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

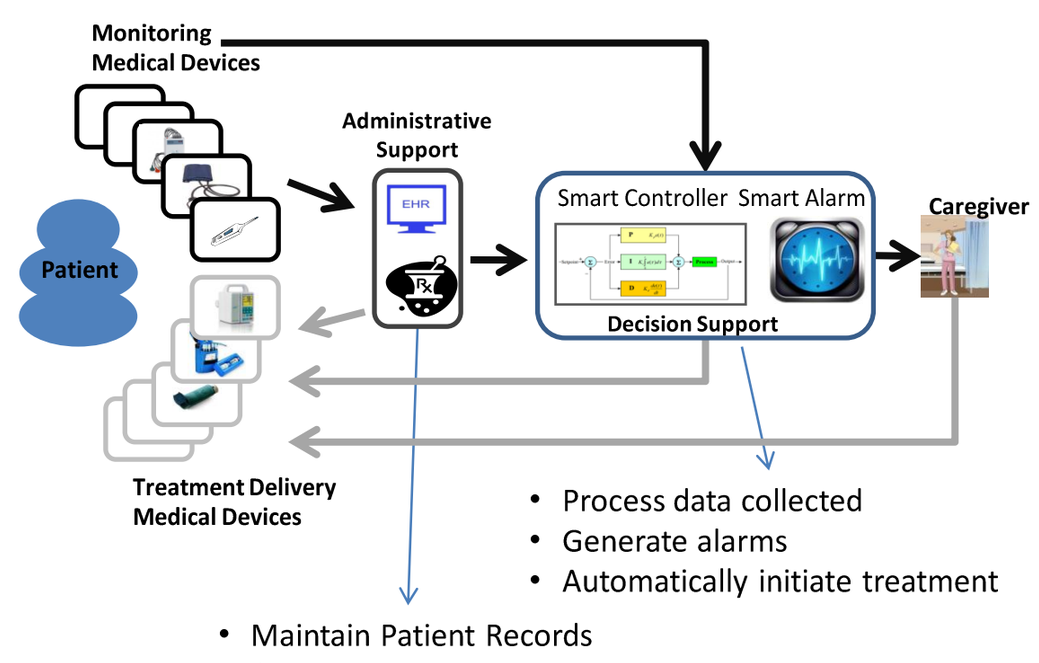
PI: Insup Lee, University of Pennsylvania (lee@cis.upenn.edu)

2014 CPS PRINCIPAL INVESTIGATOR MEETING

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



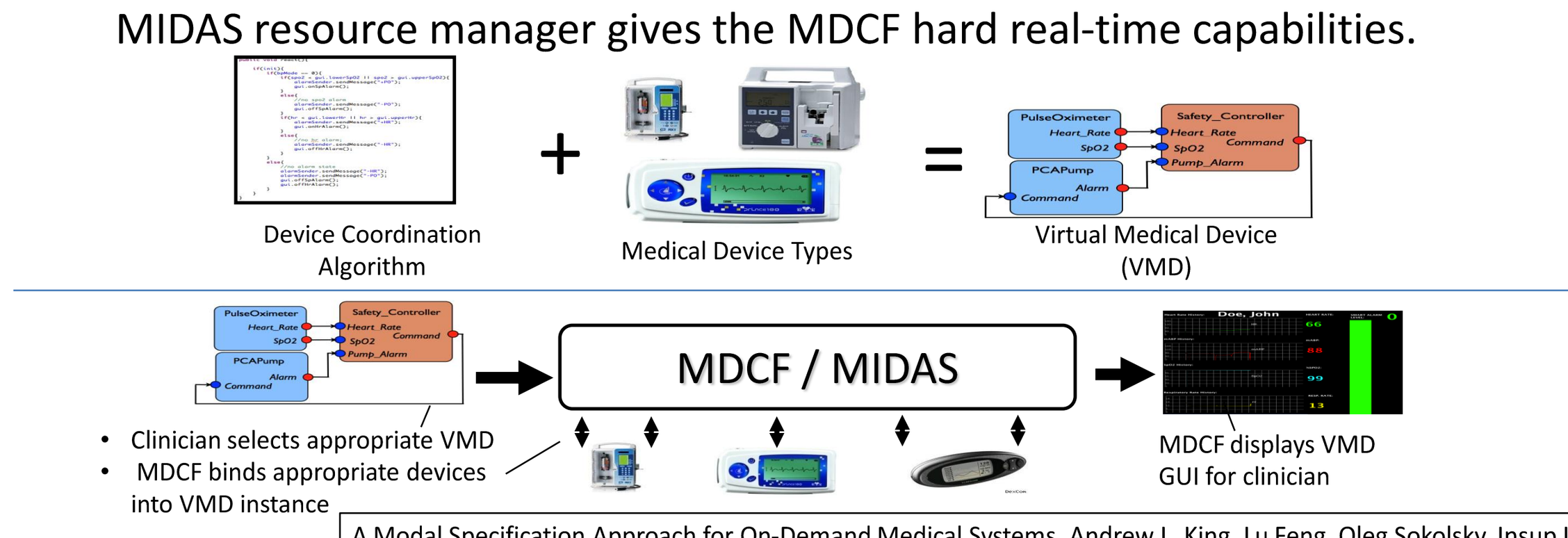
Challenges

- 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.

