CPS: Large: Assuring the Safety, Security and Reliability of Medical Device Cyber Physical Systems (NSF CNS-1035715)

PI: Insup Lee, University of Pennsylvania (lee@cis.upenn.edu)

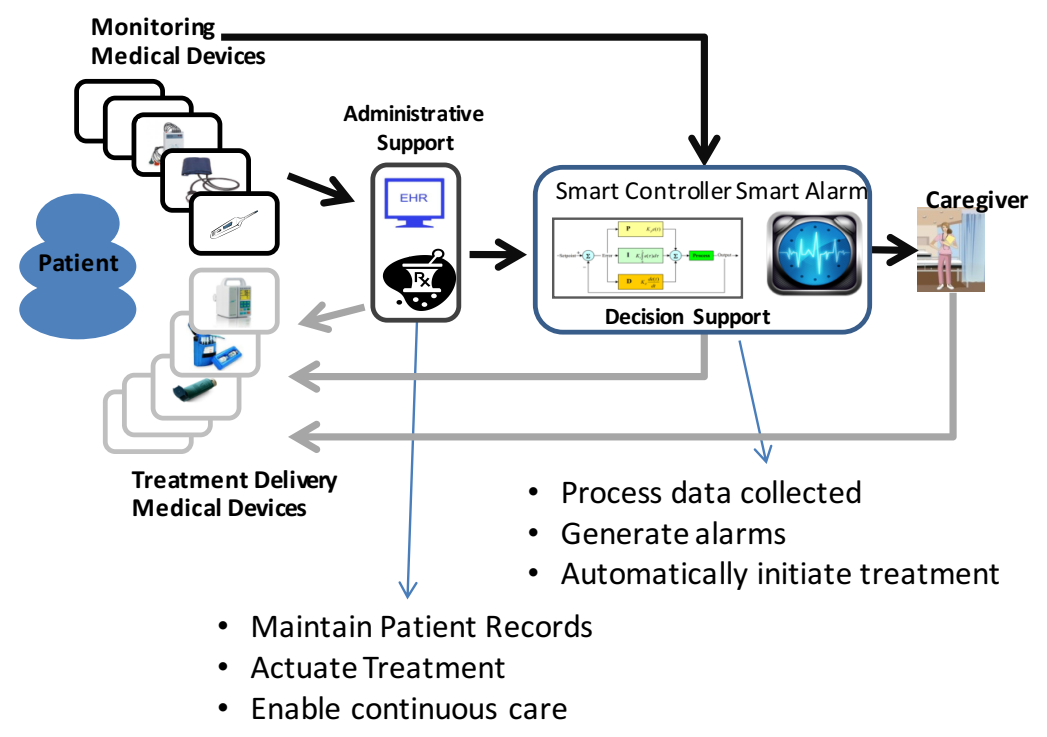
2015 CPS PRINCIPAL INVESTIGATOR MEETING

PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Introduction

- Recent years have seen medical devices go from being monolithic to a collection of integrated systems
- Modern medical device systems have thus become a distinct class of cyber-physical systems, which we call **Medical Cyber Physical Systems (MCPS)**
- The ***goal*** of this project is a new development paradigm for the design and implementation of safe, secure, and reliable MCPS:
  - A compositional development framework for safe and secure MCPS
  - An approach to evidence-based regulatory approval and incremental certification of MCPS
  - Techniques for rigorous evaluation of clinical scenarios, both operational procedures for caregivers and device systems
  - Control-theoretic methods to the design of physiological closed-loop scenarios

MCPS: Conceptual View



Monitoring Medical Devices
Administrative Support
EHR
Smart Controller Smart Alarm
Decision Support
Caregiver
Patient
Treatment Delivery Medical Devices

- Process data collected
- Generate alarms
- Automatically initiate treatment

- Maintain Patient Records
- Actuate Treatment
- Enable continuous care

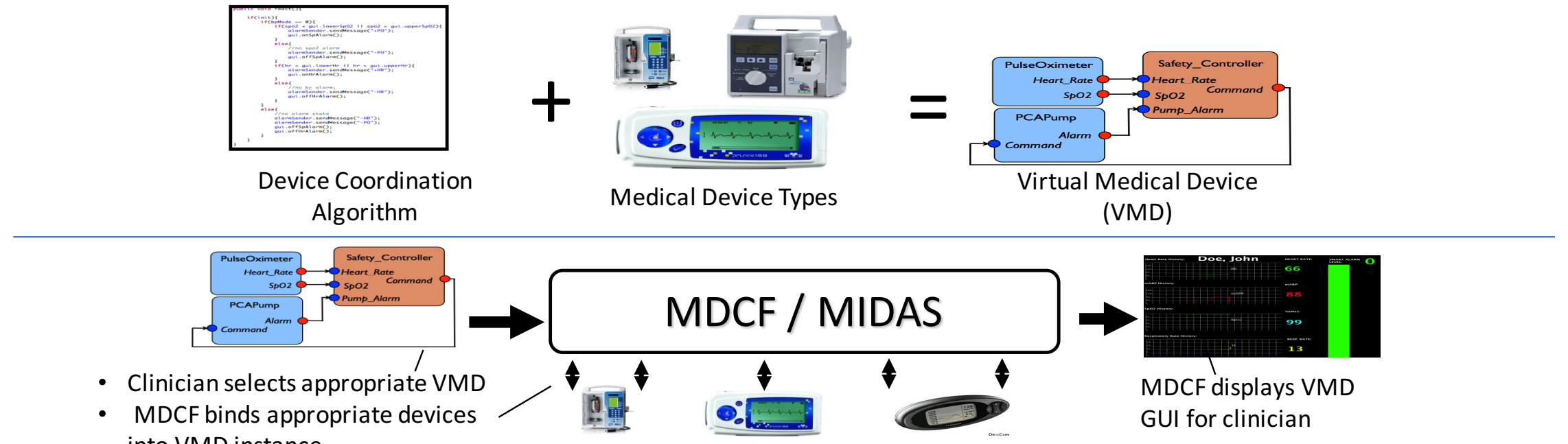
Challenges

Interoperability | Decision Support | Model-Driven Development | Closed-Loop Control | Security & Privacy

Virtual Medical Device (VMD)

VMD

- **MD PnP** (initiative for medical devices interoperability) enables a new kind of medical device, a **Virtual Medical Device (VMD)**, which is composed of medical devices coordinating over a computer network.
- VMDs will not physically exist until instantiated by a hospital. The hospital will be the systems integrator.
- The Medical Device Coordination Framework (MDCF) is prototype middleware for managing the correct composition of medical devices into VMD. The MIDAS resource manager gives the MDCF hard real-time capabilities.



