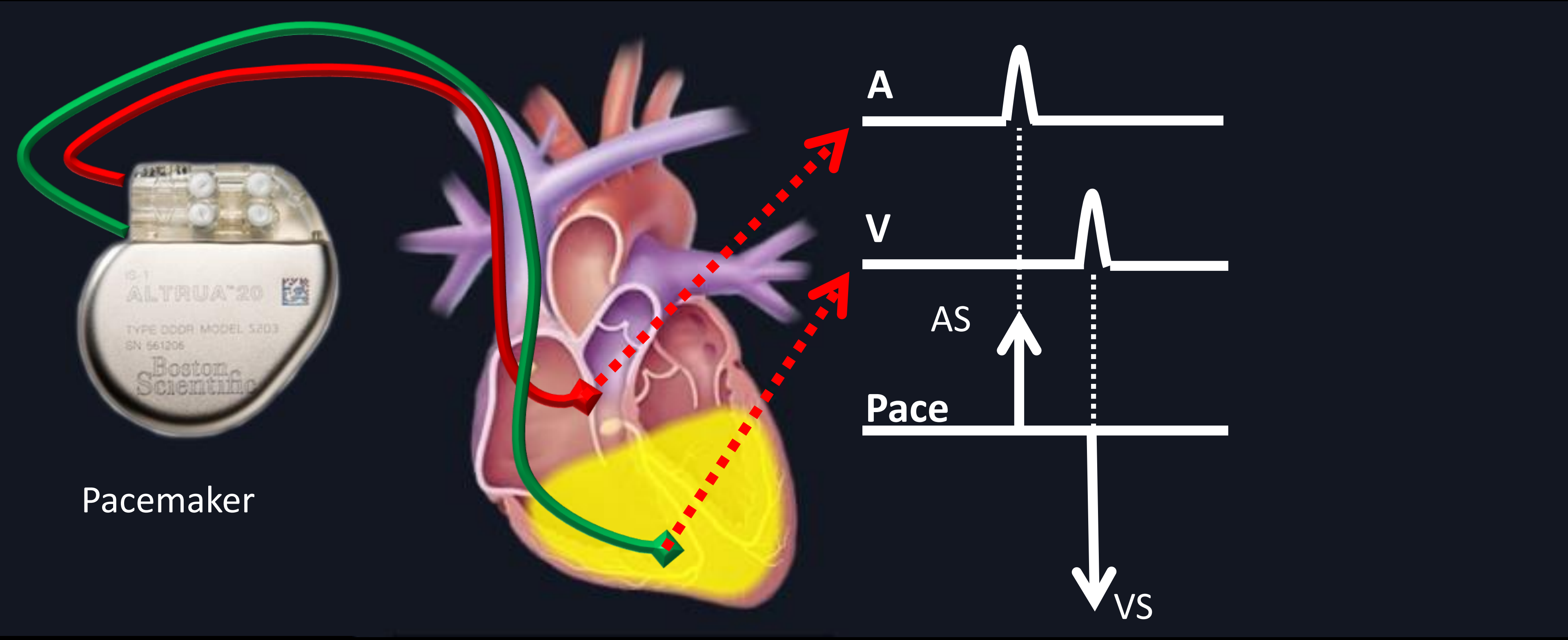
Atrial Sensing (AS)

- Generate sensed event when signal above threshold



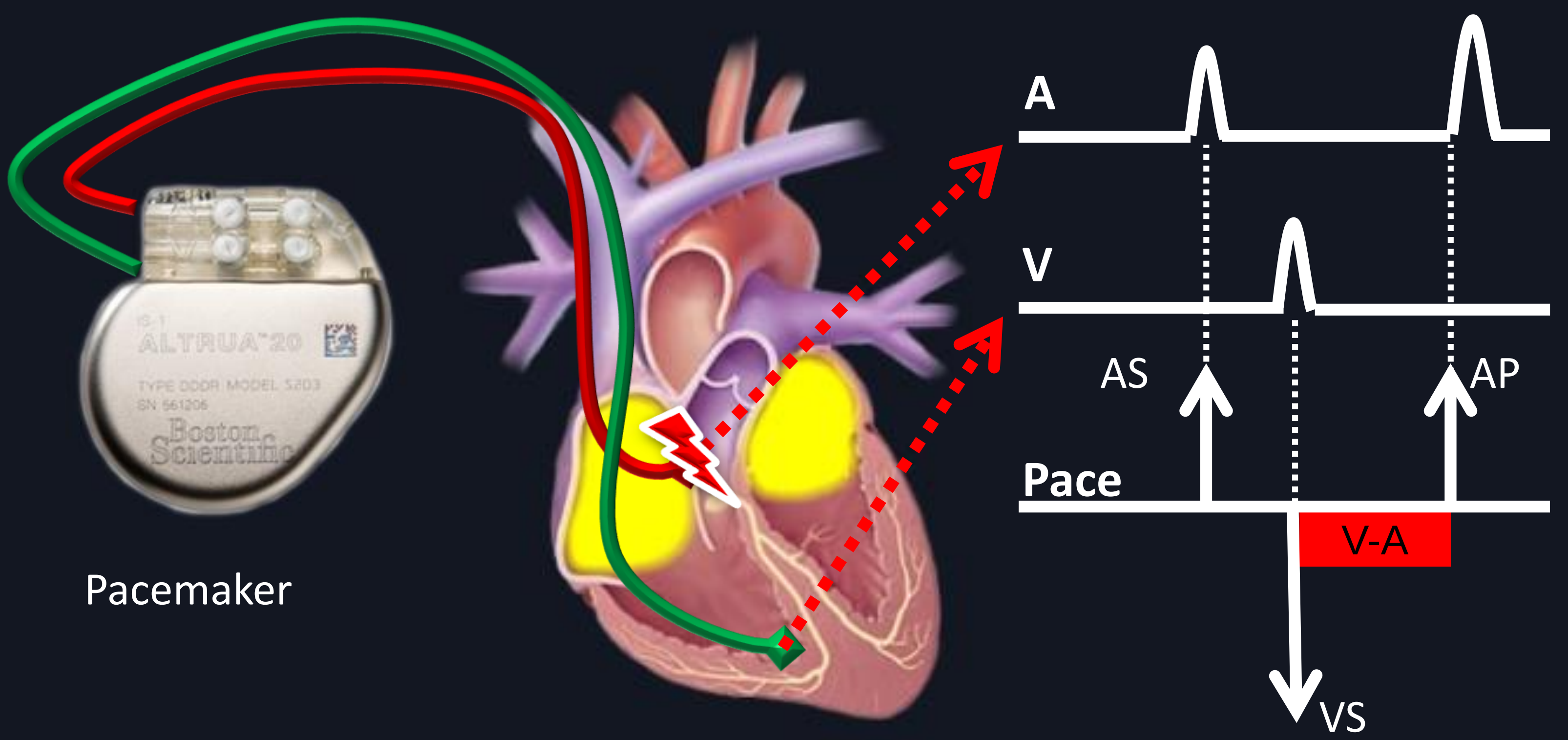
VENTRICULAR SENSE (VS)

- Same for ventricular channel



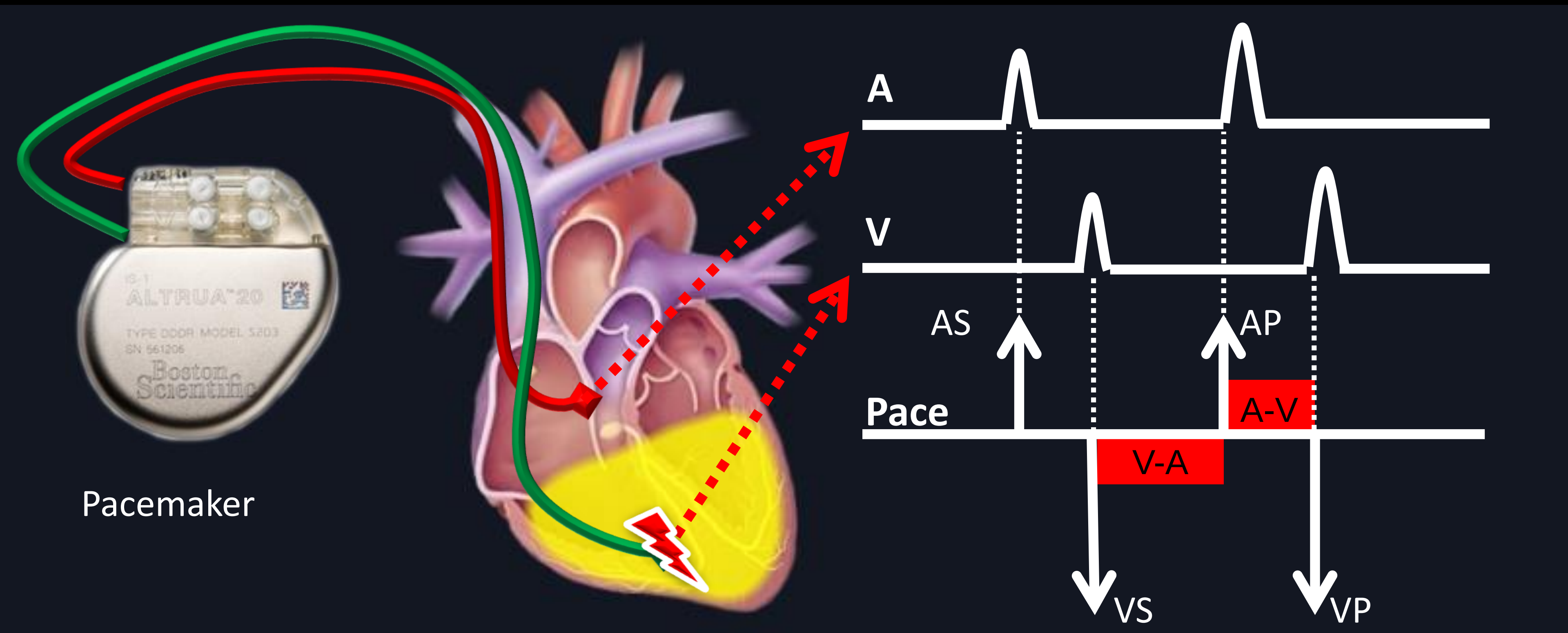
Atrial Pacing (AP)

- Pace atrium when no AS within deadline



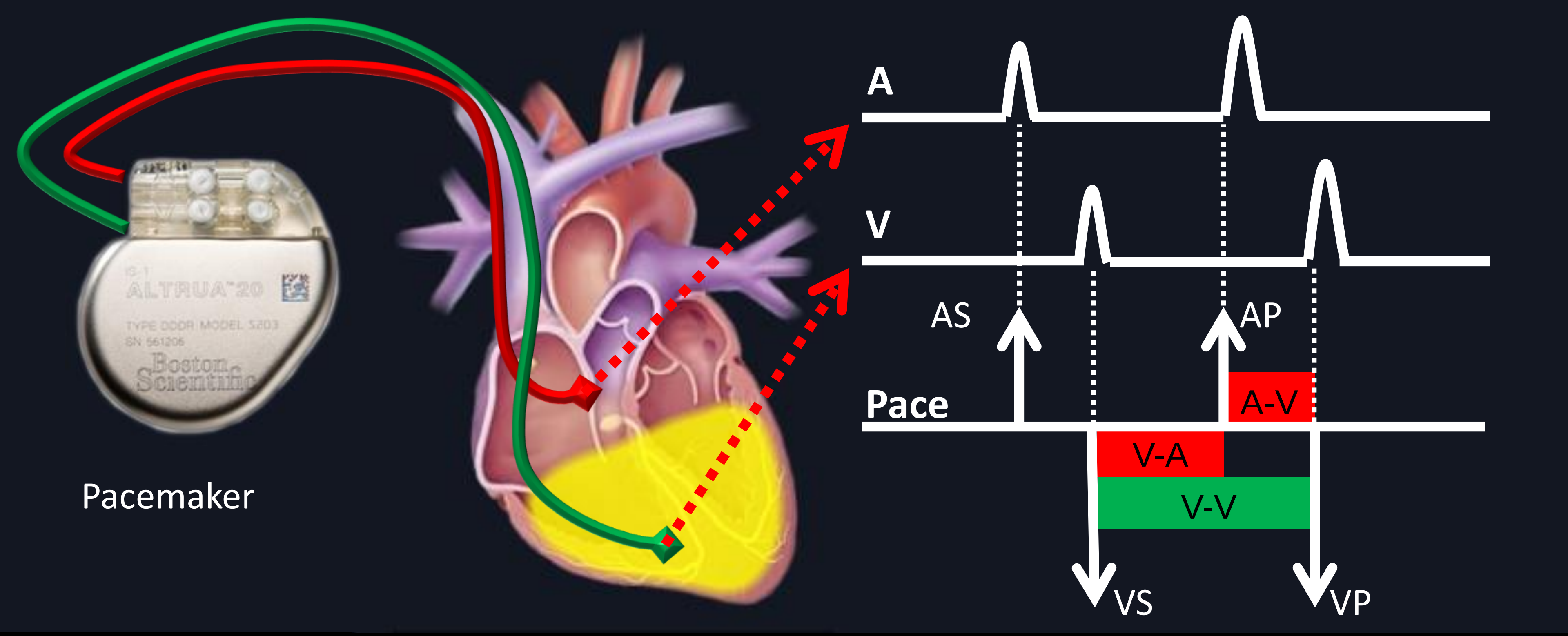
Ventricular Pacing (VP)