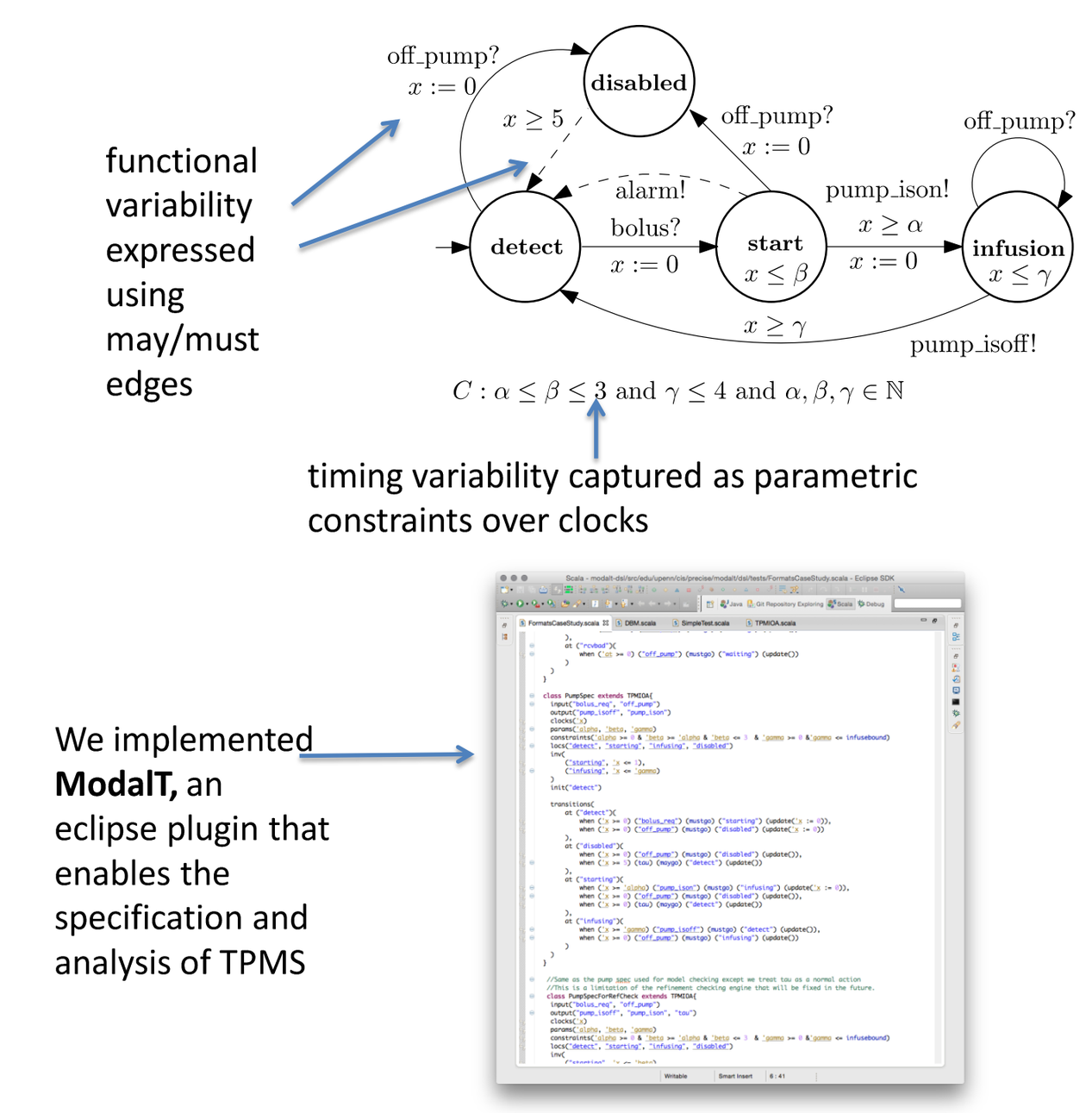


VMD Device Specification Language

- 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.

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

Progress

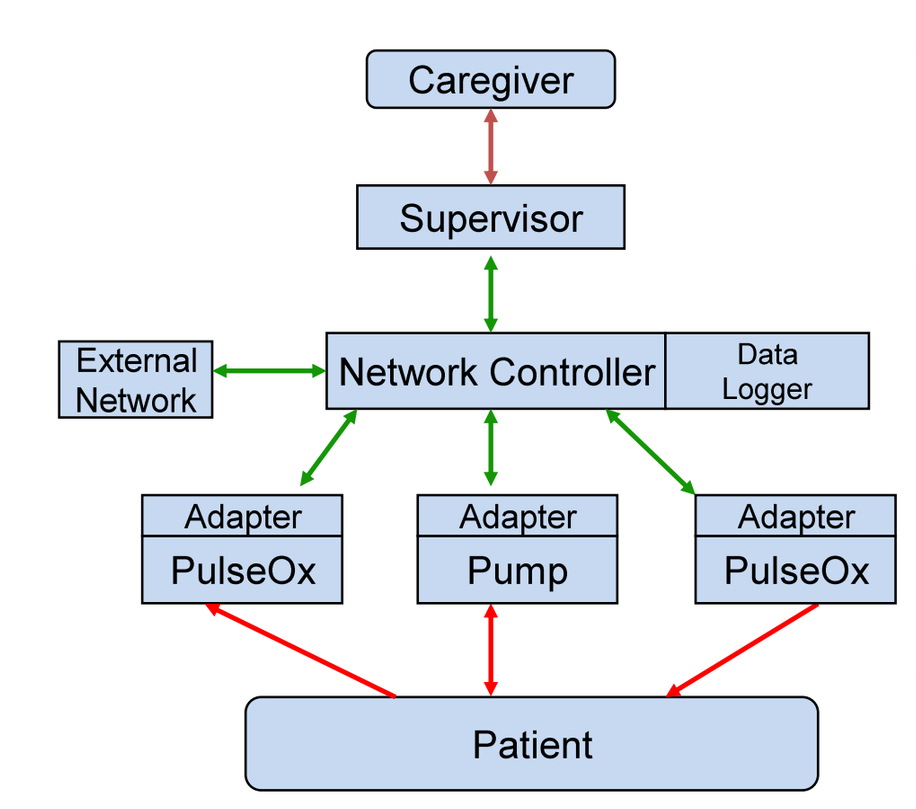


Co-Developed with "Trustworthy Composition of Dynamic App-Centric Architectures for Medical Application Platforms," NSF CPS ACI-1239324

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

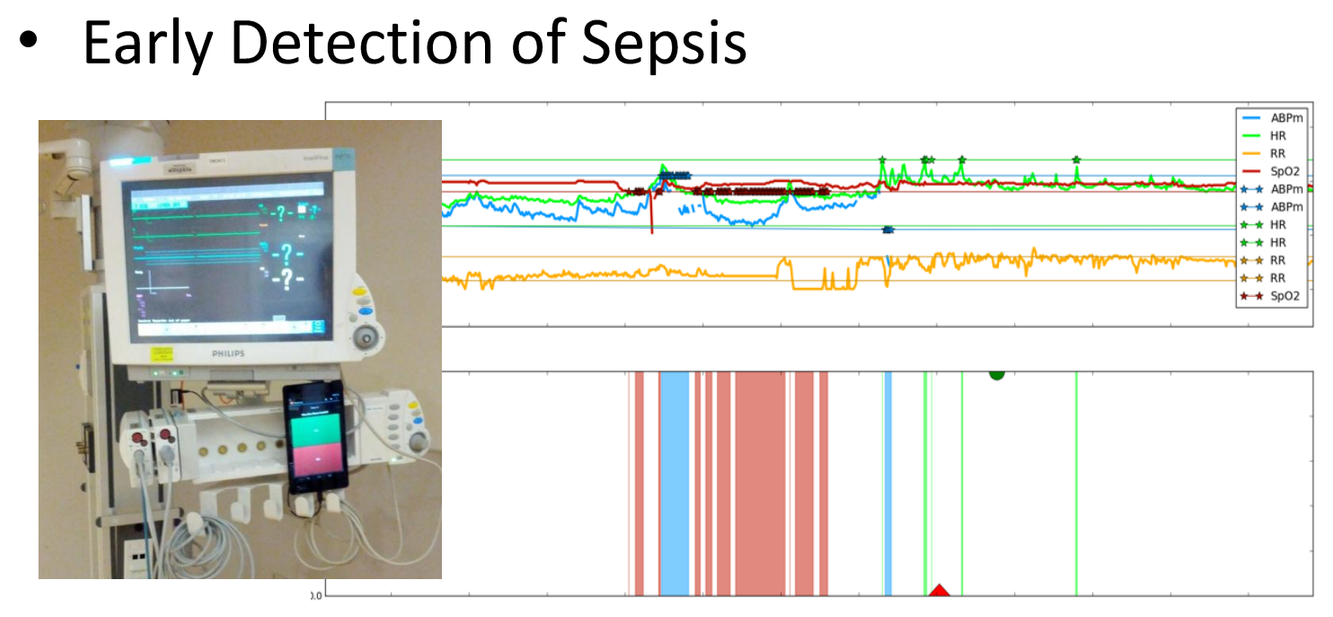
Motivation

Continuous physiologic monitoring challenges:

- Too many false alarms cause 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

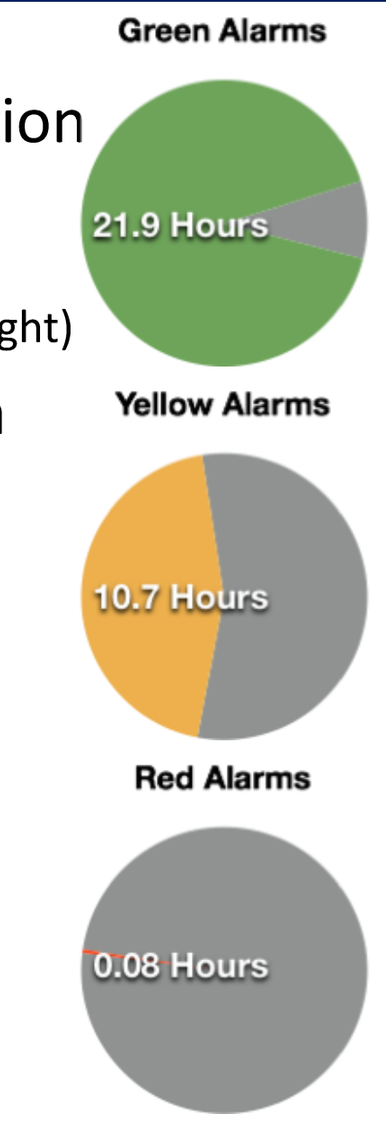
Projects

- Smart Alarm Refinement
  - Accurate detection of deterioration in Surgical ICU
- Vasospasm Clinical Decision Support
  - Learning to predict vasospasm from physiologic data
- Early Detection of Sepsis



Smart Alarm Results

- Presbyterian Hospital Surgical ICU Data Collection
  - Collection of vitals, alarms, and unique nurse annotations through monitor-adjacent tablets (see left)
  - Has allowed us to quantify alarms types and frequencies (right)
- Validation of published Smart Alarm Algorithm
  - 57% reduction in false alarms
- Refinement using Machine Learning
  - Using nurse annotations as labels for learning



Vasospasm CDS Results

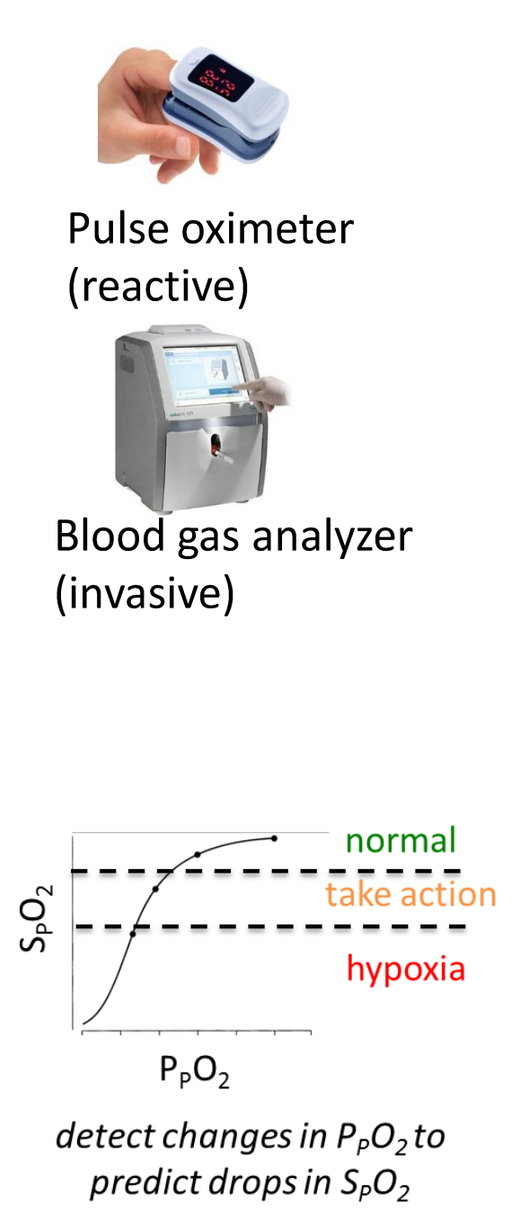
- Improvement in VSP Prediction
  - Utilized commonly collected vitals to more accurately predict vasospasm in subarachnoid hemmorhage patients
  - Uncovered previously unknown predictive vital signs (DBP)

Prediction of Significant Vasospasm in Aneurysmal Subarachnoid Hemorrhage Using Automated Data. Alexander Roederer, John H. Holmes, Michelle J. Smith, Insup Lee, Soojin Park. In Neurocritical Care, April 2014

Continuing Work

- Early Detection of Sepsis
  - Extending Smart Alarm techniques to new Sepsis dataset
- Developing context-aware patient models
  - Improve SICU deterioration detection through invariant modeling (see right)