- Clinician selects appropriate VMD
- MDCF binds appropriate devices into VMD instance

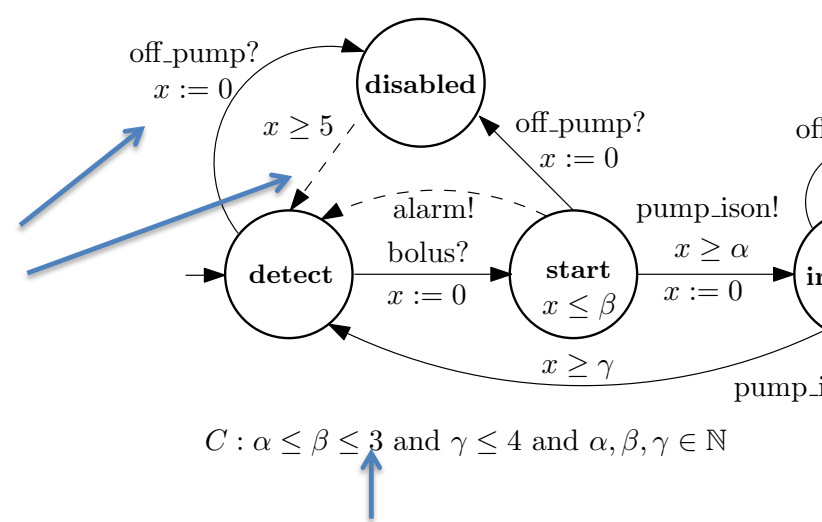
A Modal Specification Approach for On-Demand Medical Systems. Andrew L. King, Lu Feng, Oleg Sokolsky, Insup Lee. In 3rd International Symposium on Foundations of Health Information Engineering and Systems (FHIES 2013), Macau, August 2013

VMD Device Specification Language

- Time Parametric Modal Specifications (TPMS) can express timing and functional variability.
- Compatibility between apps and devices defined in terms of modal refinement.
- Refinement preserves safety and liveness, which allows us to reason about all possible VMD instantiations via a single TPMS.

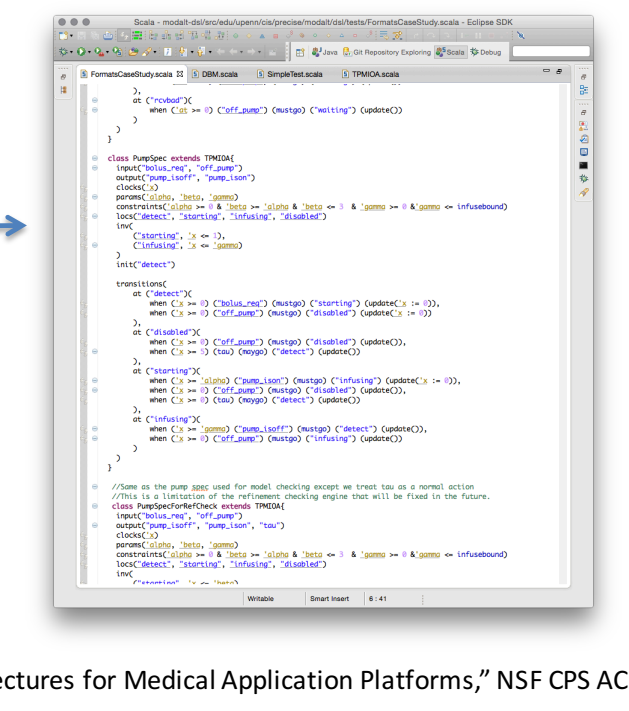
Progress

functional variability expressed using may/must edges



timing variability captured as parametric constraints over clocks

We implemented **ModalT**, an eclipse plugin that enables the specification and analysis of TPMS using efficient symbolic algorithms.

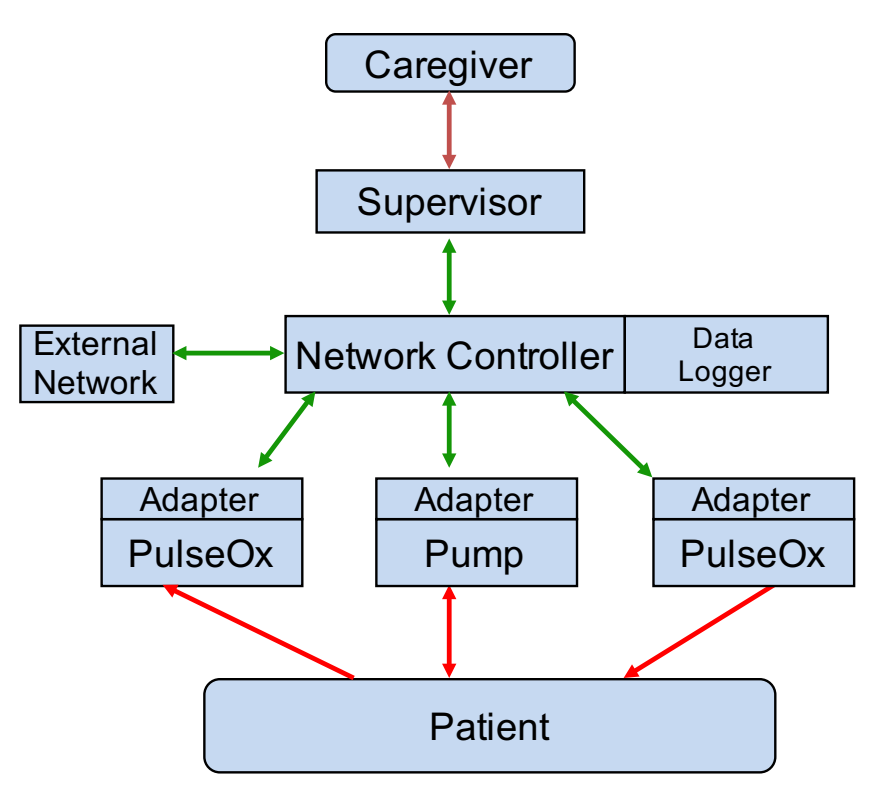


Co-Developed with "Trustworthy Composition of Dynamic App-Centric Architectures for Medical Application Platforms," NSF CPS ACI-1239324

MDPnP Lab @ CIMIT

- Released OpenICE, a DDS-based open-source implementation of MDPnP platform
- Involved with the AAMI standards groups for Assurance Cases and for Infusion Devices for better guidance on clinical issues and safety requirements

Medical Device Mobile PnP Prototype Platform (MD MP3)



- MD MP3 cart is a platform for the development of smart pump control algorithms
- It includes two pulse oximeters, a simulated respiratory rate monitor and an infusion pump specially modified to run software based on prior Generic Infusion Pump research that supports external control over the network
- It runs a real-time network over Ethernet hardware that guarantees message delivery with bounded latency