- Pace ventricle if no VS happen within deadline



Maintain minimum heart rate

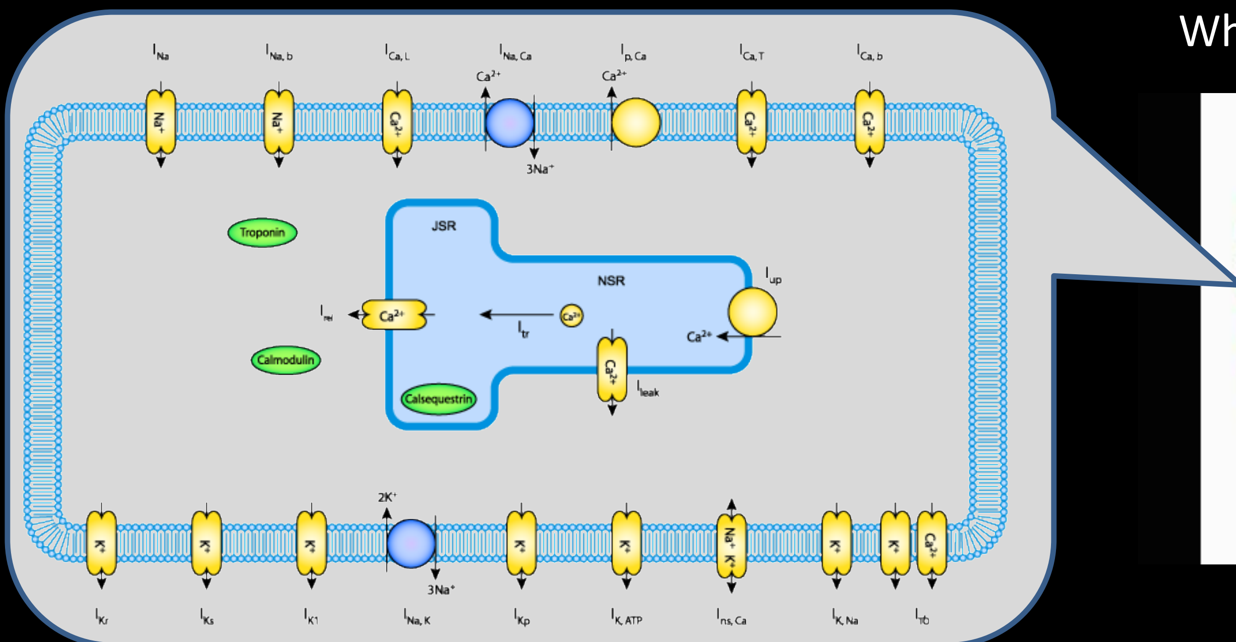
- Maximum interval between two ventricular events (max(V-A)+max(A-V))



ElectroPhysiological Models of the heart

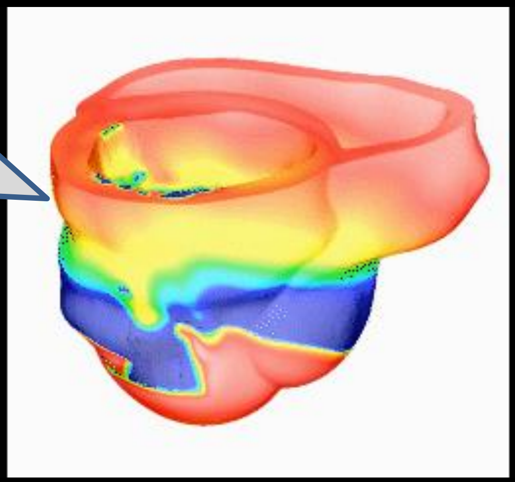
- Unnecessary details
- Infeasible model identification

Cellular Electrophysiology



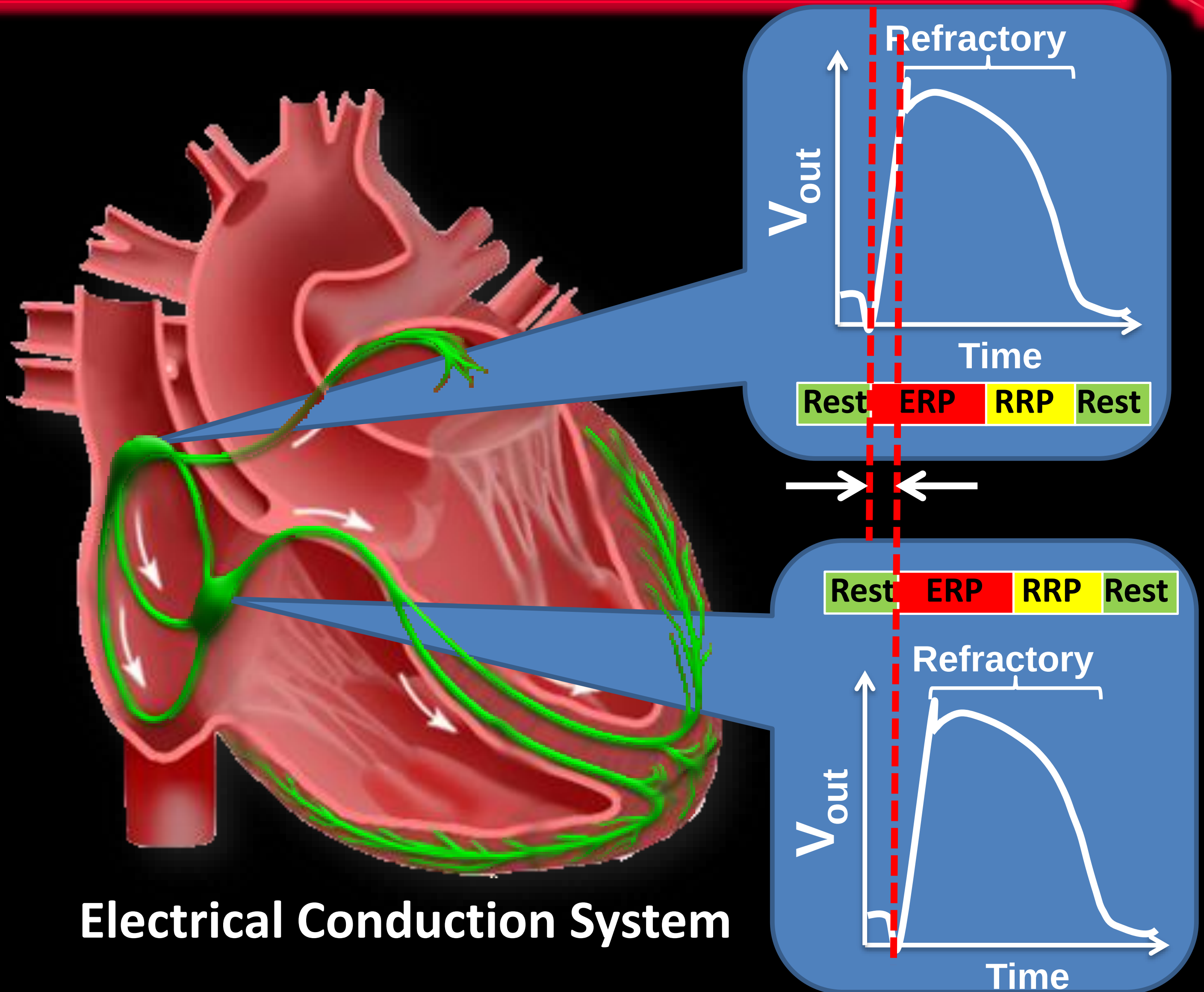
Tong et. al 2014

Whole heart Electrophysiology



Deng et. al 2016

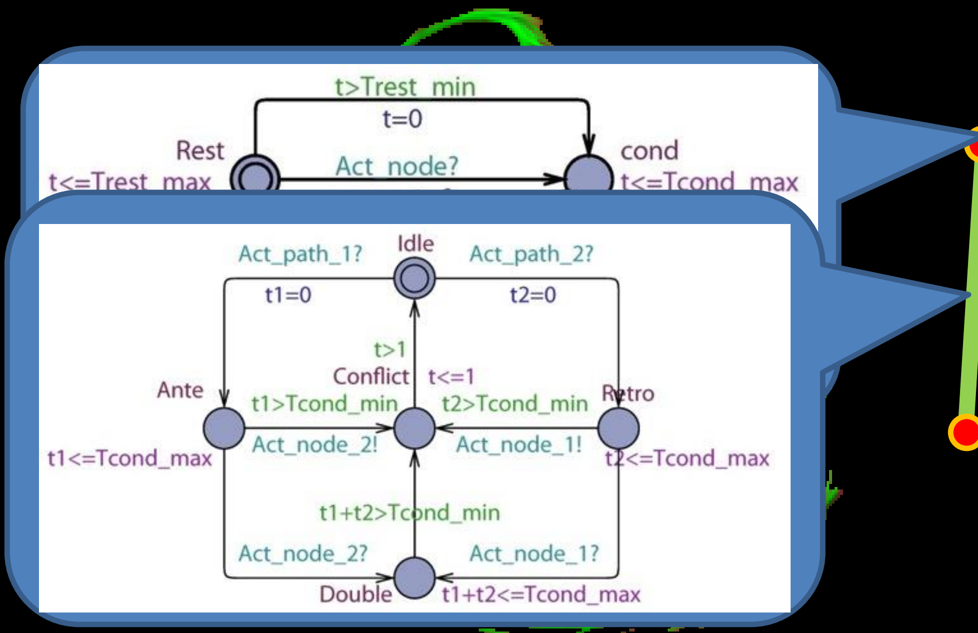
Electro-physiology of the Heart

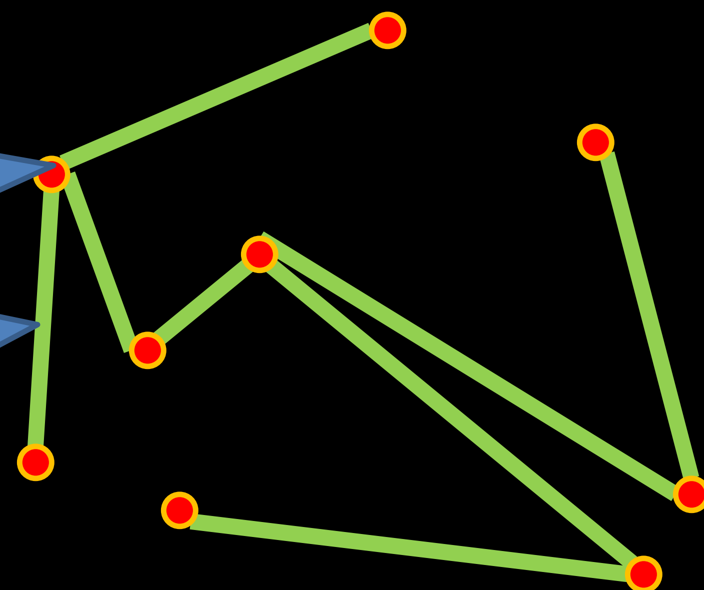


Electrical Conduction System

Timed Automata Heart Model

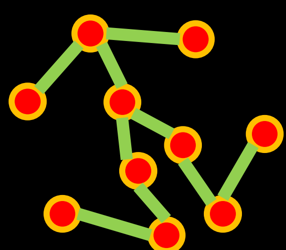
Node Automata
Path Automata

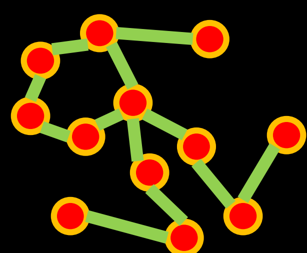


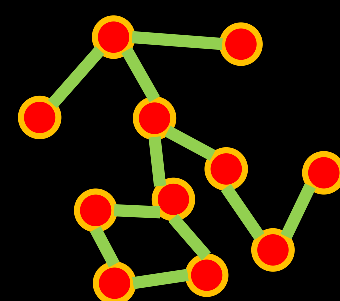


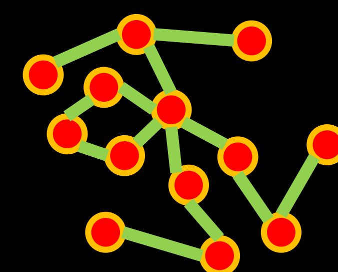
Network of Timed Automata

Represent variety of heart conditions using different topologies and timing parameters