Early Detection of Critical Shunts in Infants



Parameter-Invariant Detector

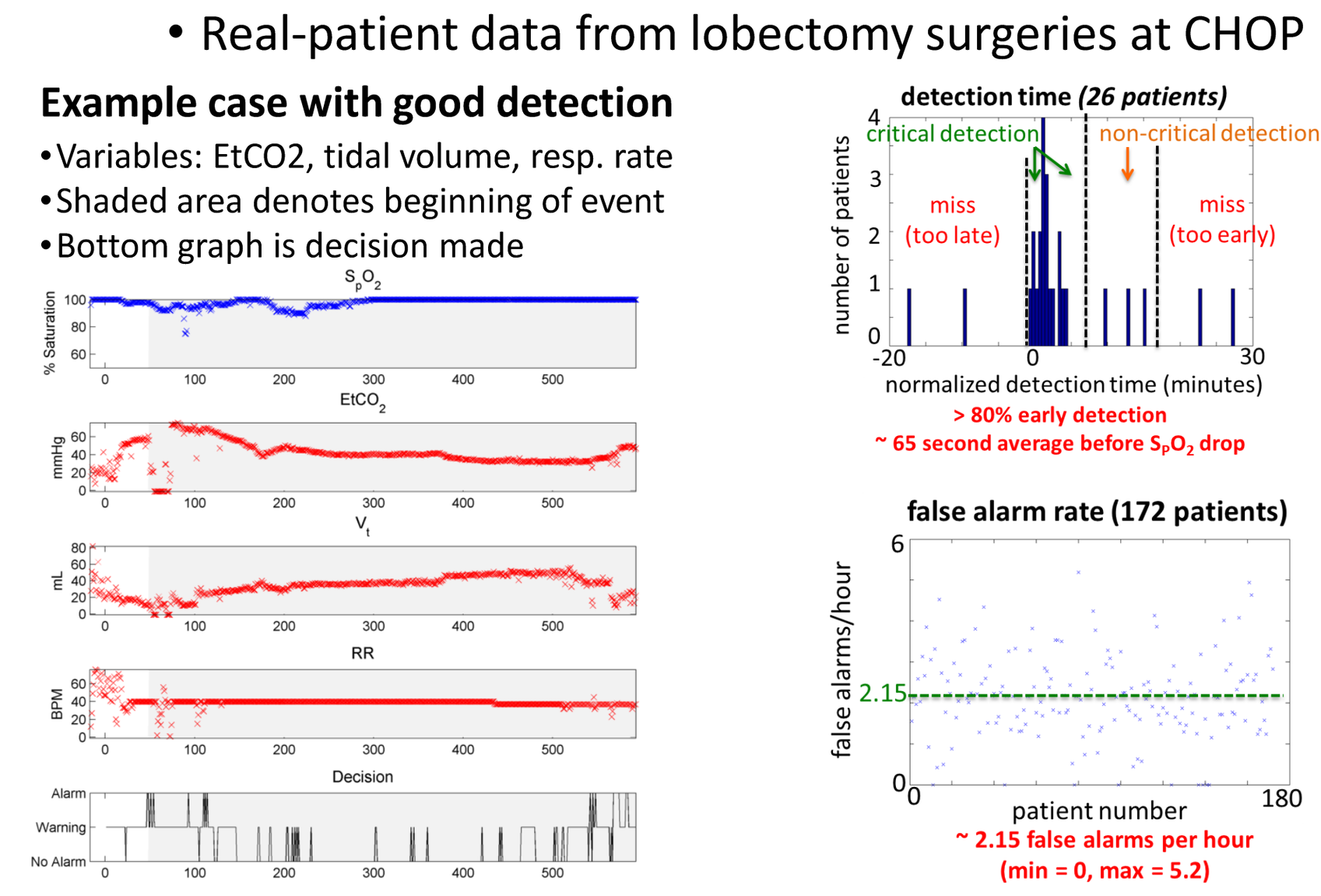
- Guaranteed false alarm rate for all patients
- Works well without rich training data

Case Study

- Real-patient data from lobectomy surgeries at CHOP

Example case with good detection

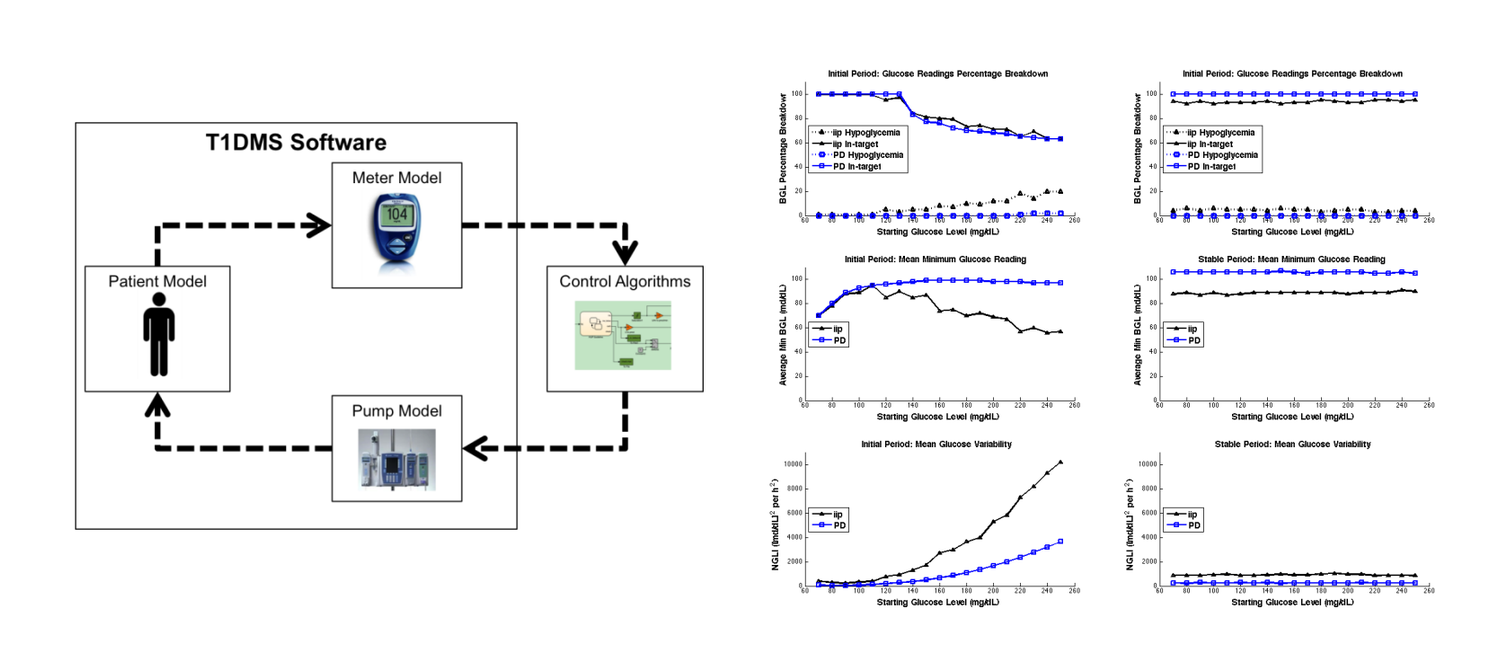
- Variables: EtCO2, tidal volume, resp. rate
- Shaded area denotes beginning of event
- Bottom graph is decision made