Smart Alarms and Decision Support

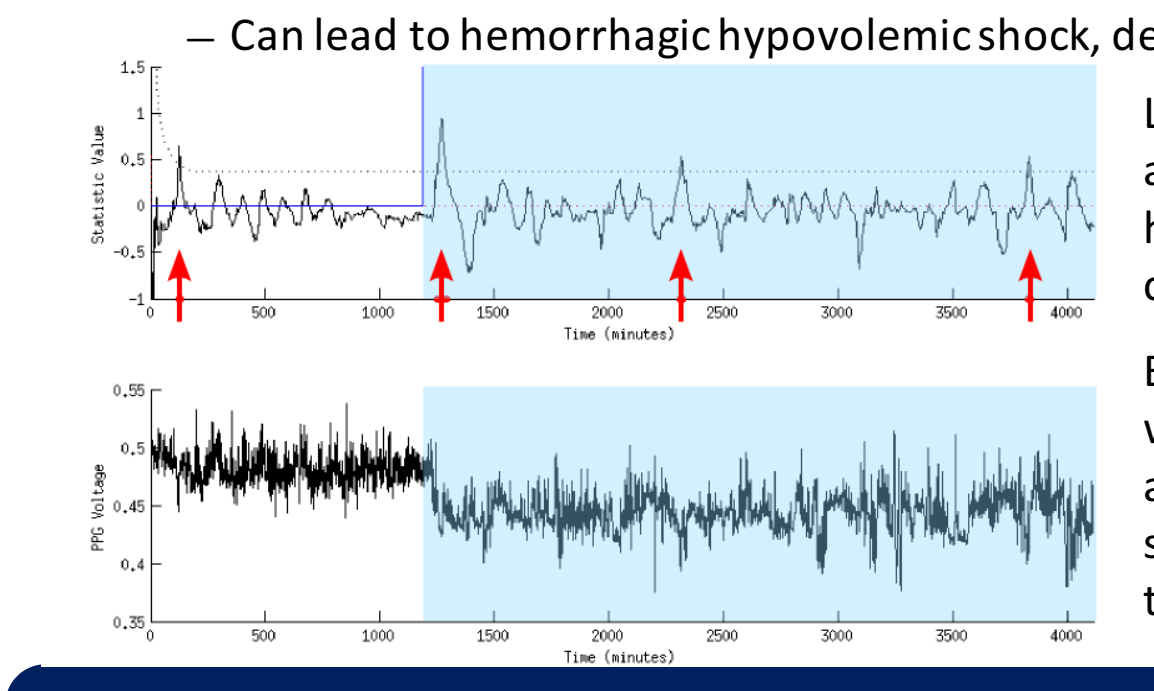
Motivation

Continuous physiologic monitoring challenges:

- Too many false alarms causes alarm fatigue
  - Alarms become useless, clinicians ignore them
  - Puts patients at risk
- Data deluge makes data-driven practice difficult
  - Clinicians discard large amounts of data
  - Reduces the promised benefit of digital medical devices

Automated Hypovolemia Detection

- Hemorrhage common in ICU
  - Can lead to hypovolemia (low volume) over time
  - Non-major hemorrhage difficult to detect due to compensatory mechanisms
- Hypovolemia
  - Can lead to hemorrhagic hypovolemic shock, death

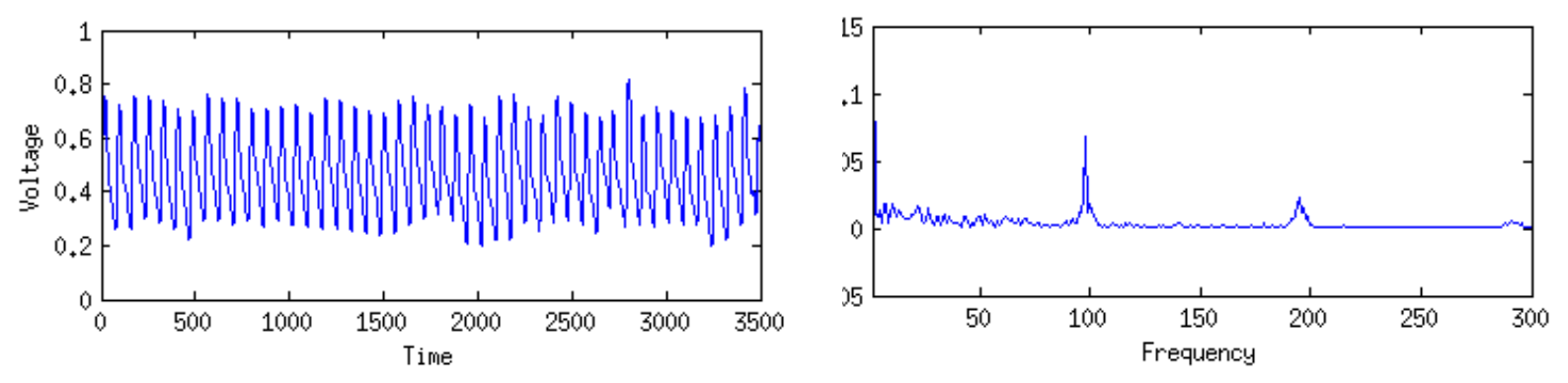


Left: shaded blue area designates post-hypovolemia. Top: calculated detector.

Bottom: PPG waveform. Red arrows designate suggested alarm times

Hypovolemia Detection Results

- Moving Average filtering of PPG Waveform
  - PPG (left) contains large amounts of cardiovascular info
  - Microvascular blood volume
  - Use Fourier Transform to detect fundamental HR frequency (right)
  - Remove sections with noise



- Parameter-Invariant Statistics
  - Model general trend of PPG under normal/hypovolemic states
  - Maintain a constant false alarm rate
- Machine Learning Parameter-Invariant Features
  - Generate numerous statistics over a number of subspaces
  - Use greedy subspace selection, select best dimensions to retain
  - Boost detection rate while maintaining false alarm rate

Robust Monitoring of Hypovolemia in Intensive Care Patients using Photoplethysmogram Signals – Alexander Roederer, James Weimer, Joseph DiMartino, Jacob Gutsche, Insup Lee IEEE Engineering in Medicine and Biology Society 2015

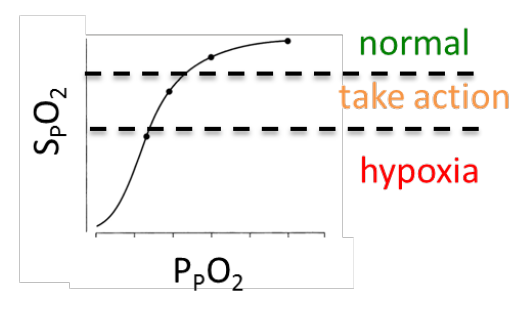
Continuing Work

- Early Detection of Generalized Deterioration
  - "Smarter Alarms" + Parameter Invariance

Early Detection of Critical Shunts in Infants

Pulse oximeter (reactive)