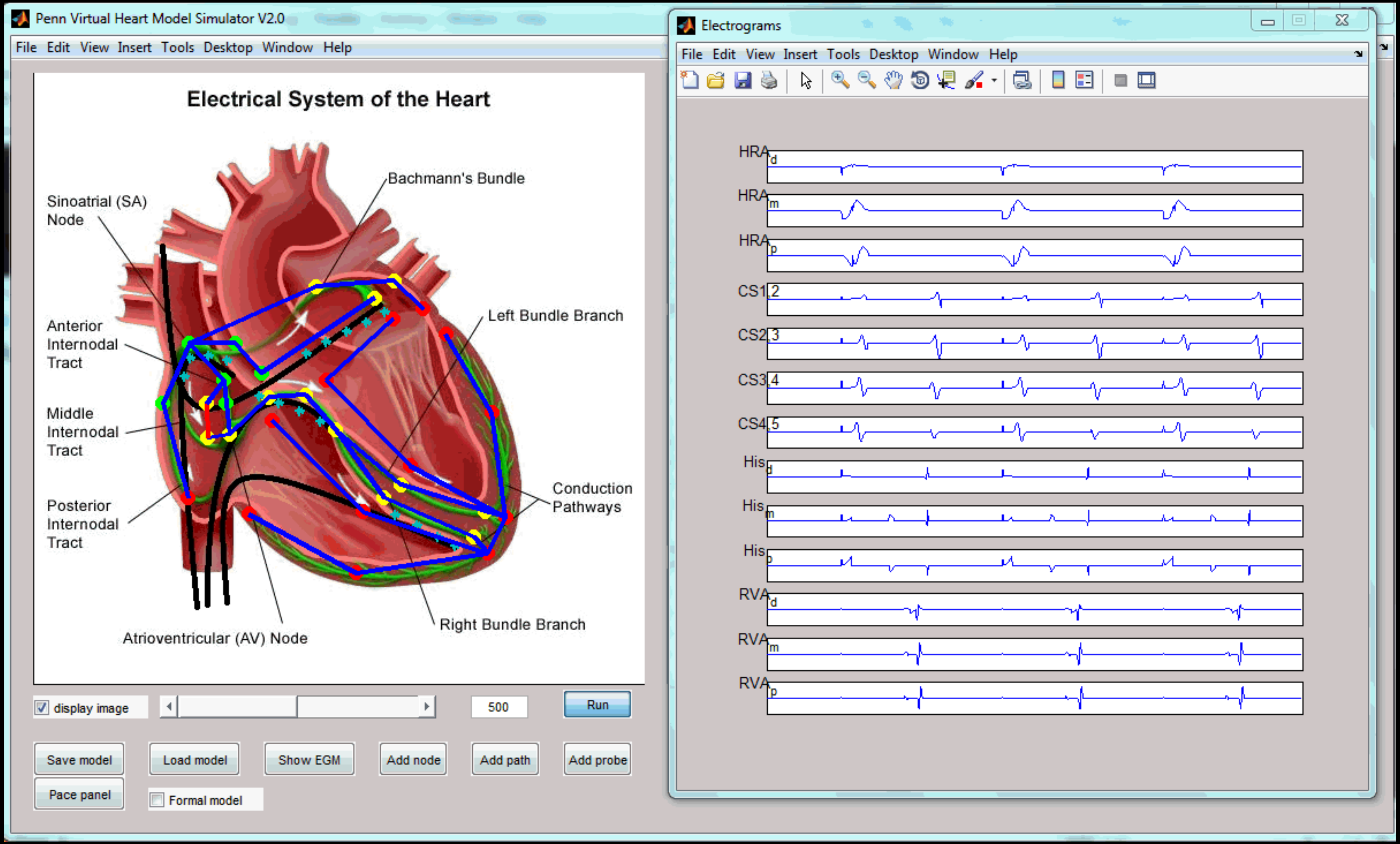

Normal Sinus Rhythm


Atrial Flutter


Ventricle Tachycardia

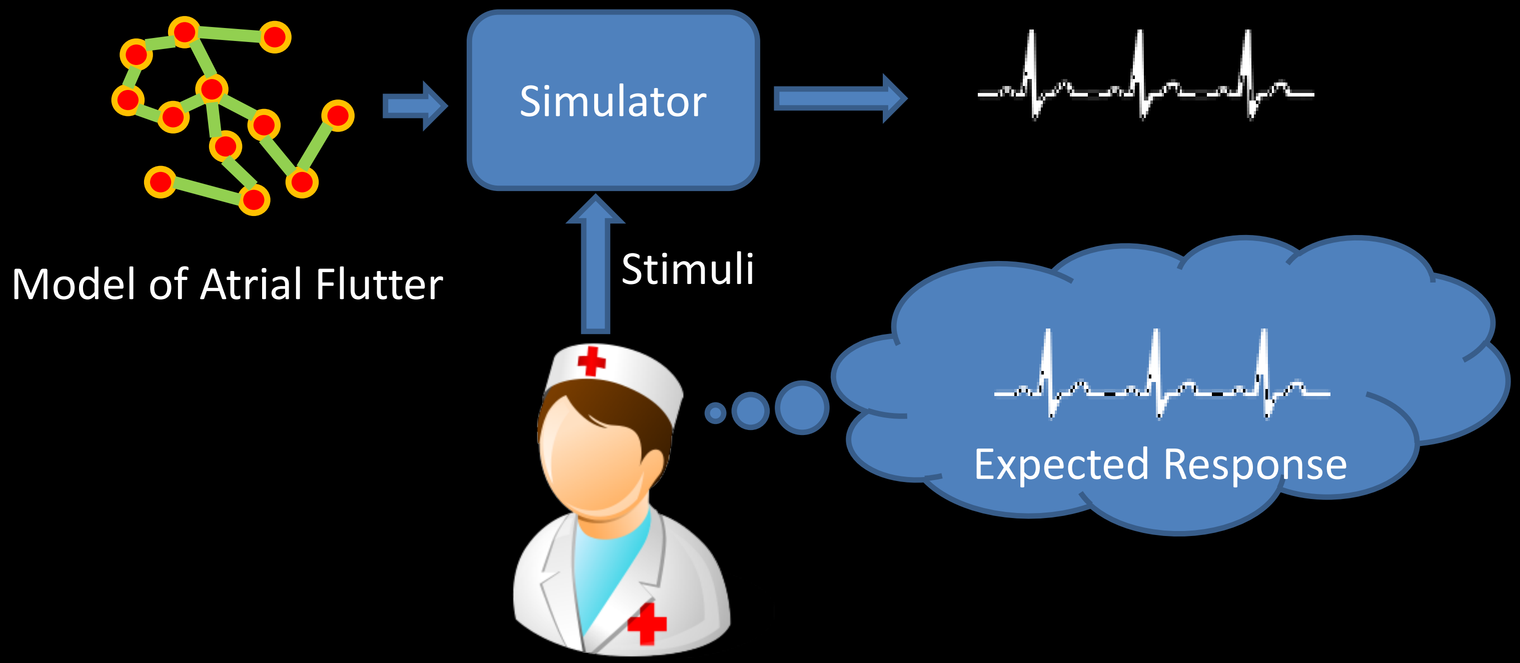

AV Nodal Reentry

Heart Model Simulation



Heart Model Validation

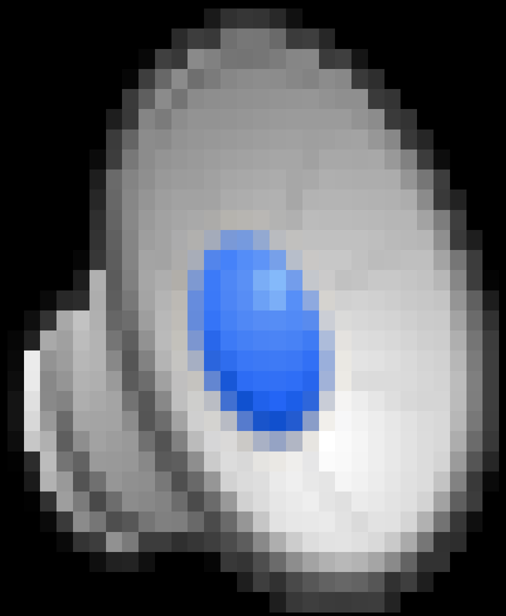
- Condition-specific heart models



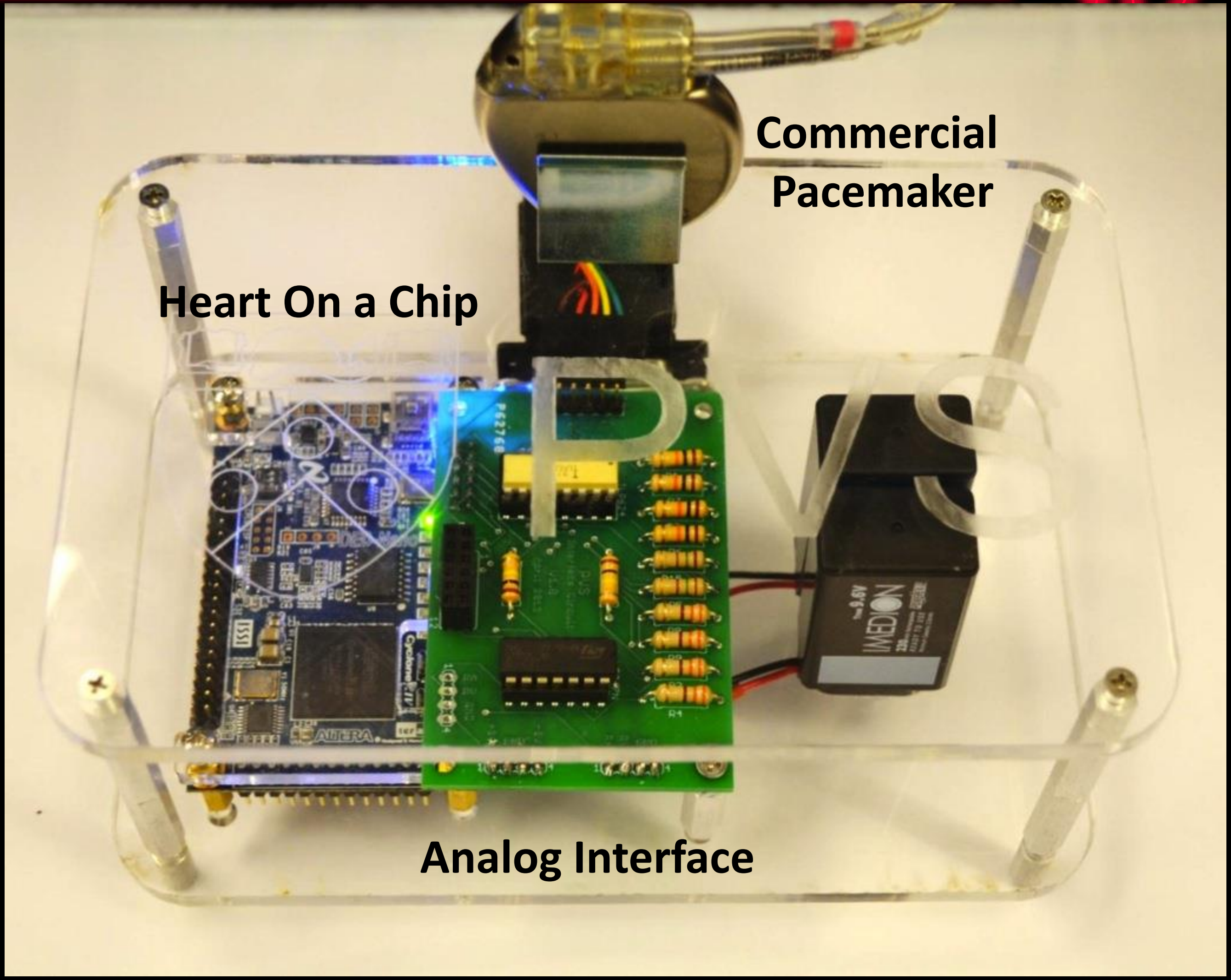
VHM Simulation

Penn Virtual Heart Model v2.0
Atrial flutter simulation

Closed-loop Heart – Pacemaker
illustrating Pacemaker Mediated Tachycardia



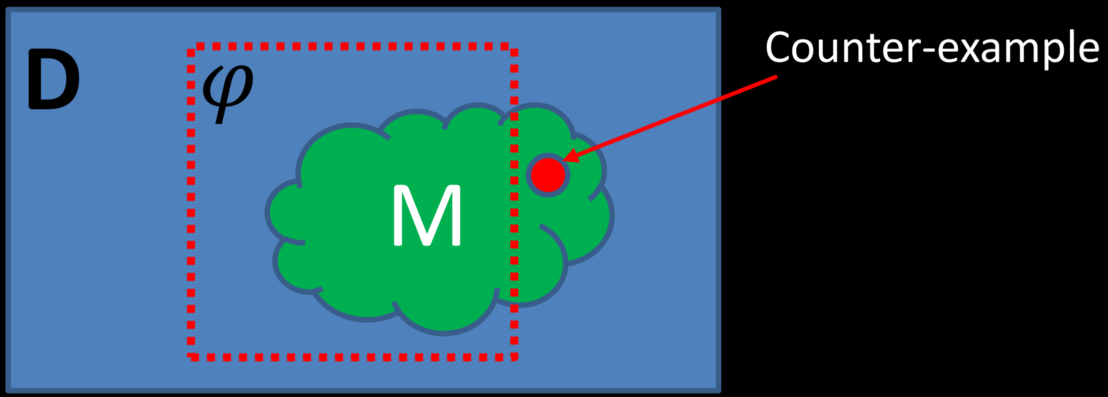
Heart On A Chip Platform



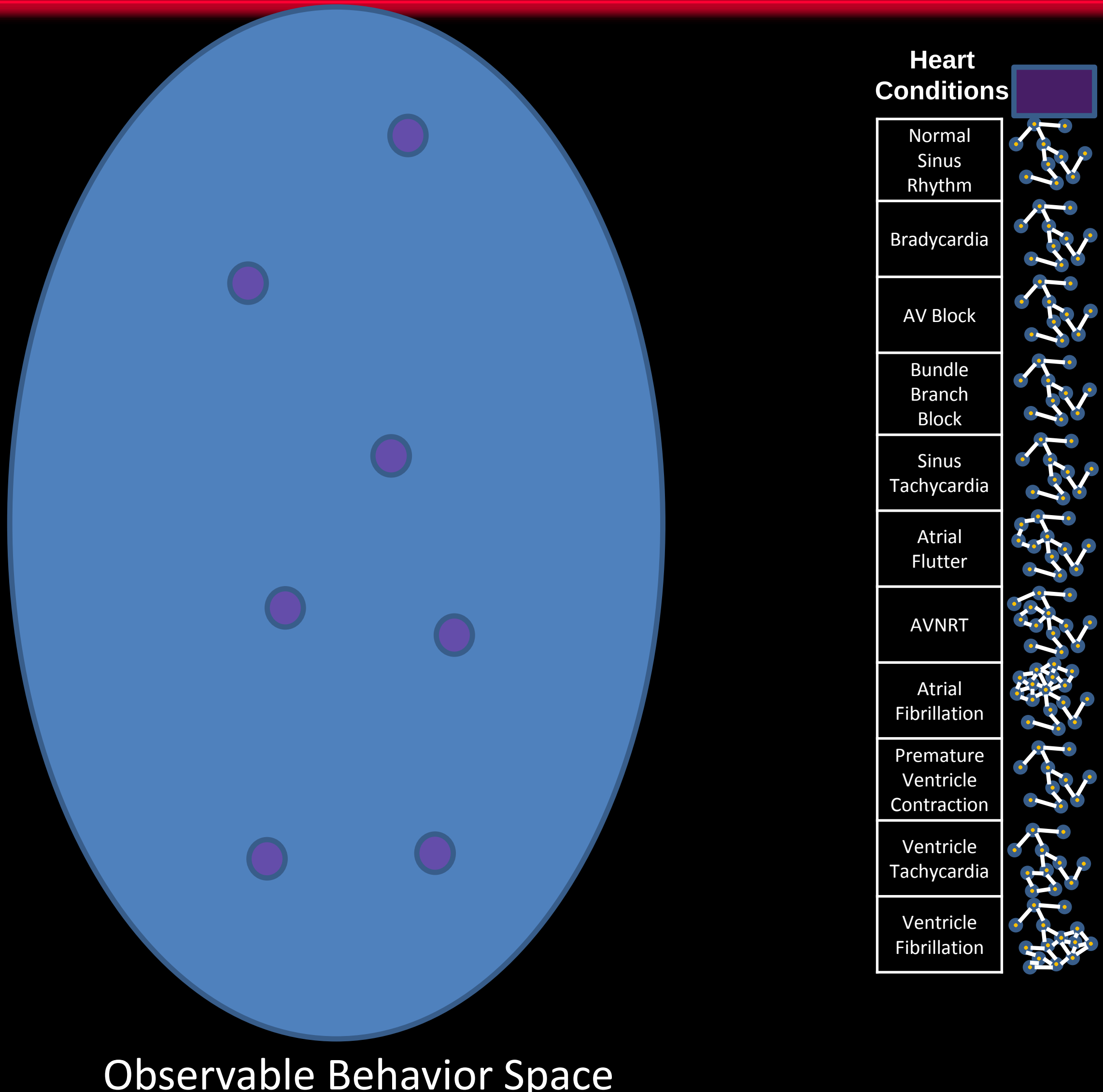
Thrust 2:
Capture Physiological Variability With Closed-loop Model Checking