Closed-Loop Medical Devices

Evaluation and Enhancement of an Intra-Operative Insulin Infusion Protocol

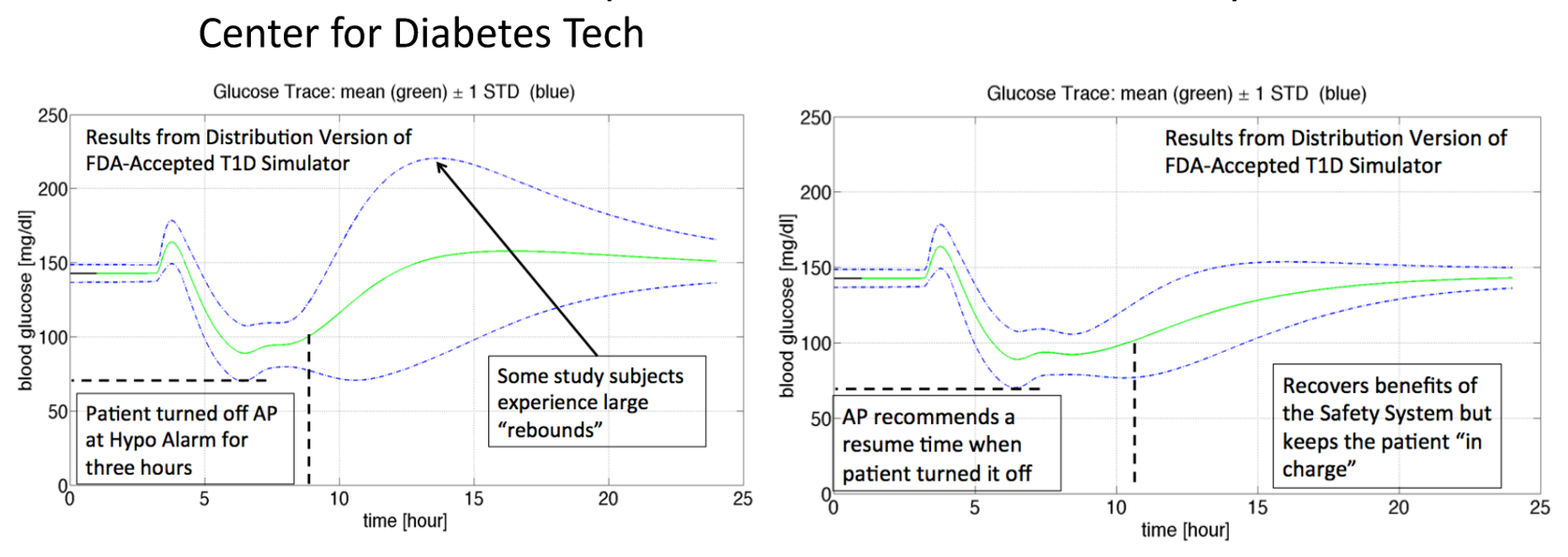
- We evaluated a currently used ICU insulin titration protocol by running in-silico experiments using an FDA-approved Type 1 Diabetic Simulator and compared its performance to a proportional-derivative algorithm we developed
- In-silico trials show that the new algorithm preserves the strengths of the current protocol and overcomes its weaknesses: it minimizes hypoglycemia risk, reduces the glucose variability and maximizes the percentage of in-target-zone glucose readings



Evaluation and Enhancement of an Intraoperative Insulin Infusion Protocol via In-Silico Simulation. Benjamin Kohl, Sanjian Chen, Margaret Mullen-Fortino, and Insup Lee. In IEEE International Conference on Healthcare Informatics (ICHI 2013), Philadelphia, PA, September 2013.

Model-based Safety Analysis of Multi-mode Human-Supervised Closed-loop Medical Systems

- The control algorithm in the artificial pancreas (AP) system can switch between different levels of automation to accommodate user preferences
- We have demonstrated that patient safety may be compromised in certain scenarios and propose a mode-switch supervision mechanism to mitigate the risks
- An unsafe mode-switch example: patient's glucose reading rapidly drops -> the "insulin brake" algorithm attenuates the infusion rate -> user chooses to turn off the pump -> patient's glucose rebounds into hyperglycemia after a prolonged period of no insulin infusion
- Joint work with Dr. Stephen Patek and Dr. Patrick Keith-Hynes at UVa Center for Diabetes Tech



Patek, Stephen D., Sanjian Chen, Patrick Keith-Hynes, and Insup Lee. "Distributed aspects of the artificial pancreas." In Allerton, pp. 543-550. 2013.

GPCA: Model-Based Development

Goals

Develop a set of generic infusion pump development artifacts that can be used as a reference standards and demonstrate safety, using a model based approach.

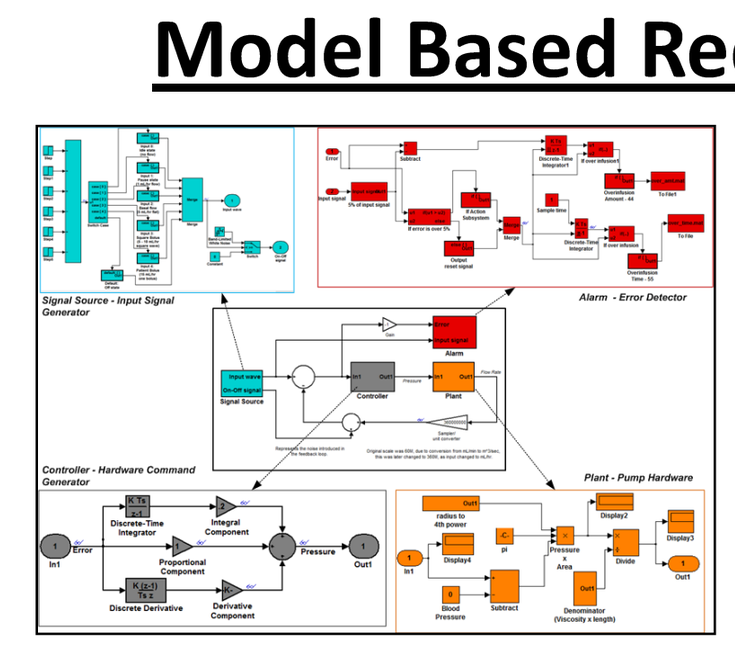
Approach

- Use modeling in the physical domain to elicit requirements.
- Provide clear, precise, and formalizable requirements.
- Decompose system hierarchically to manage complexity.
- Model requirements, component contracts, and component behaviors formally.
- Rely on ensemble of verification tools to show the decomposed system meets its top level requirements.

Challenges

- No guidance as to writing requirements for CPS.
- Approach for architectural decomposition and requirements flow-down lacking.
- Scalable compositional verification tools not available.
- Method for structuring models for verifiability missing.