Blood gas analyzer (invasive)



detect changes in P_pO_2 to predict drops in S_pO_2

Parameter-Invariant Detector

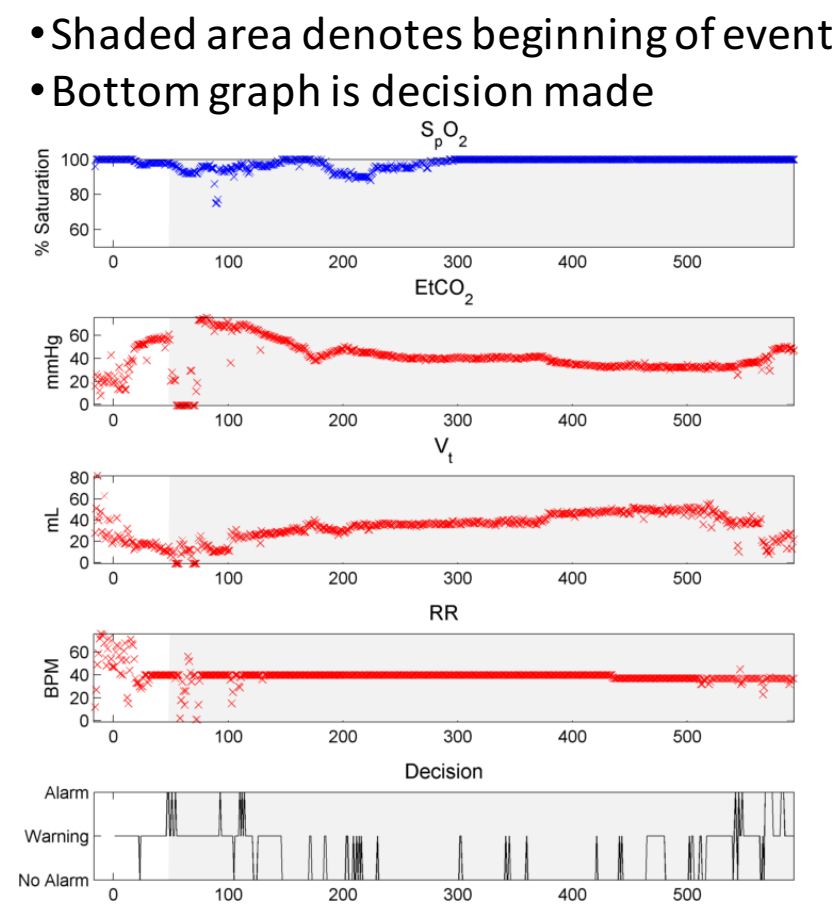
- Guaranteed false alarm rate for all patients
- Works well without rich training data

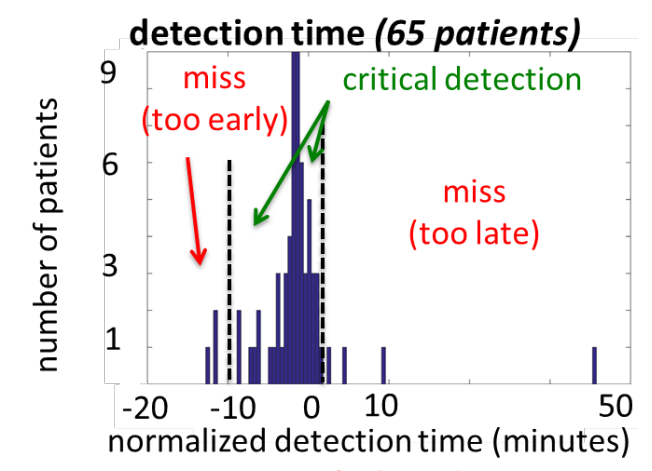
Case Study

- Real-patient data from lobectomy surgeries at CHOP
- Detector implemented in CHOP

Example case with good detection

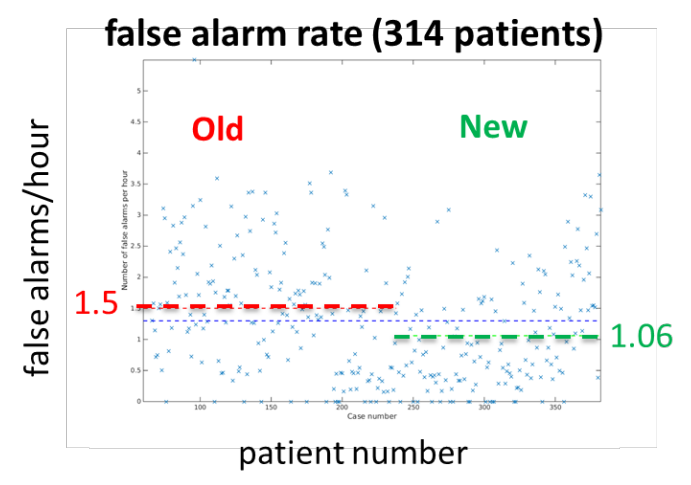
- Variables: EtCO2, tidal volume, resp. rate
- Shaded area denotes beginning of event
- Bottom graph is decision made





~ 89% early detection

~ 100 second average before S_pO_2 drop

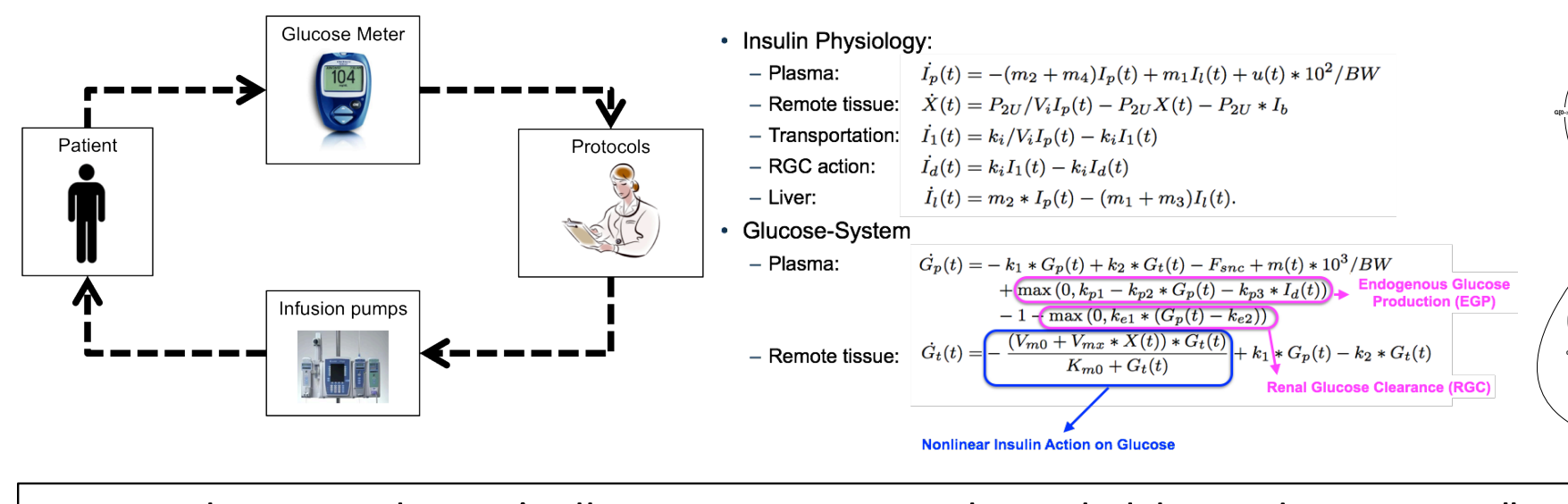


~ 1.3 false alarms per hour (min = 0, max = 5.2)