Model Checking

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

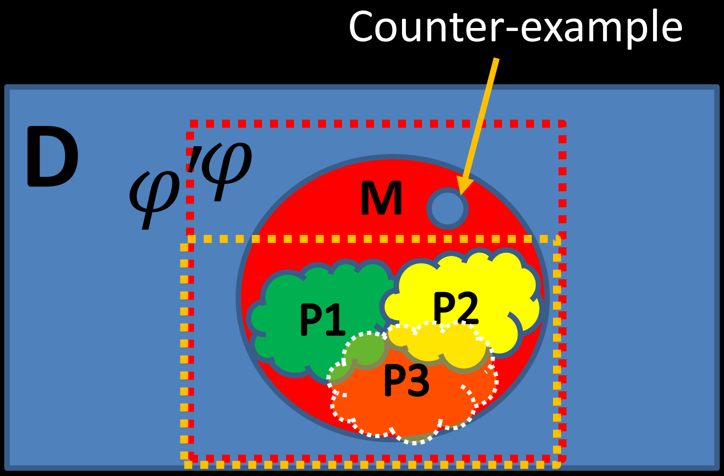


Initial Heart Models



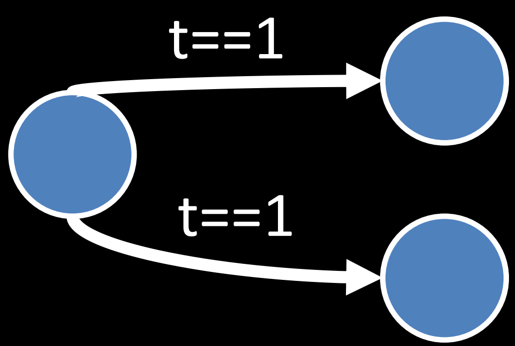
Capture Physiological Variability With Over-approximation

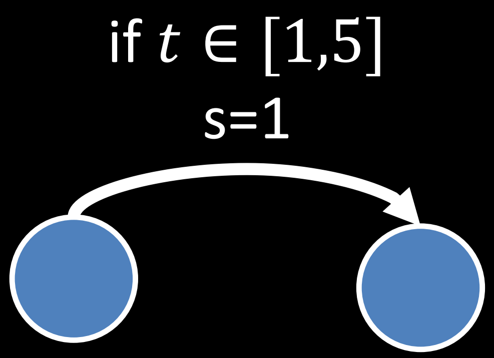
- Properties satisfied by M are also satisfied by P1, P2
- Behaviors not exist in P1, P2 may also be physiologically-valid
- Is this a valid counter-example?
- Need a framework to provide context for counter-examples



Non-determinism

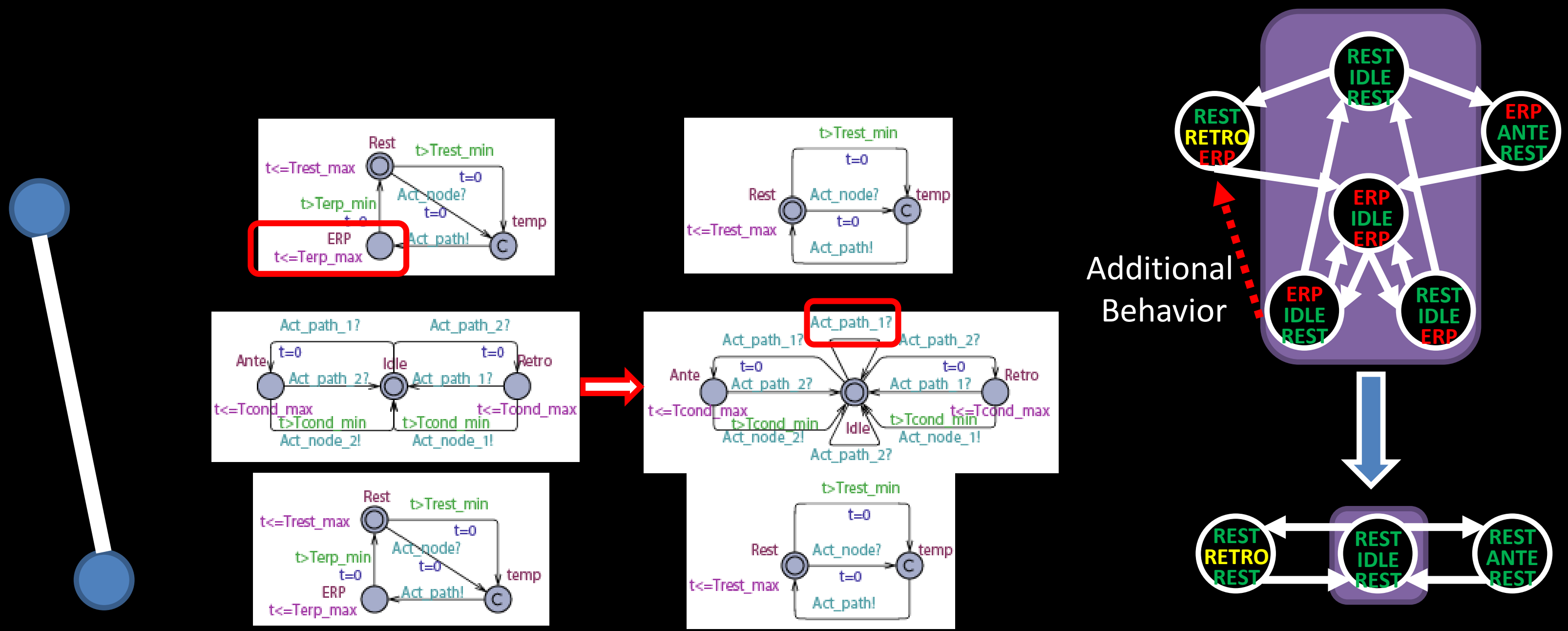
- Multiple transitions are enabled
- Relax guard conditions





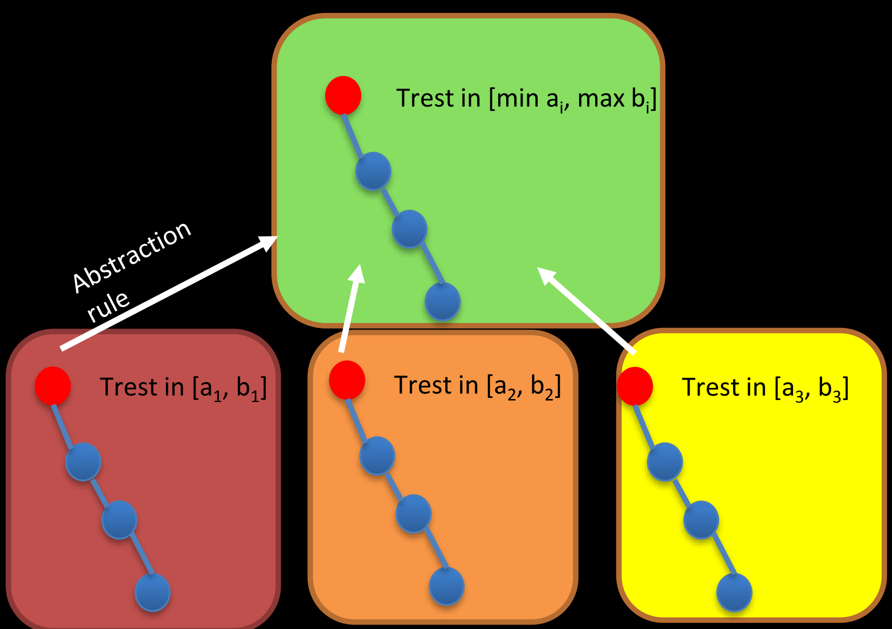
Physiological Abstraction Rules: Simplify

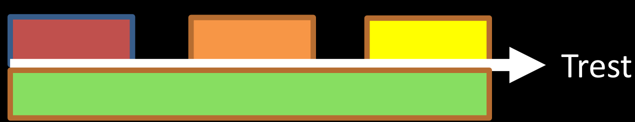
- Simplify the model to increase non-determinism for more behavior coverage



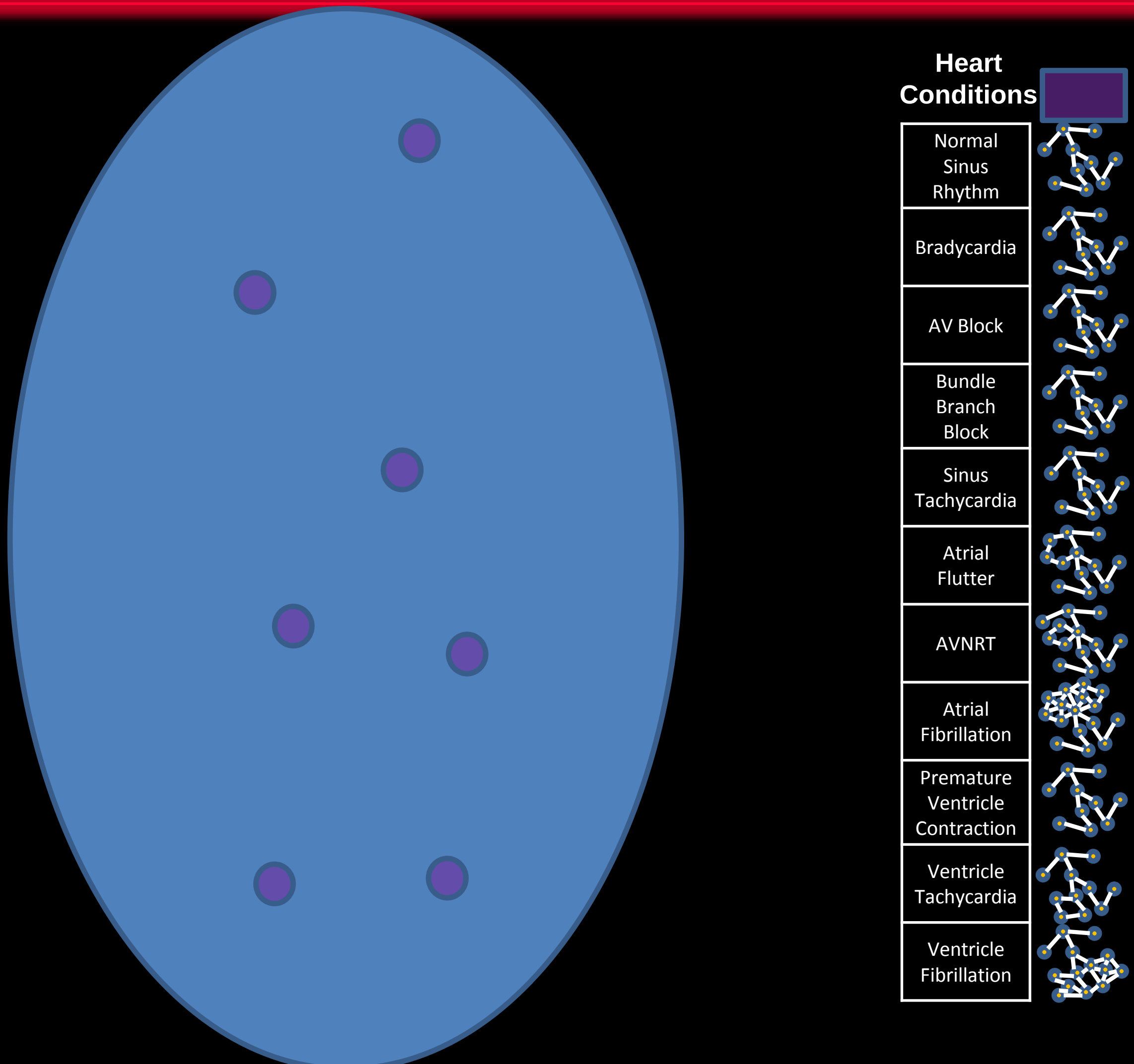
Physiological Abstraction Rules: Combine