Model Based Requirements Analysis

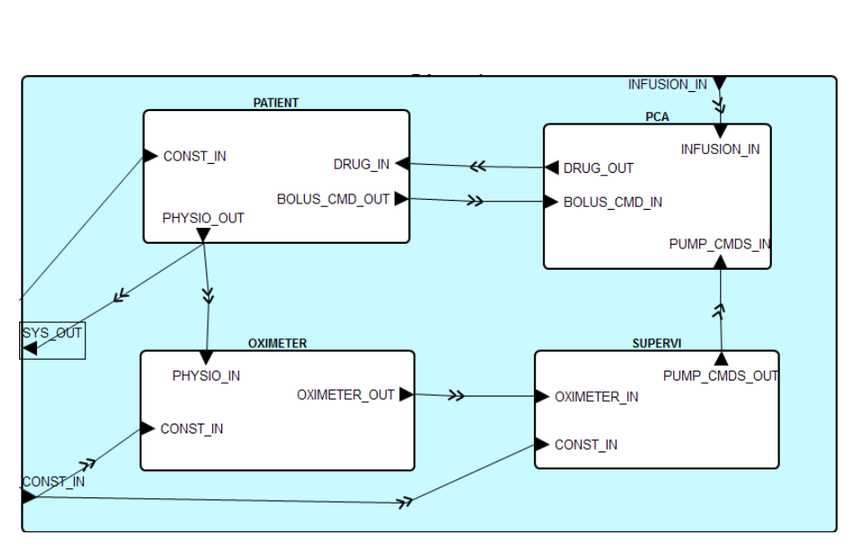


Control System models

- Explore behaviors of physical system
- Evaluation control approaches
- Discover system requirements

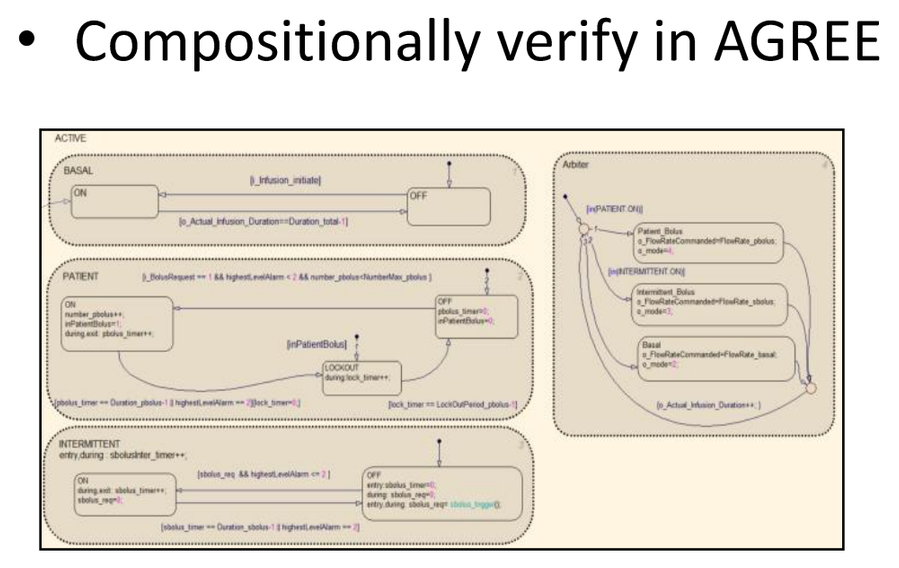
Architectural models

- Precisely scope system.
- Decompose into components.
- Formalize system requirements and component contracts.
- Compositionally verify in AGREE



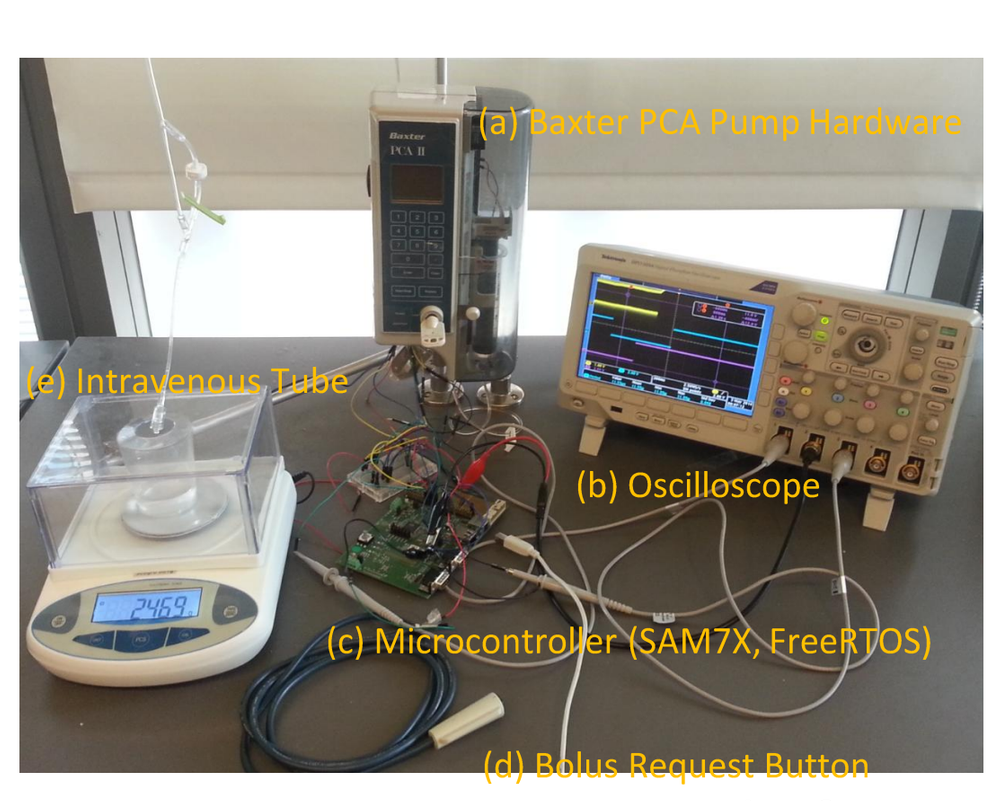
Behavioral models

- Capture detailed behavior of components.
- Verify behavior satisfies component contract.
- Generate code.



Validation

- We are validating the development process using the GPCA reference implementation platform