Closed-Loop Medical Devices

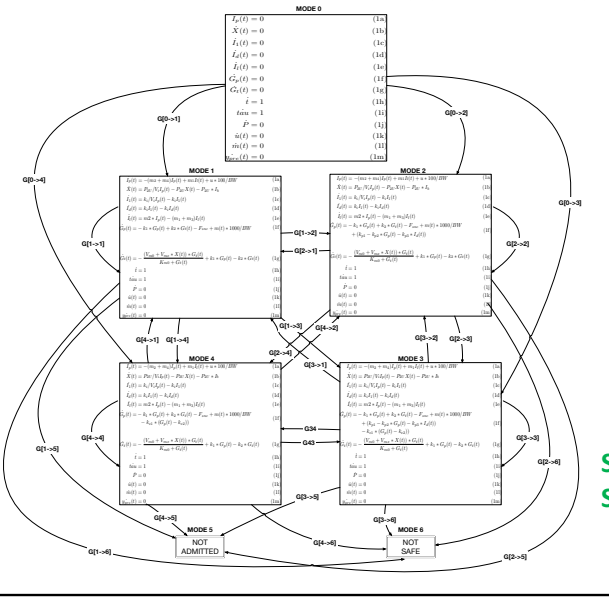
Modeling Intra-Operative Glucose Control

- Intra-operative blood glucose (BG) control
  - Stress-induced hyperglycemia (high BG) → elevated risk of infection
  - Hypoglycemia → life threatening
- Caregivers follow insulin infusion protocols
  - Protocols are empirically designed to an "average" patient
- Problem: Is a protocol safe for all patients?
- Physiological model: an FDA-accepted high-fidelity model customized to the intra-operative scenario
  - Nonlinearity, 7 states, 18 patient-specific parameters
- Control protocol: a mode-switch PD controller from previous work (Kohl, Chen, Mullen-Fortino & Lee, ICHI'2013)



Towards Formally Verifying Safety Properties

- Hybrid system model of the closed-loop system
  - Discrete states: 4 combinations of two non-negative physiological terms EGP & RGC, initial state, "Not Admit" state, "Not Safe" state
  - Given any model parameter and initial state (within the physiologically possible ranges), does glucose level stay within the safe region?
- dReach model checker for a proof-of-concept study
  - A challenging benchmark: Under the "full-state full-parameter" setting, dReach did not finish verifying path depth of 4 in 30 hours
- A benchmark for medical CPS: under-actuated, limited-sensed, un-identifiable parameters, non-linear dynamics, hybrid systems
- Formal verification rules out unsafe design in pre-clinical trials



	Physiological Range State	Physiological Range Parameter	Path Length	Time (hours)	Result
Full population All Initial States	Full	Full	3	30	safe
	Full	Full	4	DNF	-
Single Patient All Initial States	Full	p_0	3	0.1	safe
	Full	p_0	4	0.6	safe
	Full	p_0	5	3.1	safe
	Full	p_0	6	8.2	safe
	Full	p_0	7	16.4	safe
	Full	p_0	8	DNF	-
Small Population Small Initial State Set	$x_0 \pm 0.5$	$p_0 \pm 0.5$	3	0.1	safe
	$x_0 \pm 0.5$	$p_0 \pm 0.5$	4	0.4	safe
	$x_0 \pm 0.5$	$p_0 \pm 0.5$	5	1.1	safe
	$x_0 \pm 0.5$	$p_0 \pm 0.5$	6	2.9	safe
	$x_0 \pm 0.5$	$p_0 \pm 0.5$	7	8.1	safe
	$x_0 \pm 0.5$	$p_0 \pm 0.5$	8	DNF	-

Sanjian Chen, Matthew O'Kelly, James Weimer, Oleg Sokolsky, and Insup Lee. "**An intraoperative glucose control benchmark for formal verification.**" 5th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), Atlanta, Georgia, October, 2015 ***(Model code available online, check paper for details)***

Safety-Assured Model-Based Development for Medical Devices

Platform-Specific Code Generation from Platform-Independent Timed Models Analysis

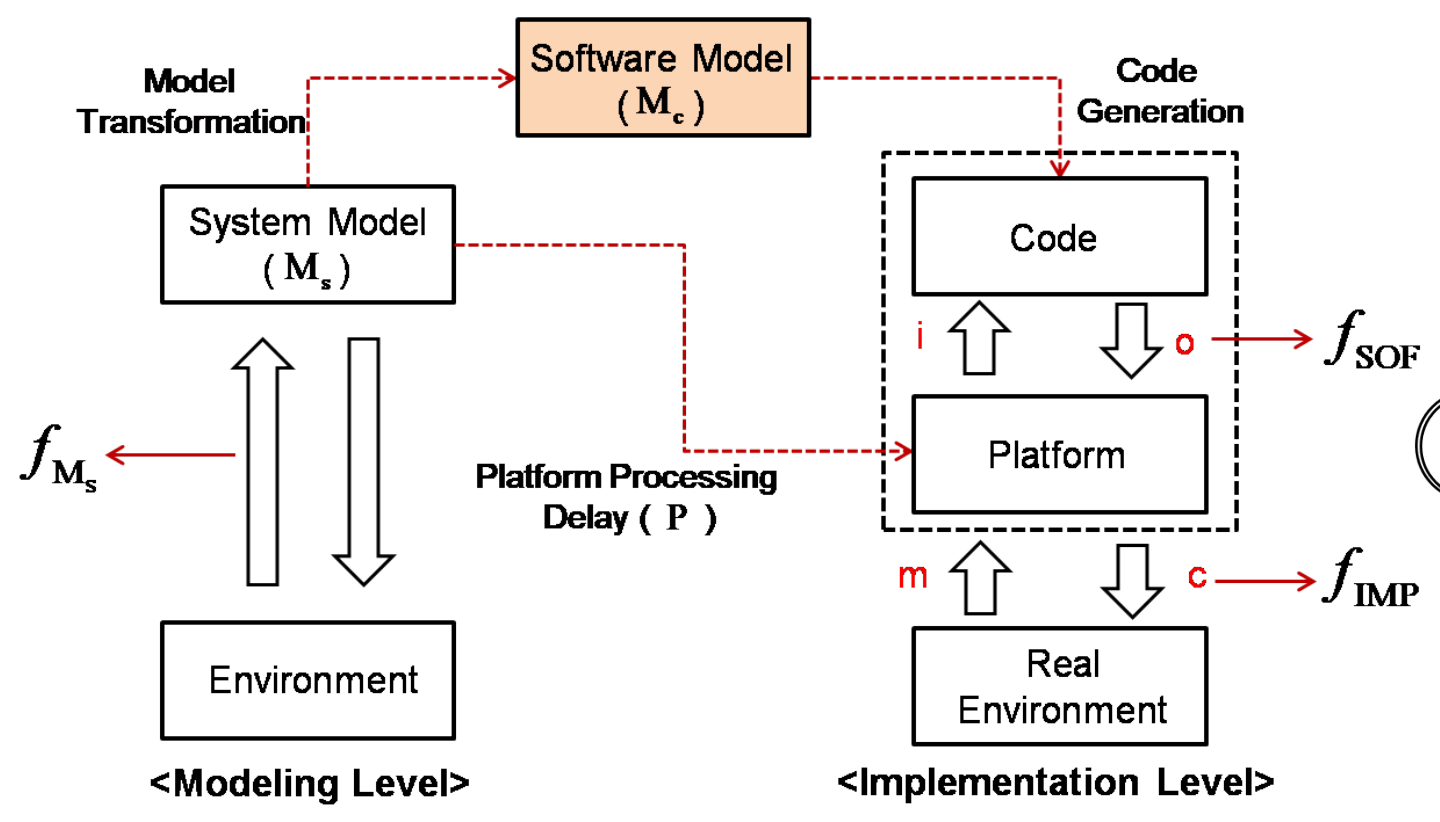
Motivation: Platform-Independent Timing Abstraction