- Combine models of different heart conditions for more behavior coverage



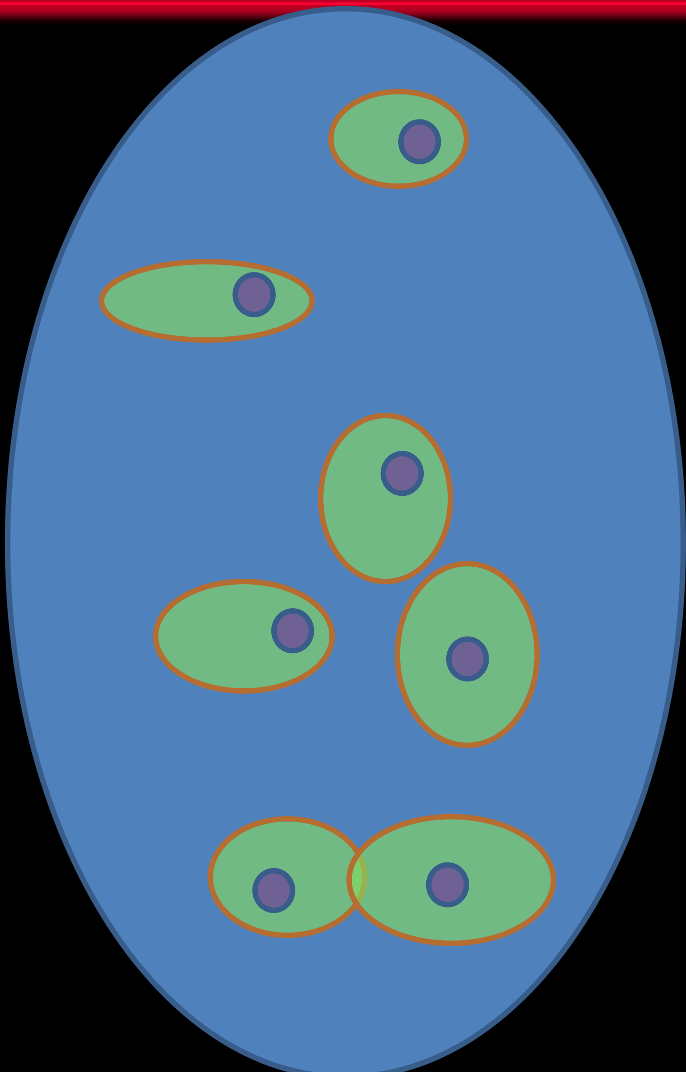


Initial Heart Models

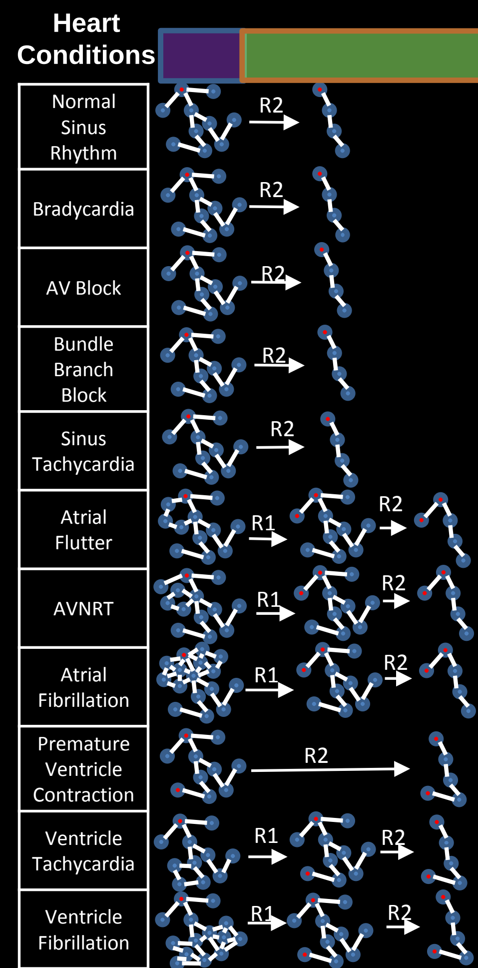


Observable Behavior Space

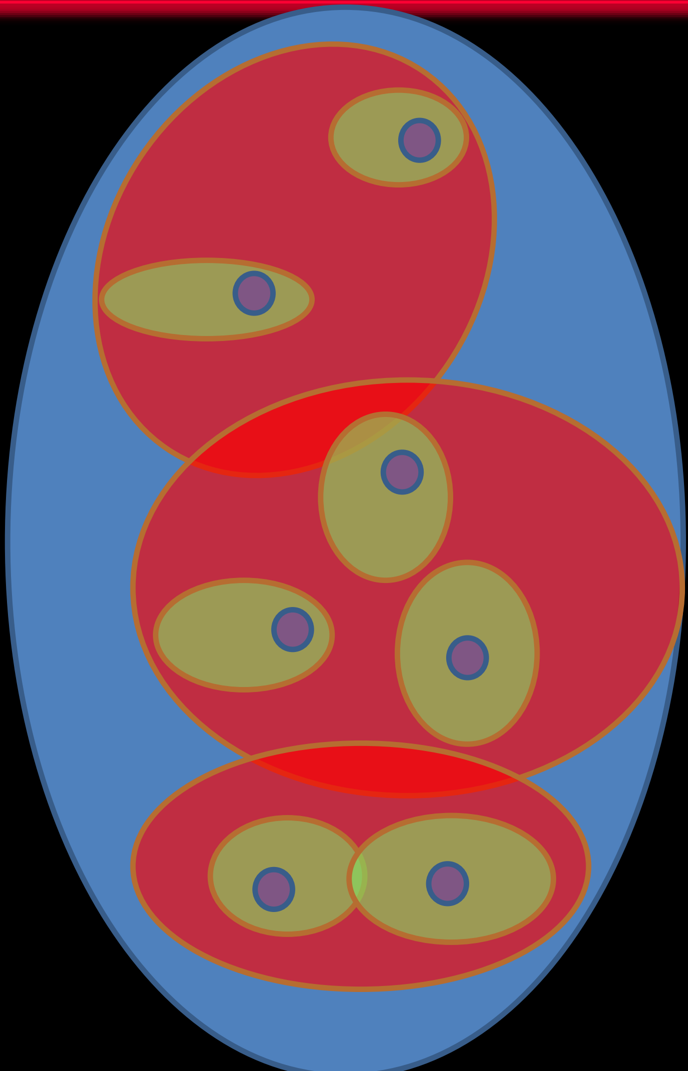
Abstraction Tree: Heart Model Abstraction



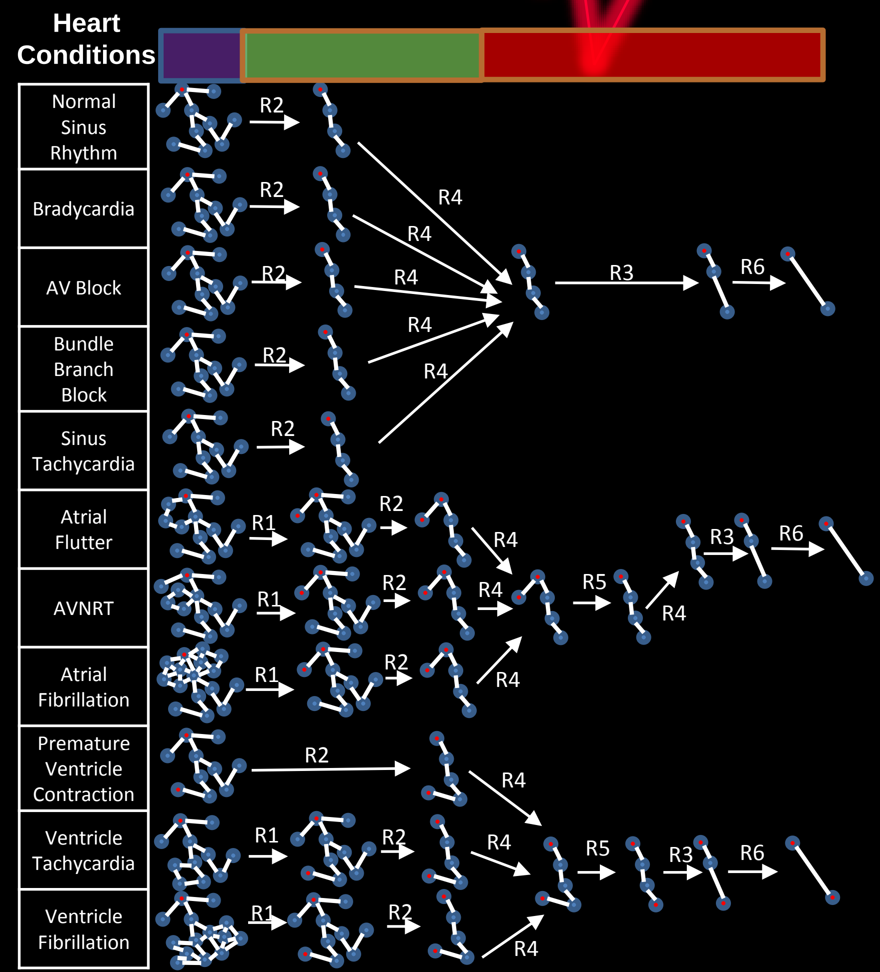
Observable Behavior Space



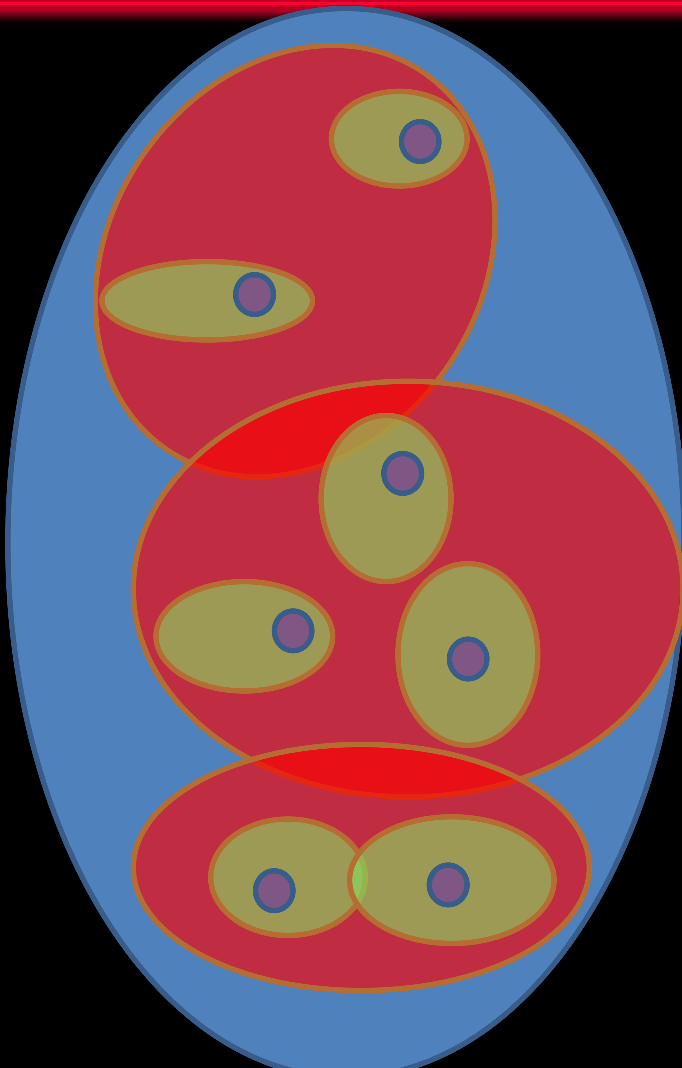
Abstraction Tree: Heart Model Abstraction



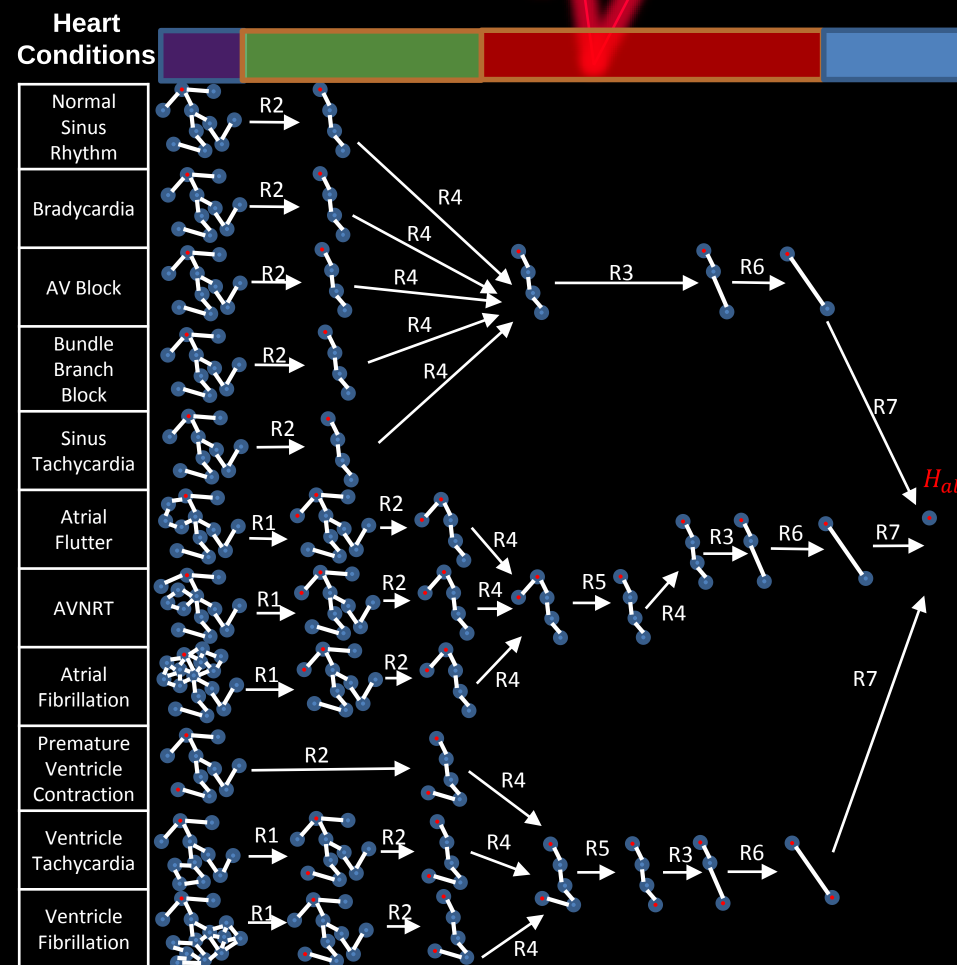
Observable Behavior Space



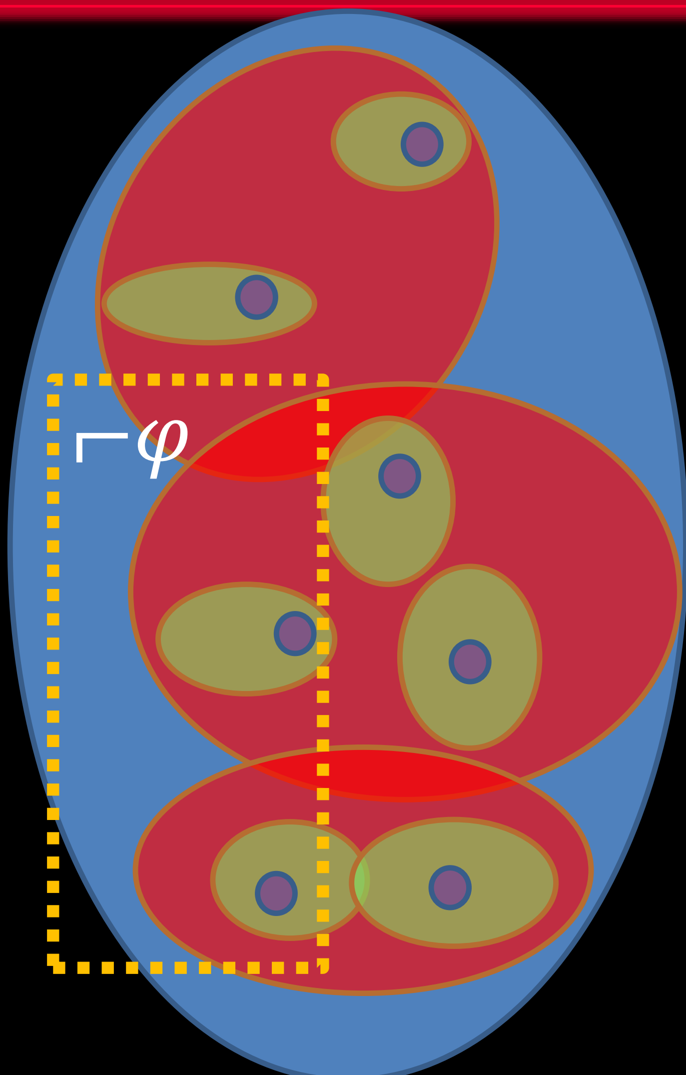
Abstraction Tree: Heart Model Abstraction