<Baxter Syringe Pump Platform>

Platform-Specific Timing Analysis

Motivation: Platform-Independent Timing Abstraction

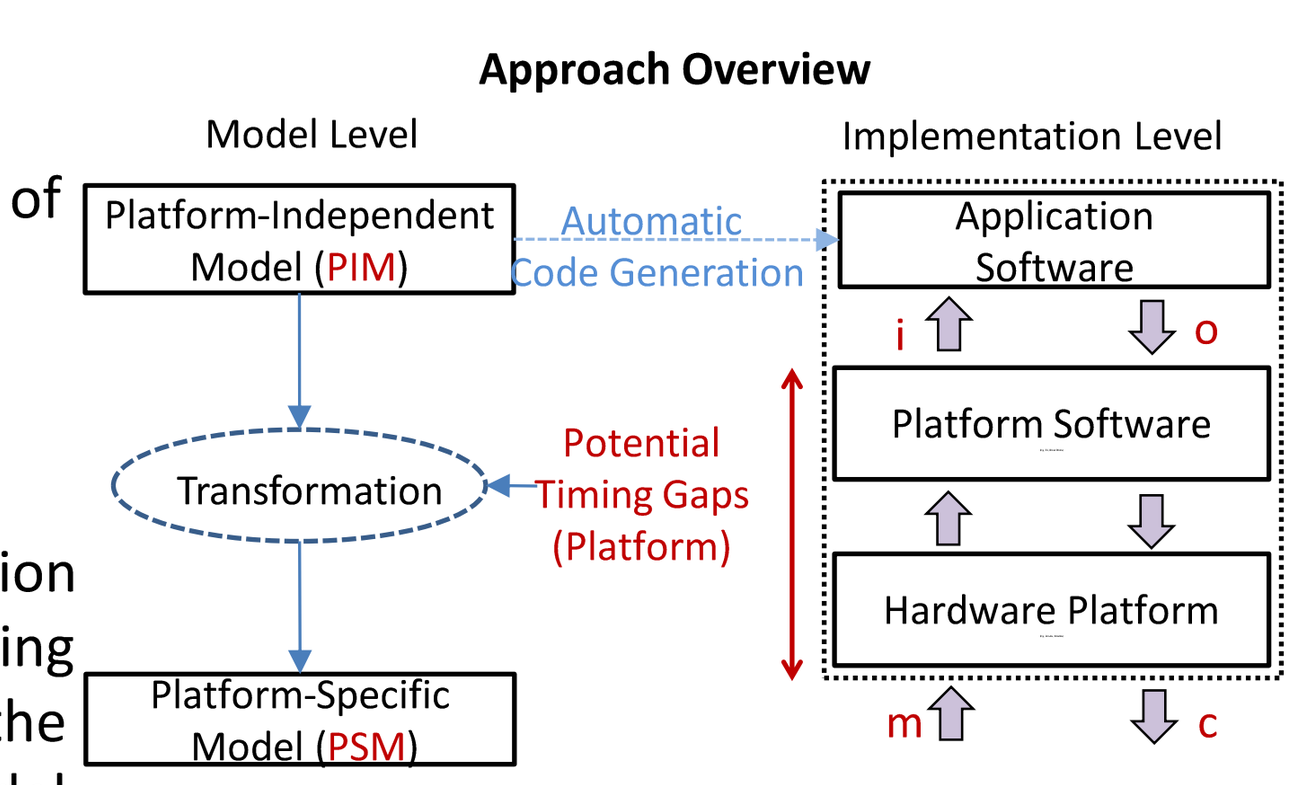
- Efficient model verification by hiding the details of the complex platform-specific timing information (e.g., OS scheduling)
- Initiating the modeling phase without sufficient platform-specific timing information

Goal

- Timing analysis of the platform-independent software executing on a particular platform

Approach

- Define the categorized implementation schemes
- Systematic transformation of the PIM into the PSM
- Validation of the approach using the GPCA reference implementation platform
- (Benefits) Formal verification of the implementation timing behavior decoded from the platform-independent model



Security architecture for MCPS

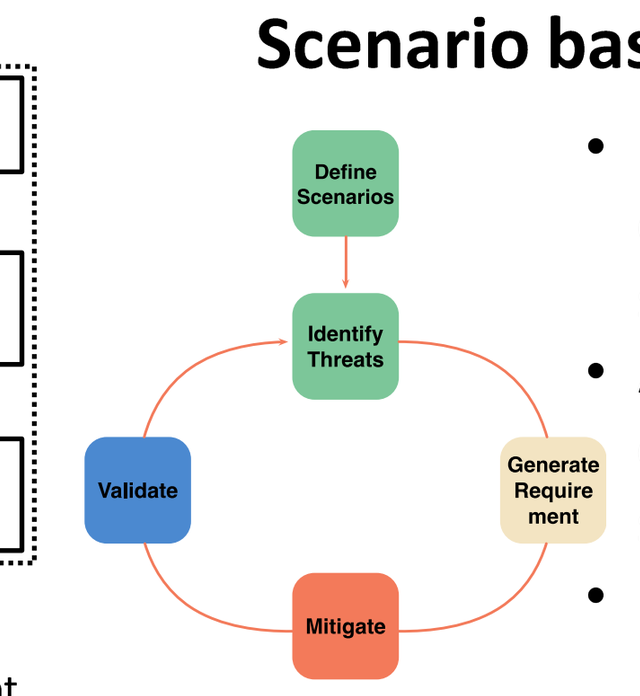
Motivation

- Lack of architectural security solution in practice
- Lack of security requirement definition or instructions in standard

Goals

- Establish a clinical scenario driven process for the identification of security threats in MCPS
- Develop a relatively comprehensive set of security requirements
- Propose a generic security architecture

Scenario based process



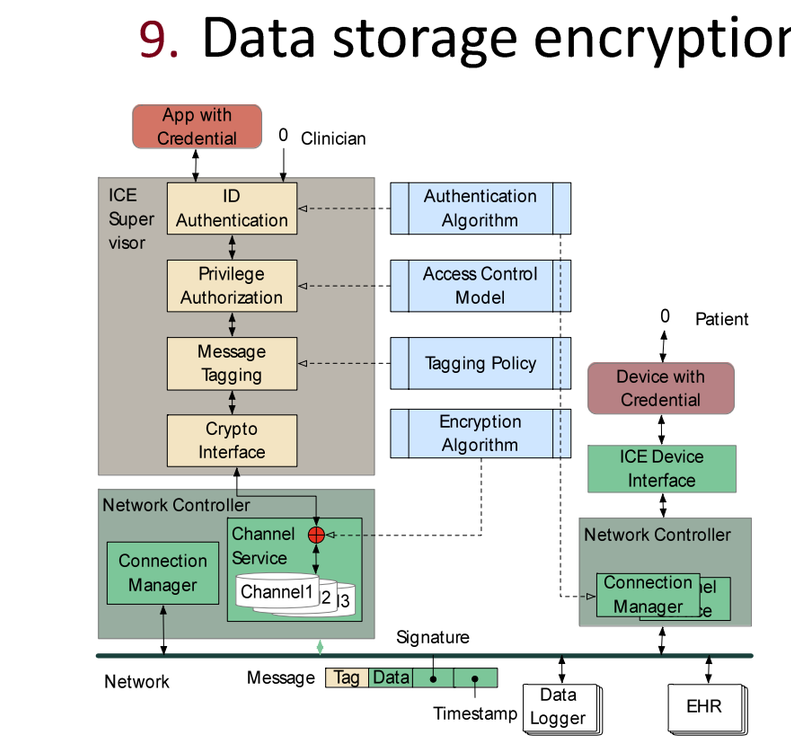
- Traverse clinical scenarios defined in ASTM F-2761 standard
- Apply STRIDE threat category to each asset in scenarios
- Iterate to refine security requirements.

Security requirement set

1. Device and user identification
2. Undeniable log for actions with signature and timestamp.
3. Verification of device (including Apps) authenticity and integrity
4. Communication encryption.
5. Channel flow control
6. Configurable access control
7. Dynamical adjustment for App's privileges
8. A break-the-glass mechanism.
9. Data storage encryption

Security architecture

- Standard oriented
- Modularized design for different requirement set
- Unified interface, customizable Implementation



Next steps

- Evaluate security requirements with domain experts
- Prototype the architecture on an MCPS instantiation
- Verify the architecture against the requirements

Analysis for Medical Device 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?