- Enables efficient model verification by hiding the details of the complex platform-specific timing information (e.g., OS scheduling)
- Allows developers to initiate the modeling phase without sufficient platform-specific timing information

Challenges for Code Generation

- System model reflects timing of observable events from the perspective of the environment
- Generated code reflects timing from the perspective of the software
- Additional delays introduced by the plaform, e.g., device drivers and communication jitter, need to be accounted for in a way that preserves properties verified on the model
- Once platform timing parameters are known, timing constants in the generated code need to be adjusted to preserve timing properties of the system implementation from the environment perspective

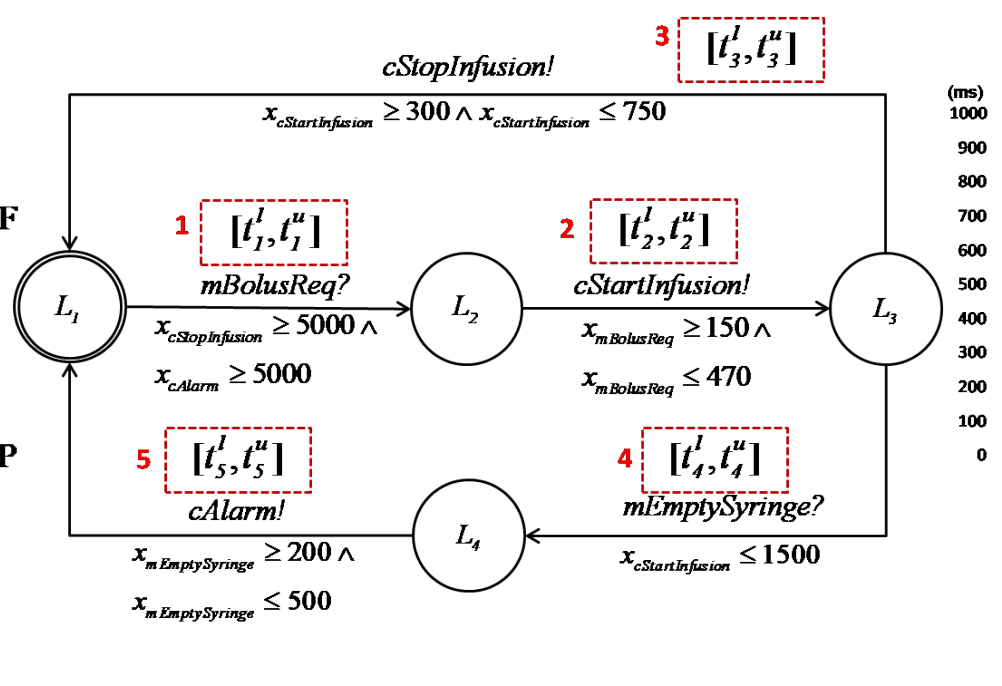
BaekGyu Kim, Lu Feng, Oleg Sokolsky, and Insup Lee, "**Platform-Specific Code Generation from Platform-Independent Timed Models,**" IEEE Real-Time Systems Symposium (RTSS), San Antonio, Texas, December 2015 (to appear)



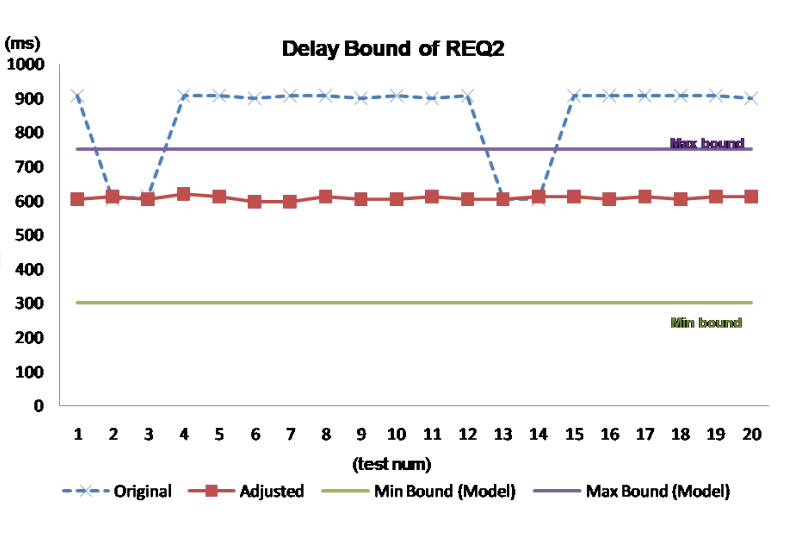
Approach

- Define a model transformation to adjust timing constants
- Transformation is formalized as an integer linear programing (ILP) problem:
  - Objective is to minimize the perturbation of time intervals between observable events
  - Constraints ensure that original time bounds are preserved from the environment perspective

Evaluation: Simplified GCPA Model



cStopInfusion!
$x_{cStartInfusion} \geq 300 \wedge x_{cStartInfusion} \leq 750$
1 $[t_1^l, t_1^u]$
mBolusReq?
$x_{cStopInfusion} \geq 5000 \wedge$
$x_{cAlarm} \geq 5000$
2 $[t_2^l, t_2^u]$
cStartInfusion!
$x_{mBolusReq} \geq 150 \wedge$
$x_{mBolusReq} \leq 470$
3 $[t_3^l, t_3^u]$
4 $[t_4^l, t_4^u]$
mEmptySyringe?
$x_{cStartInfusion} \leq 1500$
5 $[t_5^l, t_5^u]$
cAlarm!
$x_{mEmptySyringe} \geq 200 \wedge$
$x_{mEmptySyringe} \leq 500$
L_1
L_2
L_3
L_4