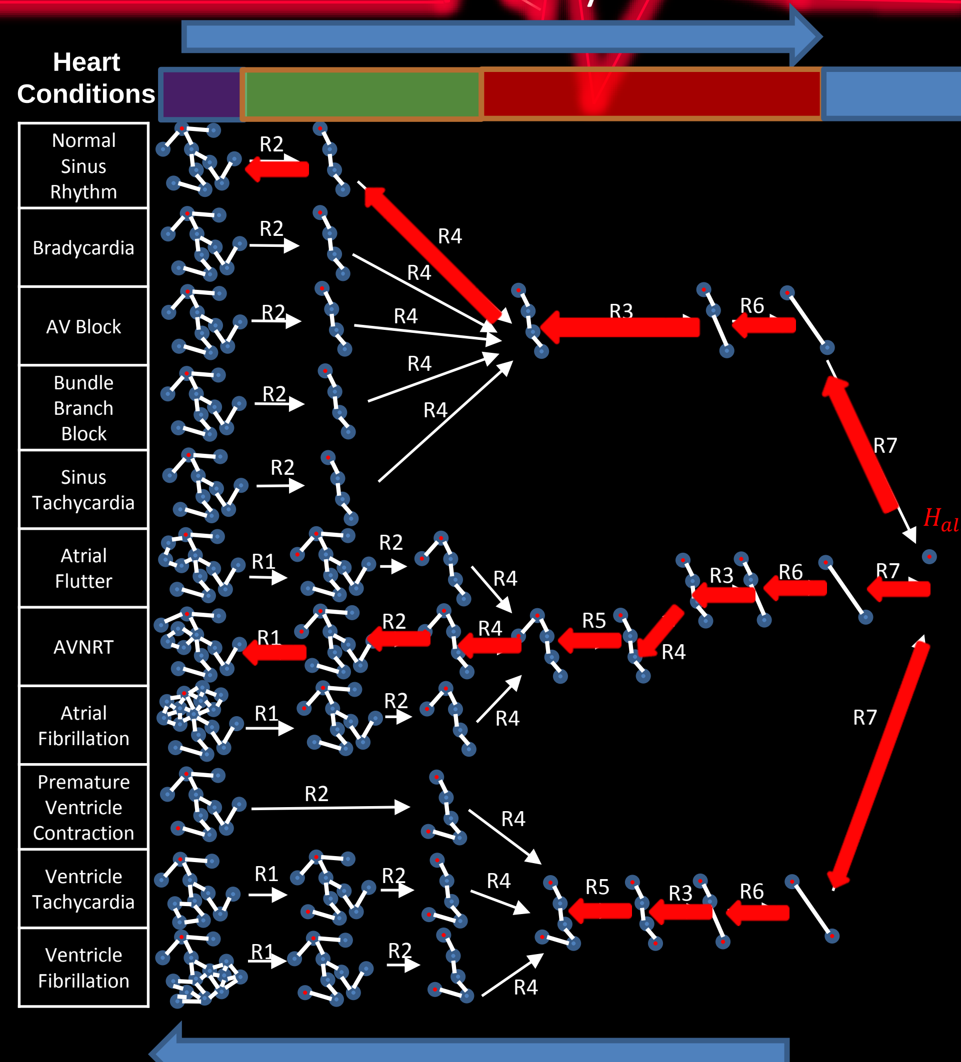
Observable Behavior Space



Abstraction Tree: Heart Model Refinement



Observable Behavior Space



Physiological Context

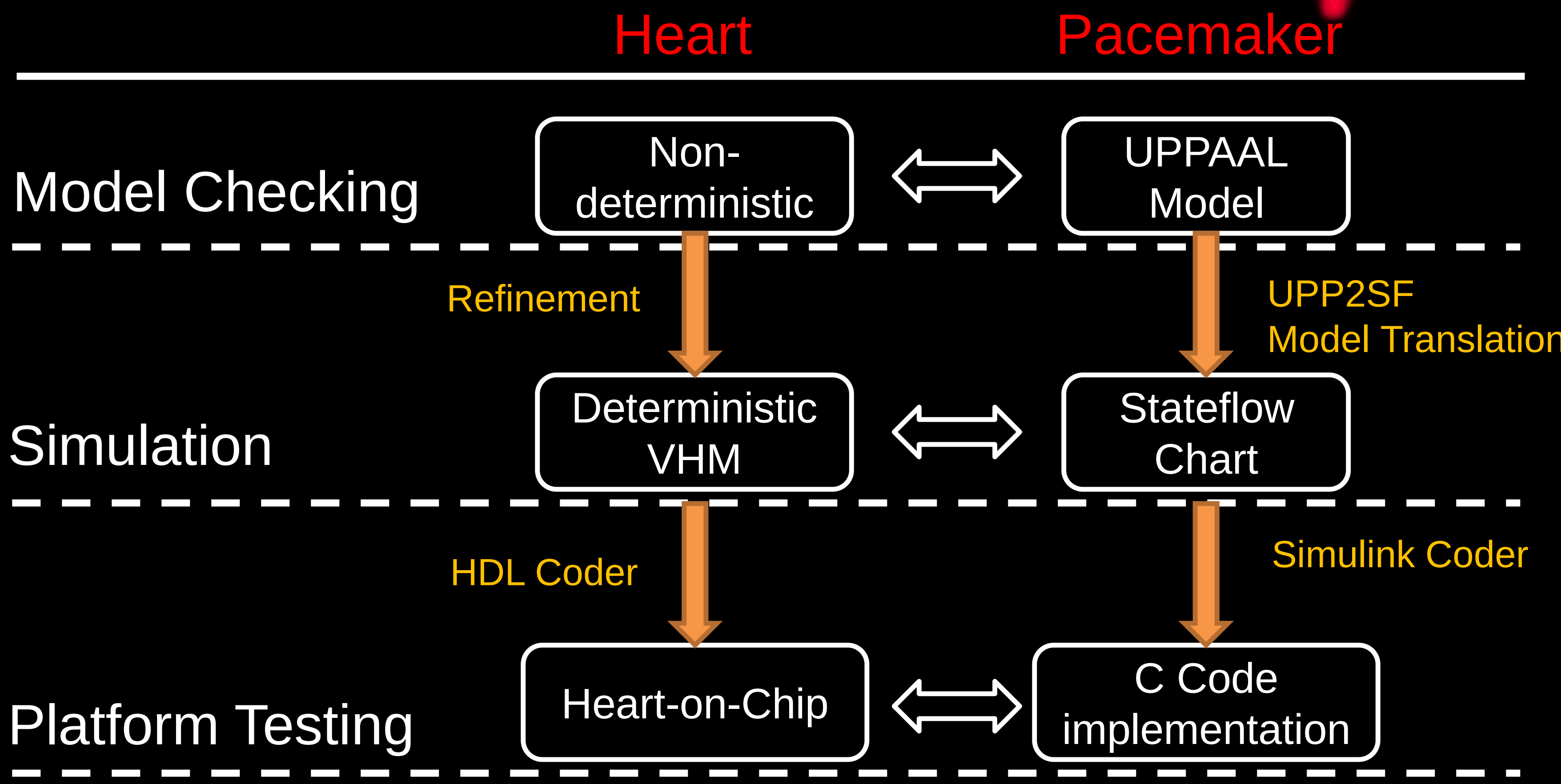
Properties Verified

- 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



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

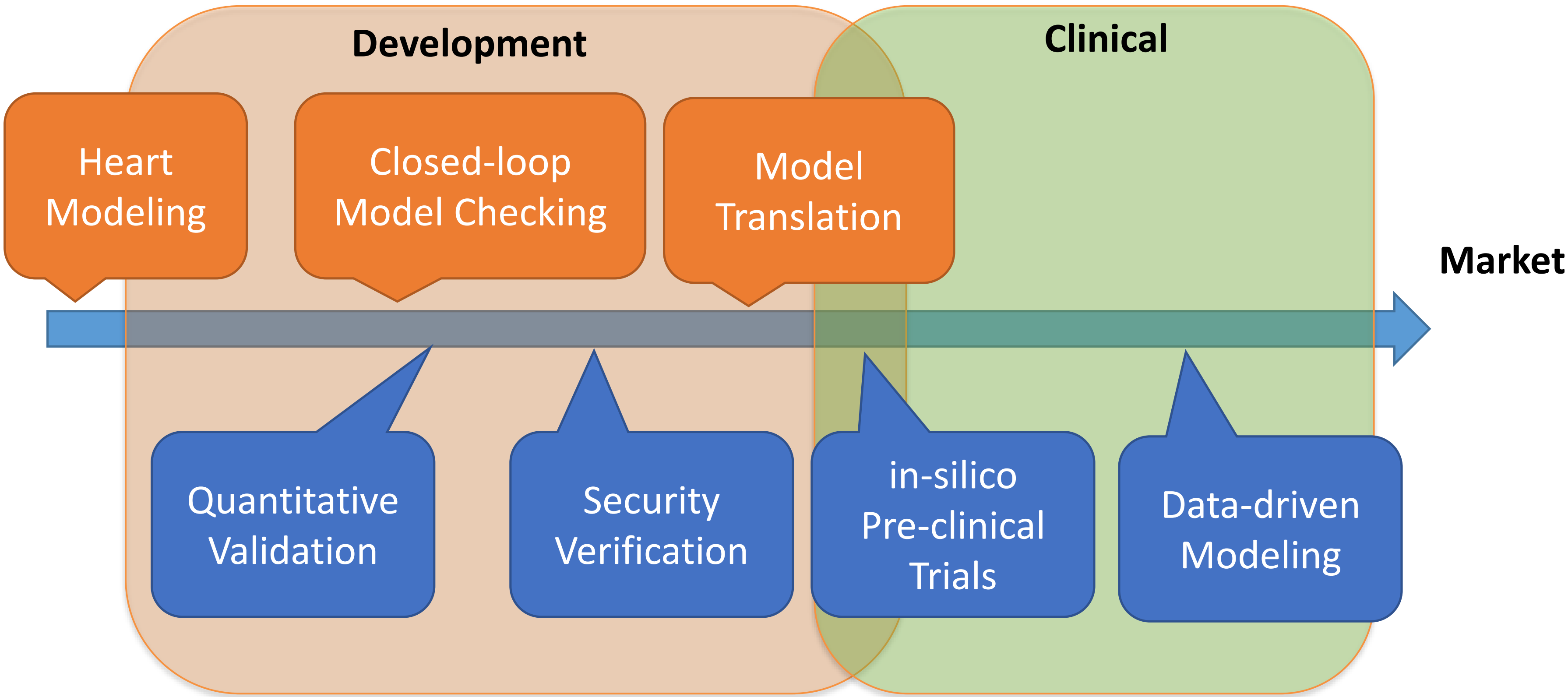
Cyber-Physical Systems

ICCPS'11
ECRTS'11
IEEE Proceedings'12

Biomedical Engineering

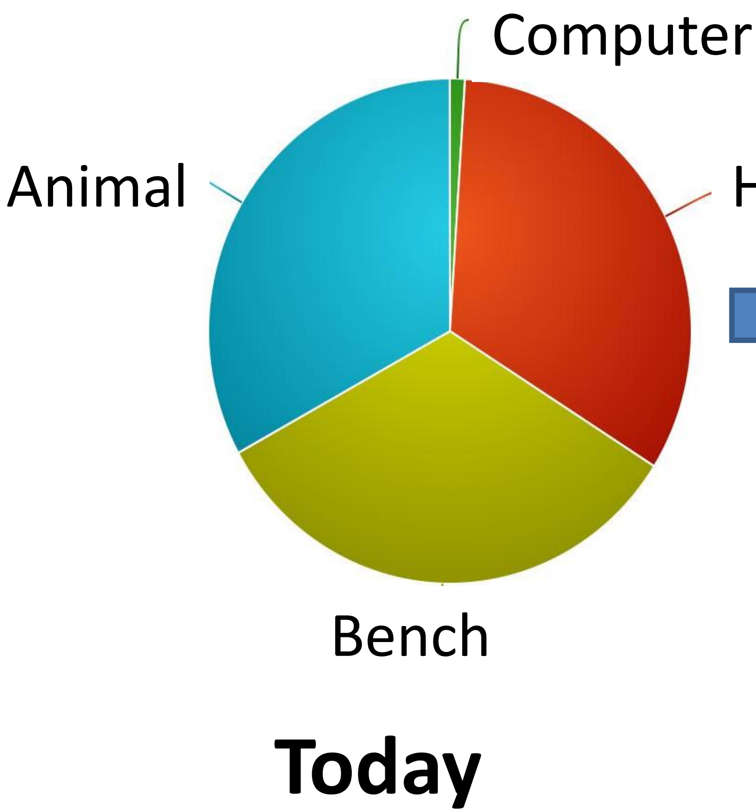
EMBC'10
EMBC'11
EMBC'16

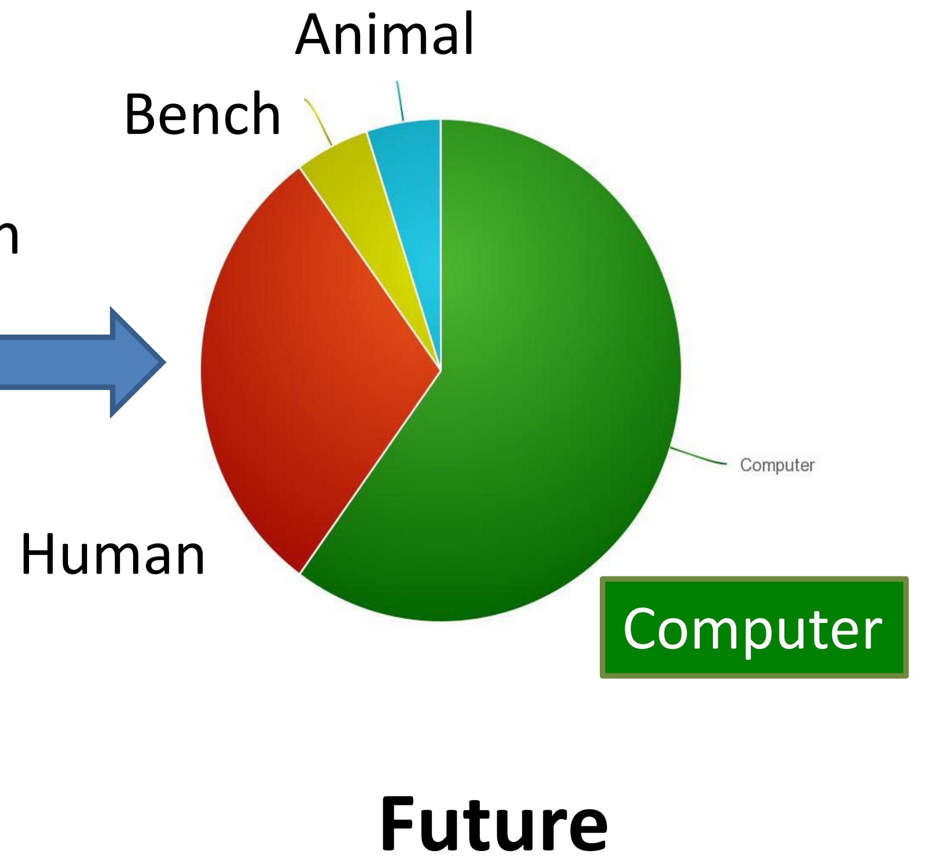
Research Summary & Plan



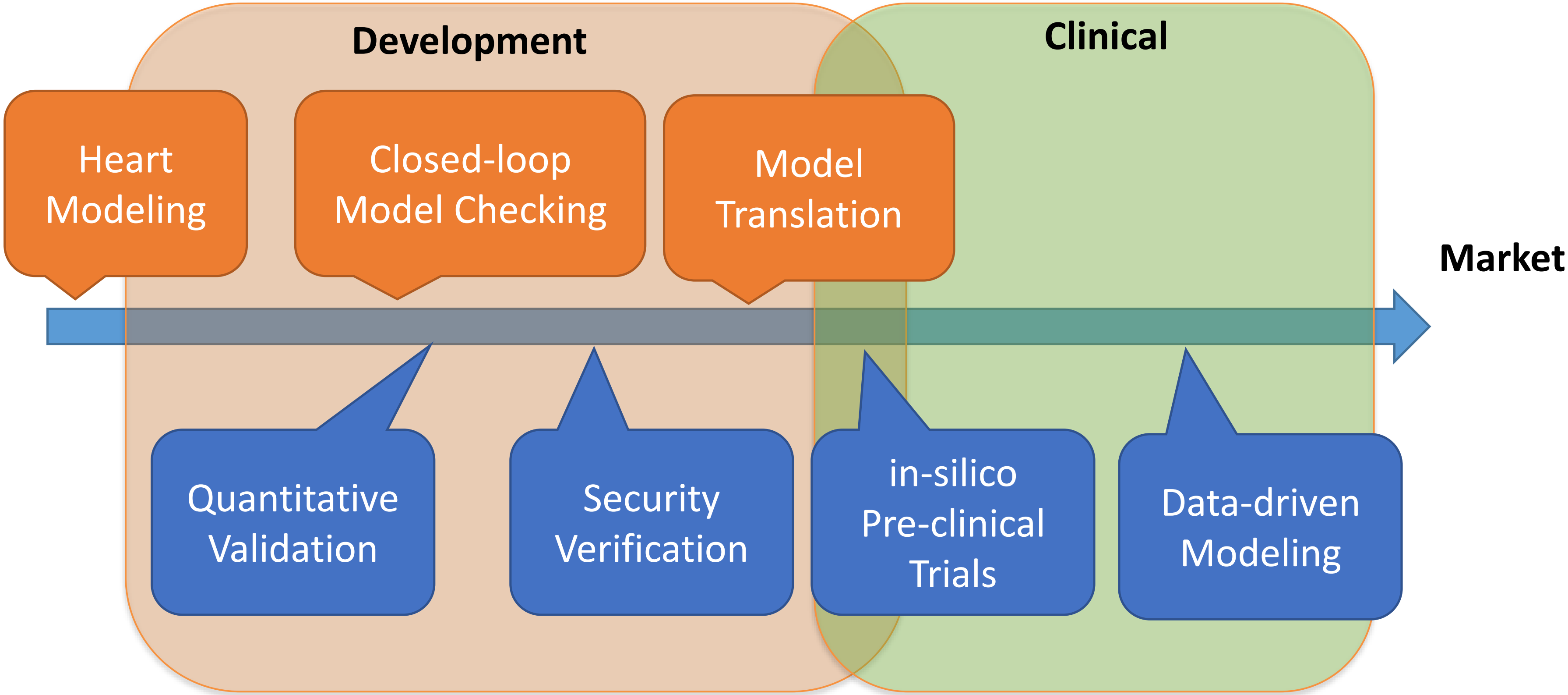
Providing Regulatory-grade Safety Evidence With Computer Models

Safety Evidence for Medical Devices





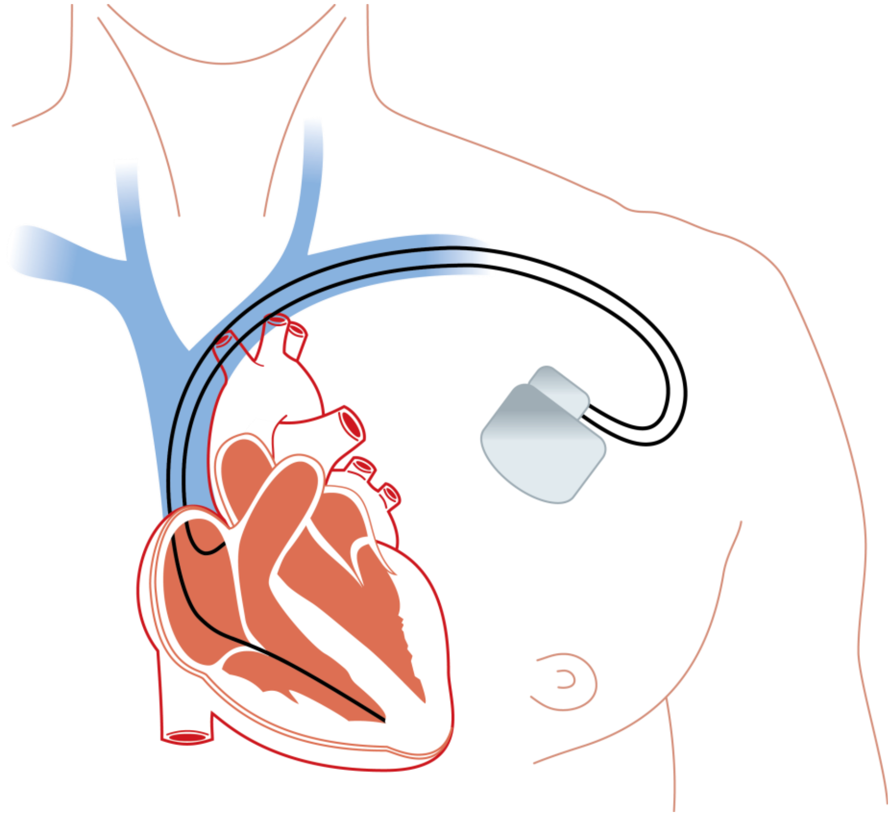
Research Summary & Plan



Providing Regulatory-grade Safety Evidence With Computer Models

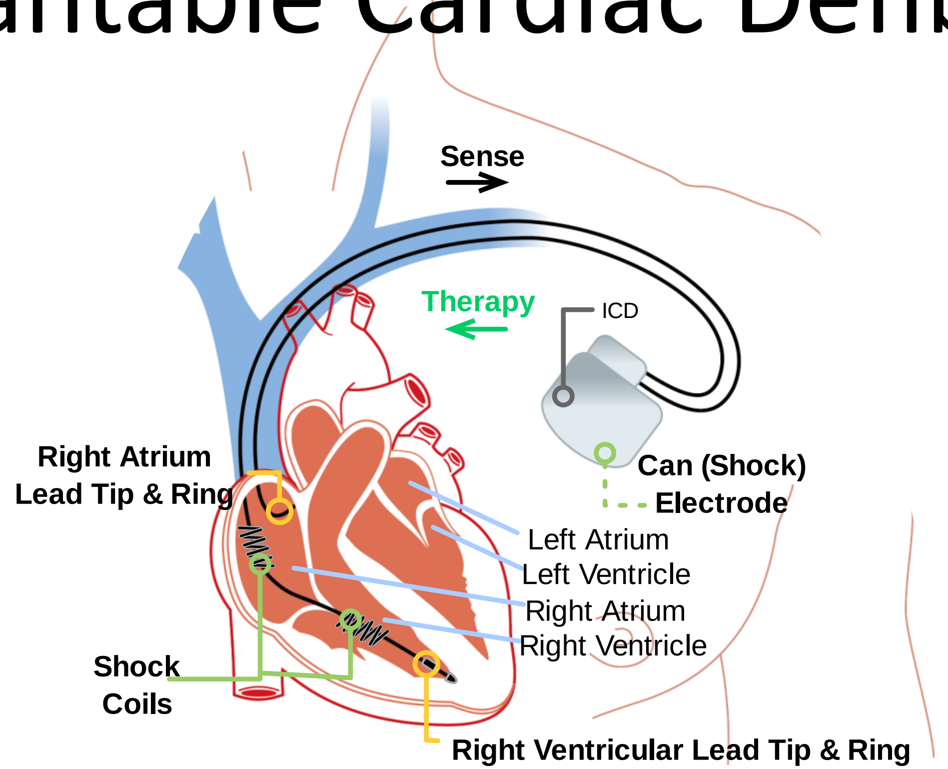
The clinical trial

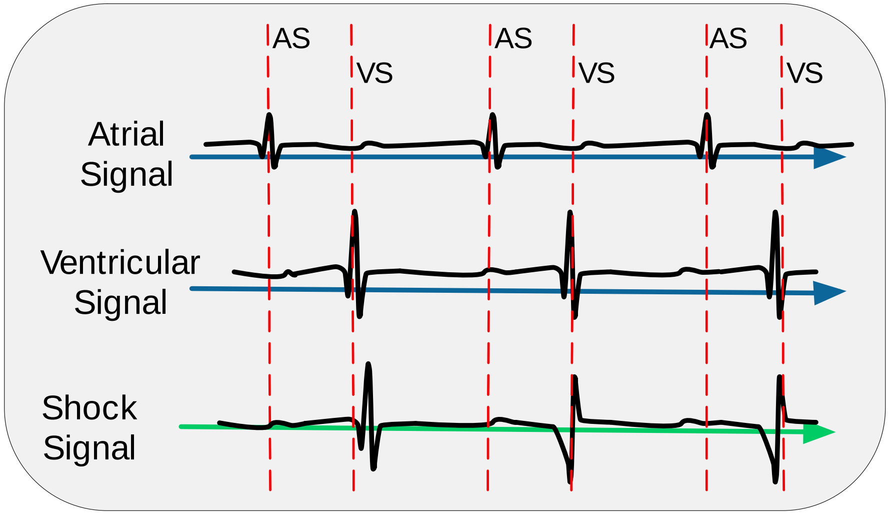
Animal testing