Benefits

- **Liability attribution**–manufacturers should be hold liable for adverse events caused by their own devices
- **Hazard identification**–discovering potentially unknown hazards in medical device inter-operability setting

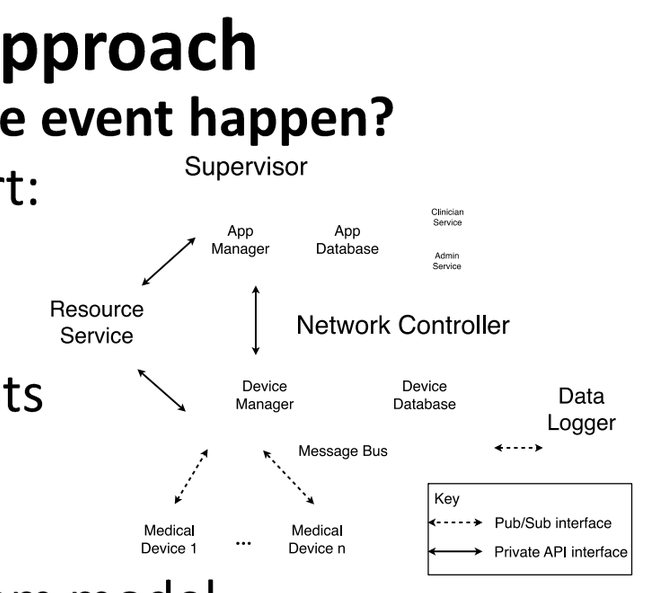
Challenges

- When does an adverse event happen?
- How to define causality?
- How to reason about causality?

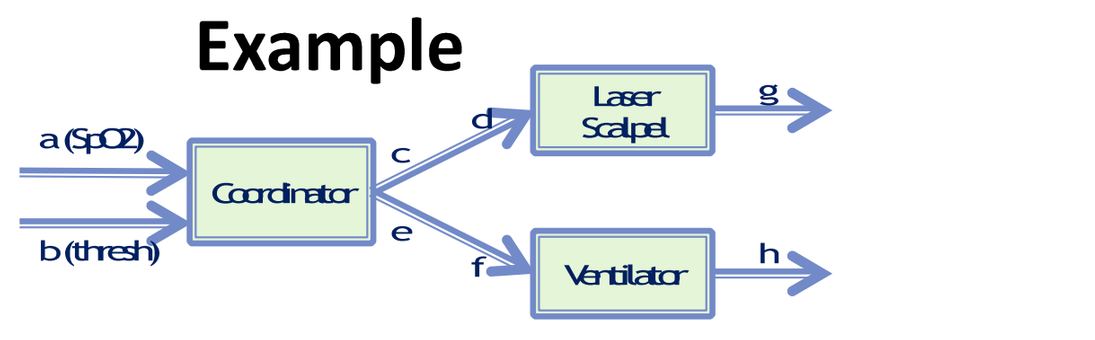
Shaohui Wang, Anaheed Ayoub, Radoslav Ivanov, Oleg Sokolsky, and Insup Lee. **Contract-based Blame Assignment by Trace Analysis.** In Proceedings of HiCoNS'13, the 2nd International Conference on High Confidence Networked Systems.

Approach

- **When does an adverse event happen?**
  - – Architectural support: **medical device data logger** for MDCF
  - – Detect adverse events and device failures by comparing system execution logs to system model
- **How to define causality?**
  - – Use counterfactual reasoning: if a device failure were fixed and the system execution would not trigger adverse event, then the device failure is a necessary cause (analogously for sufficient cause)
- **How to reason about causality?**
  - – Symbolically "reconstruct" all possible system executions and check against causality definitions
  - – A fully automated process



Example



- **System**: (a) whenever a < b, h must be T, (b) g and h cannot both be T
- **Coordinator**: if a ≥ b: c = T, e = F; else: c = F, e = T
- **Laser Scalpel**: g = d **Ventilator**: h = f
- **Trace**: {a→98, b→95, c→F, d→F, e→T, f→T, g→T, h→T}

Analysis:

- – System property violation occurred
- – Coordinator (C) and Laser Scalpel (L) faulty
- – If L outputs g = F to fix its own error, the system violation disappears. So {L} is a necessary cause for adverse events
- – Similarly, {C} and {C, L} are necessary causes too–then minimized to {C} and {L}

Safety Assurance of On-Demand MCPS

Goal

Develop an approach for building safety cases for the certification of 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

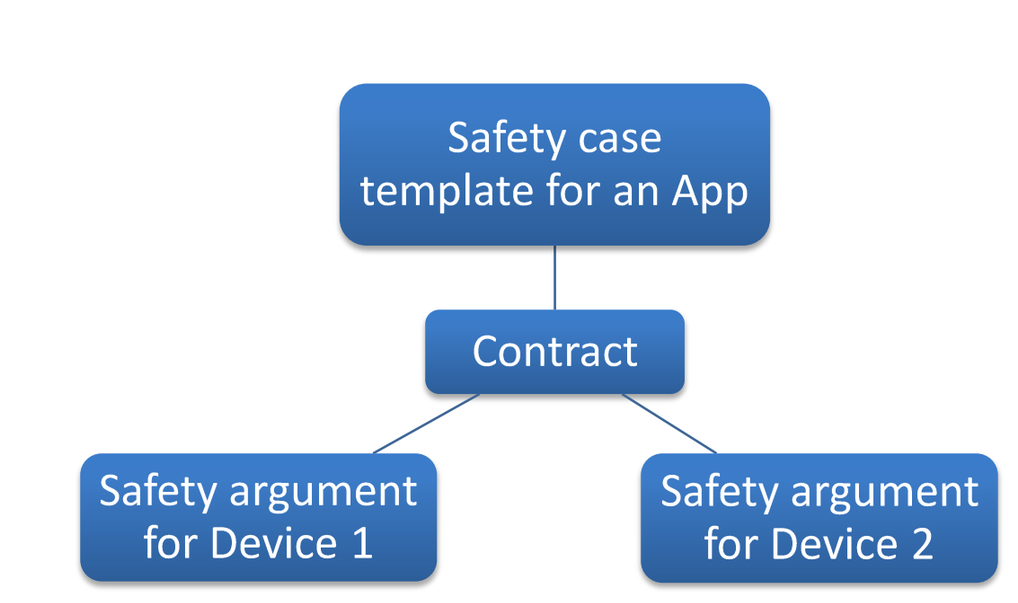
Our two-step approach

Step 1

- Create a safety case template for an APP at the design time

Step 2

- Instantiate the template and generate a concrete safety case instance at the system deployment phase



Team

University of Pennsylvania

Rajeev Alur	Lu Feng
Ross Koppel	Liang Cheng
Insup Lee	Sanjian Chen
Rahul Mangharam	BaekGyu Kim
George Pappas	Andrew King
Rita Powell	Alexander Roederer
Oleg Sokolsky	Shaohui Wang

University of Minnesota

Mats Heimdahl	Michael Whalen
Nicholas Hopper	Sanjay Rayadurgham
Yongdae Kim	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)