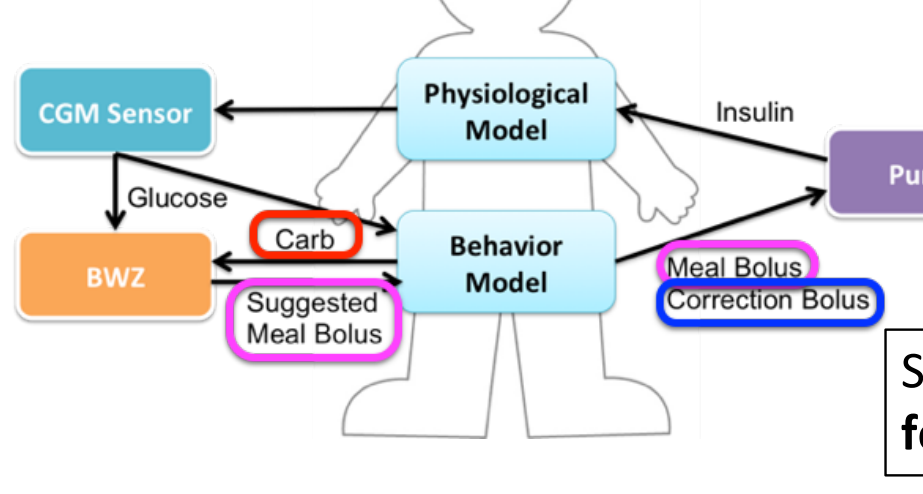


- Sample requirement:
  - (REQ2) The bolus infusion should be active at least 300 ms, and at most 750 ms;
- Platform delays measured on a Baxter infusion pump platform, e.g.:
  - P(mBolusReq)=[50,151],P(cStartInfusion)=[100,303]
- Code generated from the transformed model satisfies the requirements in all tests

Patient Behavior Modeling

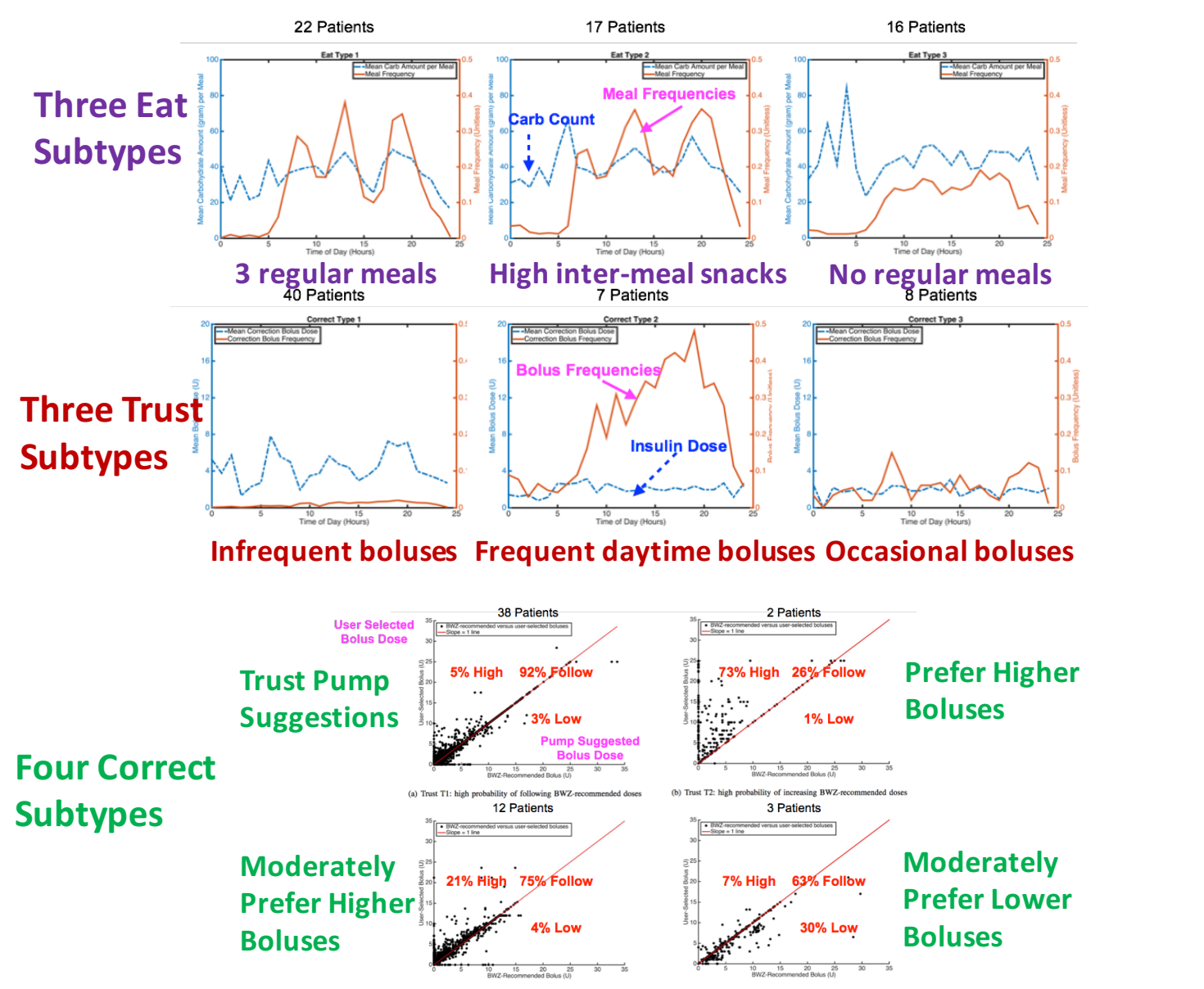
Modeling Insulin Pump User Behaviors

- About 350,000 diabetics currently use insulin pumps
- Insulin pumps require user supervision
  - Input meal information, approve pump-suggested boluses
- Problem: How does behavior impact glucose physiology?
- Clinical dataset: 55 patients at Hospital of UPenn (HUP), age 45.7 ± 15.3, body weight 79.2 ± 21.9 kg
  - Represents the majority of insulin pump users seen at HUP
- Three behavior aspects
  - **Eat**: distributions of mealtime and carb counts
  - **Trust**: the likelihood of user following pump-suggested boluses and distributions of dose adjustments
  - **Correct**: distributions of correction-bolus frequencies and doses



User Behaviors Types

- K-means clustering of individual behavior profiles



Closed-Loop Analysis

- A commonly-accepted physiological model parameterized to reproduce key BG metrics for individuals
- Encode physiological and behavior models in PRISM model checker
- Evaluate how switching behaviors may change glucose outcomes in a risk-free software verification setting
- The results can inform better patient education and diabetic peer-support

	ETC Type	Hypoglycemia Rate (%)	Hyperglycemia Rate (%)
Actual type	E3T2C1	**6.93**	8.43
Change E subtype	E1T2C1	6.20	12.78
	E2T2C1	5.99	13.72
Change T subtype	E3T1C1	0.02	10.33
	E3T3C1	0.04	10.09
	E3T4C1	0.02	11.05
Change C subtype	E3T2C2	7.04	6.30
	E3T2C3	6.95	7.93
Change multi-subtypes	E2T1C1	0.04	16.46
	E2T2C1	5.99	13.72
	E3T1C3	0.10	9.76
	E2T1C3	0.08	15.42