The ultimate closed-loop validation

Implantable Cardiac Defibrillator





RIGHT

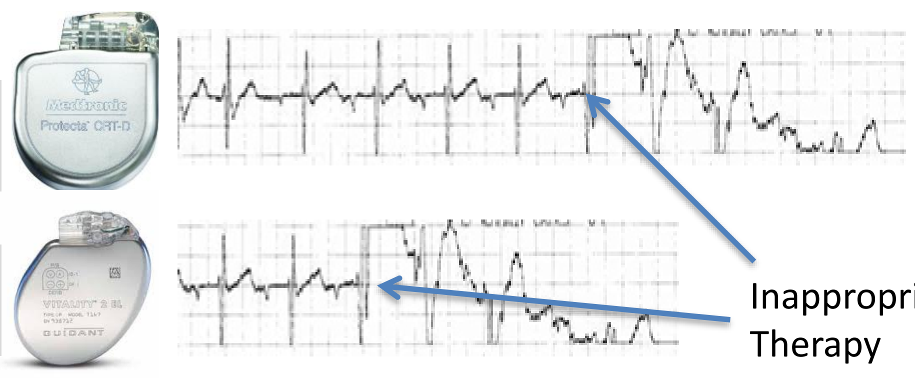
The Rhythm ID Going Head to Head Trial*

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**)



Inappropriate Therapy

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

*Berger et al., “The Rhythm ID Going Head to Head Trial”, Journal of Cardiovascular EP, Vol. 17, No. 7, July 2006

RIGHT Trial Results – Inappropriate Therapy

Gold et al RIGHT of Inappropriate ICD Therapy 373

Table 2 Adjudication summary of spontaneous episodes where therapy was delivered

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

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

Inappropriate Therapy

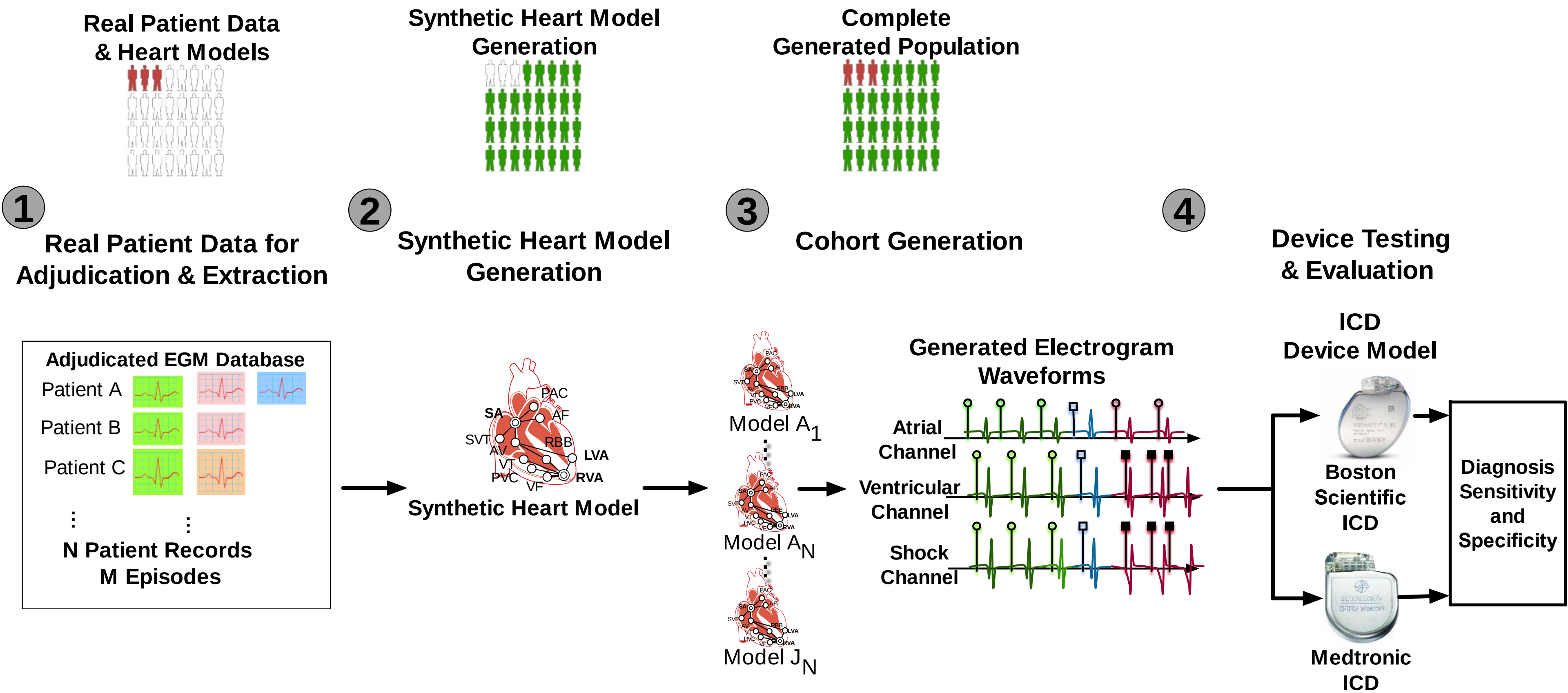
VITALITY 2: 62.2%

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



Learn Parameter distribution

Sampling parameters from distribution

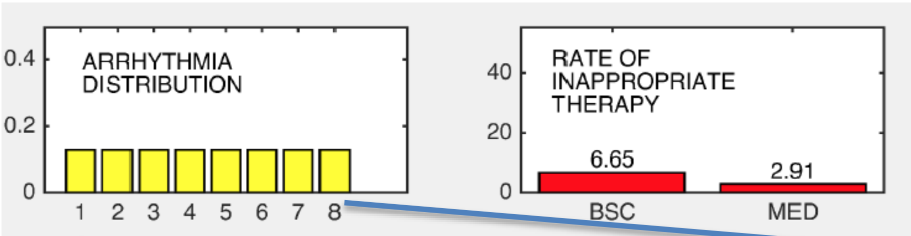
10,000's Condition-specific Model Generation