Sanjian Chen, Lu Feng, Michael Rickels, Amy Peleckis, Oleg Sokolsky, and Insup Lee "**A Data-Driven Behavior Modeling and Analysis Framework for Diabetic Patients on Insulin Pumps**." The IEEE International Conference on Healthcare Informatics (ICHI), Dallas, Texas, USA, October 2015

Analysis of Adverse Events

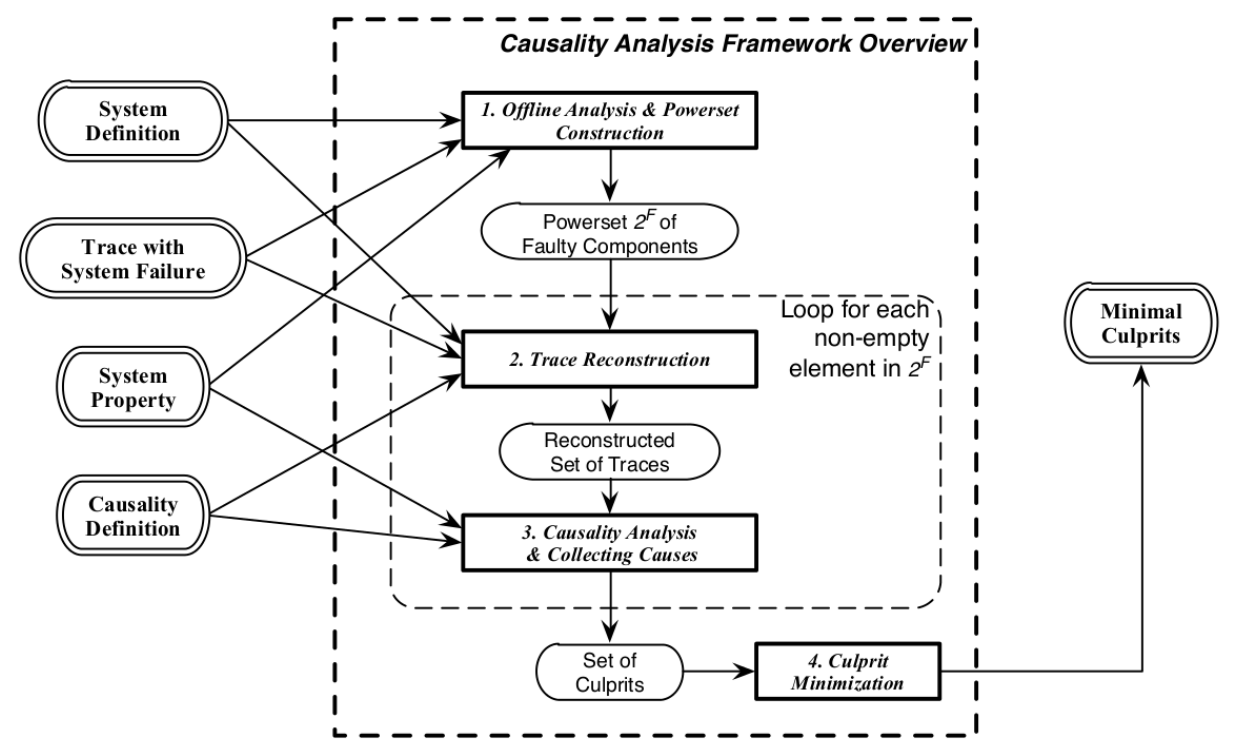
Goal

- In an ICU where many medical devices are connected to a patient, how to identify the device(s) that caused for patient adverse event if one occurs?

Approach

- Symbolic reconstruction of counterfactual traces
  — Check whether the failure is eliminated when behaviors of the chosen subset of components is restricted to their interface specifications
  — If so, a set of culprits is identified
- Formalized as causality analysis
- System implementation using a data logger on the MDCF interoperability plaform

Shaohui Wang, Yoann Geoffroy, Gregor Gössler, Oleg Sokolsky, and Insup Lee. **A Hybrid Approach to Causality Analysis.** In Proceedings of RV'15, the 15th International Conference on Runtime Verification



Causality Analysis Framework Overview
System Definition
Trace with System Failure
System Property
Causality Definition
1. Offline Analysis & Powerset Construction
Powerset 2^F of Faulty Components
2. Trace Reconstruction
Loop for each non-empty element in 2^F
Reconstructed Set of Traces
3. Causality Analysis & Collecting Causes
Set of Culprits
4. Culprit Minimization
Minimal Culprits

Recent extensions

- **Combine horizontal and vertical causality**
  – Improves accuracy of the analysis by eliminating effects of induced faults
- **Use separable components**
  – Rely on actual output of a component during counterfactual trace reconstruction to reduce uncertainty in the analysis

Safety Assurance of On-Demand MCPS

Goal

Develop a regulatory framework and associated safety argument strategy used to build safety cases and regulate on-demand medical CPS

Challenges

Safety system certification: the state of the art

- considers the completely assembled system as a whole, because safety is an emergent property
- a certified system needs to be re-certified if some of its components are changed

On-demand MCPS represents a new paradigm for safety-critical systems

- the final system is assembled by the user instead of the manufacturer
- how can we assure the system safety when we don't know a priori what exact medical devices will be used

Our approach

Regulatory Framework

- Certify Devices, Apps, and Platforms separately if they implement their logical interfaces correctly.

Model Based Reasoning

- Use models to reason about app safety: Model entire system as composition of app, device specifications and environment.

Model-Based Safety Cases

- Justify models based on assurances provided by the regulatory framework.

Progress

- We have developed a regulatory framework proposal and associated App Safety Case Strategy.
- We have applied our argument strategy to a number of on-demand app case-studies including:
  - Closed-loop PCA.
  - Laser-Ventilator Safety Interlock.

Publications

- King *et al.* Towards Assurance for Plug & Play Medical Systems. *SAFECOMP* 2015
- Feng *et al.* A Safety Argument Strategy for PCA Closed-Loop Systems: A Preliminary Proposal. *5th Workshop on Medical Cyber-Physical Systems* 2014

Team

University of Pennsylvania

Rajeev Alur
Ross Koppel
Insup Lee
Rahul Mangharam
George Pappas
Rita Powell
Oleg Sokolsky

Lu Feng
Liang Cheng
Sanjian Chen
BaekGyu Kim
Andrew King
Alexander Roederer
Shaohui Wang

University of Minnesota

Mats Heimdahl
Nicholas Hopper
Yongdae Kim

Michael Whalen
Sanjay Rayadurgham
Anitha Murugesan

Hospital of the University of Pennsylvania

C. William Hanson III
Margaret Mullen-Fortino
Soojin Park
Victoria Rich

Center for Integration of Medicine and Innovative Technology (CIMIT)

Julian Goldman
David Arney

Collaborators

John Hatcliff (Kansas State)
Paul L. Jones (FDA)
Yi Zhang (FDA)