10,000's Condition-specific electrograms

Closed-loop evaluation

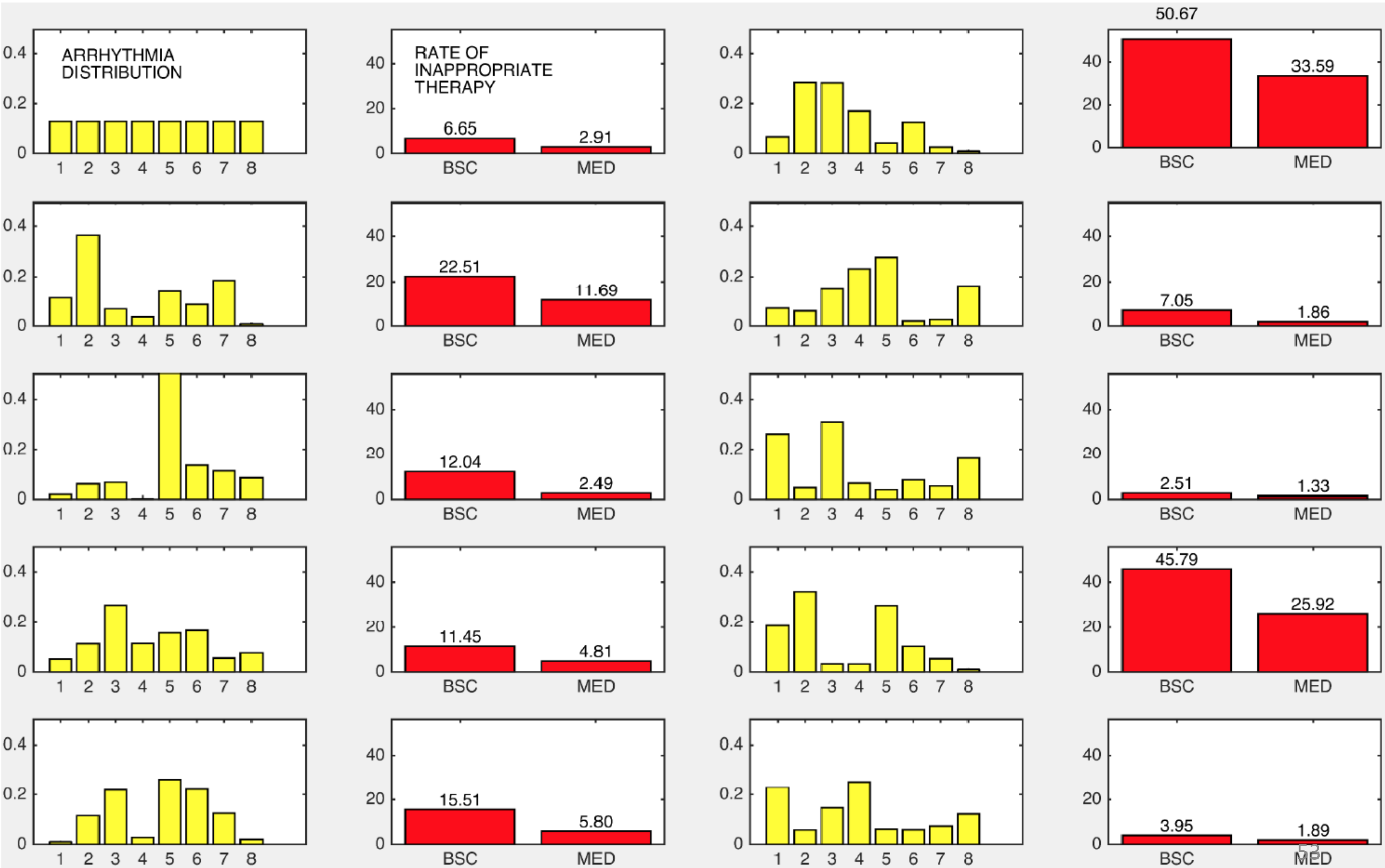
NSF Frontiers CyberCardia $4.2M. Started May 2015 to May 2020.

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

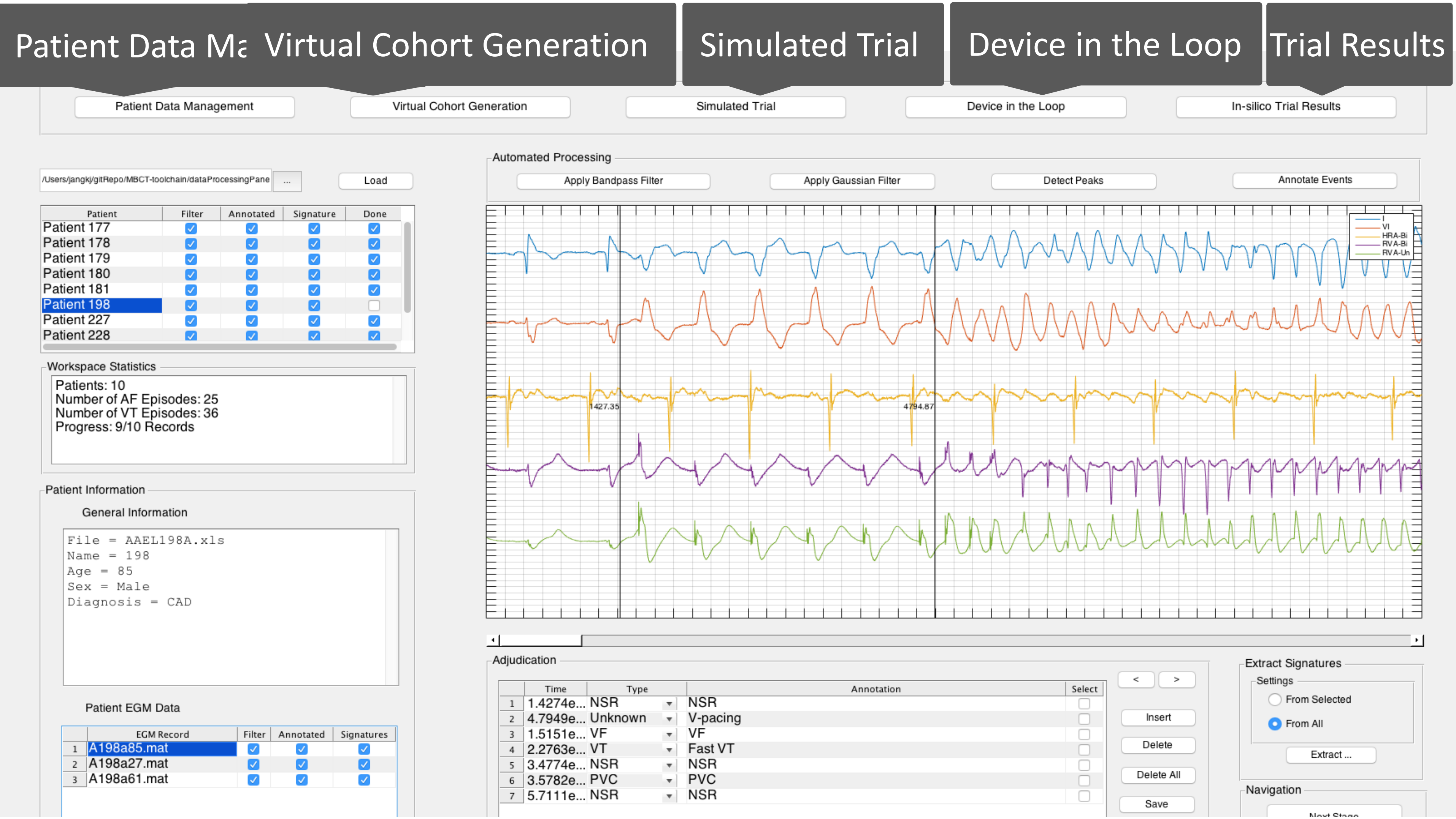


Result 2: Patient Condition-level Analysis

Table 1: Specificity for SVTs and sensitivity for VTs.

Arrhythmia	Boston Sci. ICD	Medtronic ICDs	P value
	Specificity (%)		
Atrial Fibrillation	99.8	99.6	0.3167
Atrial flutter	58.3	79.33	<0.0001
Premature ventricular complexes	100	100	1
Nonsustained ventricular tachycardia	100	99.8	0.3171
Other Supraventricular tachycardia	96.3	99.7	<0.0001
Brady-Tachy	100	98.83	0.0079
	Sensitivity (%)		**P value**
Ventricular fibrillation	100	100	1
Ventricular tachycardia	100	100	1

In-Silico Pre-Clinical Trials Toolchain

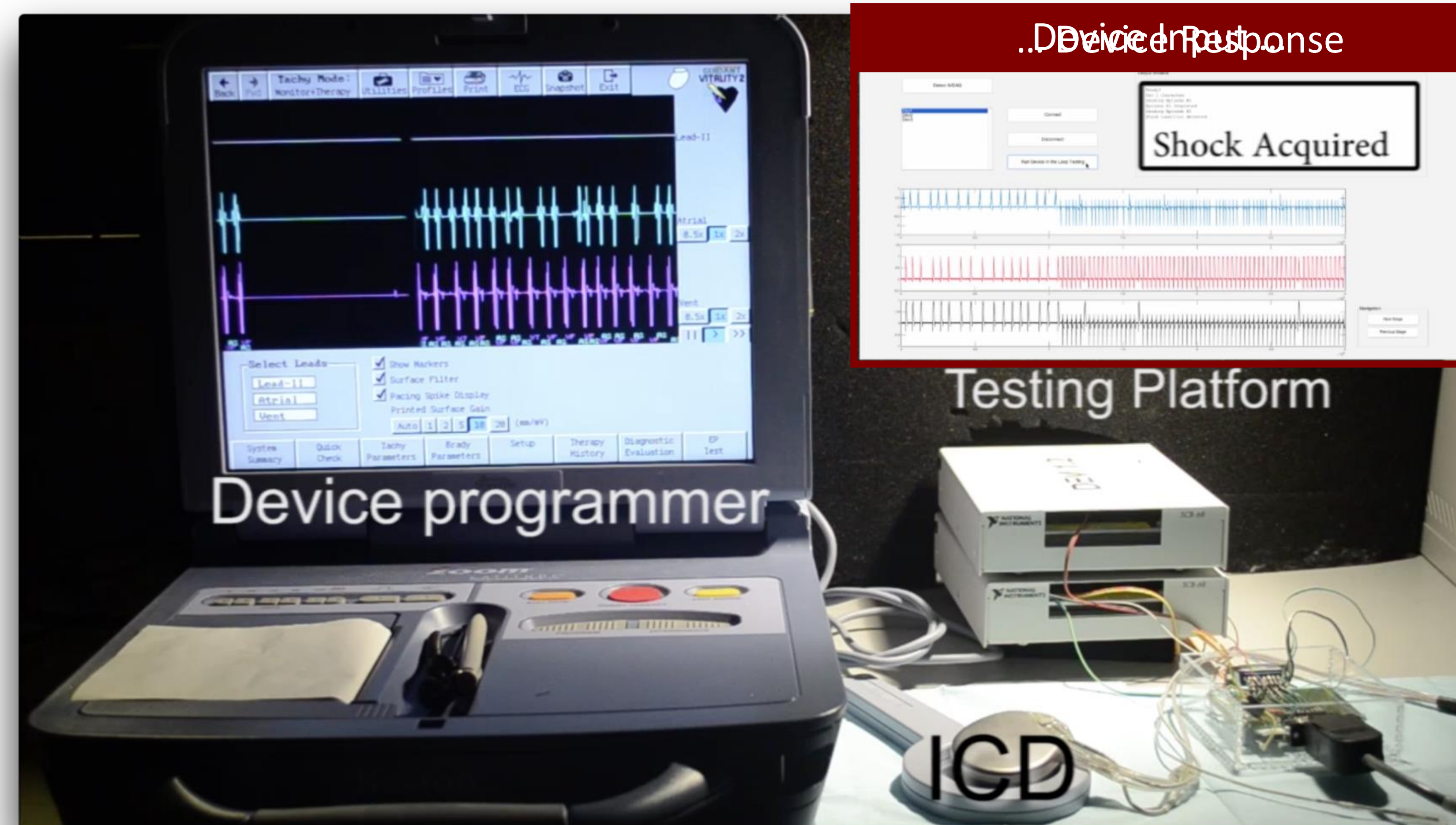


Analysis of results

Penn Engineering

CyberCardia

Device-in-the-loop Testing



Understanding the Application Domain

Medical Collaborators

Director, Cardiac Electrophysiology,
Philadelphia VA Medical Center

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

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

Developing clinical assist system for atrial fibrillation

Electrophysiology Fellow,
Hospital of the University of Pennsylvania

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

Penn Engineering

Industrial Collaborations

Boston Scientific — Advancing science for life™

Provided algorithm descriptions, sample devices, programmers, testing platform

Medtronic

Provided algorithm descriptions, sample devices, programmers, test cases

MathWorks®

Provided model-based design toolbox

NATIONAL INSTRUMENTS™

Provided software and hardware

Penn Engineering

Scott Smolka
Stony Brook

Rance Cleaveland
UMD / Fraunhofer

Rick Gray
FDA

Elizabeth Cherry
RIT

Ed Clarke
CMU

CyberCardia

NSF CPS Frontier

James Glimm
Stony Brook

Sean Gao
MIT

Radu Grosu
Stony Brook /
Vienna

Arnab Ray
Fraunhofer

Rahul Mangharam
Penn

Flavio Fenton
Gatech

Sanjay Dixit
Director of Cardiac
Electrophysiology
Philadelphia VA Hospital

5 Computer Scientists, 2 Cardiologist,s 1 Physicist, 1 BioMed Engineer, 2 Mathematicians, 1 Electrical Engineer

Thanks!

Questions?