# CPS: Synergy: Collaborative Research: Trustworthy Composition of Dynamic App-Centric Architectures for Medical Application Platforms (NSF CNS-1239543/1239324)

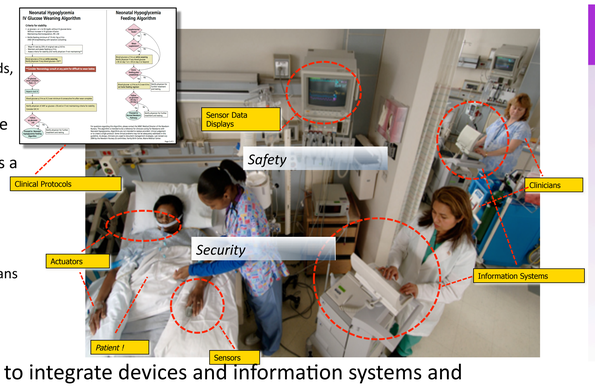

**CPS PRINCIPAL INVESTIGATOR MEETING**

**Lead PI: John Hatcliff (KSU – hatcliff@ksu.edu), PI: Insup Lee (U Penn)**


Problems / Challenges

## Lack of "System of Systems" Support

- Delivering modern medical care involves complex cyber-physical systems…
  - many medical devices, electronic medical records, clinicians/care-givers …all working together to achieve a goal
- Although most modern medical devices have some form of connectivity, they are not integrated so that they can work together as a system
  - devices are "unaware of their context", e.g., details of patient parameters, history, current procedures they may impact/distort readings
  - data from multiple devices is not combined to produce more meaningful information to clinicians
  - actions of multiple devices cannot be automatically coordinated to achieve greater safety and efficiency

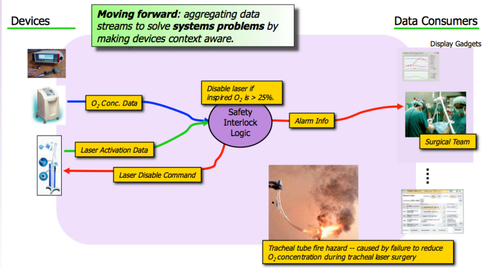



There is no means to integrate devices and information systems and coordinate their actions as a cyber-physical *system of systems*

## What Could be Achieved if Devices formed a System of Systems (SoS)?

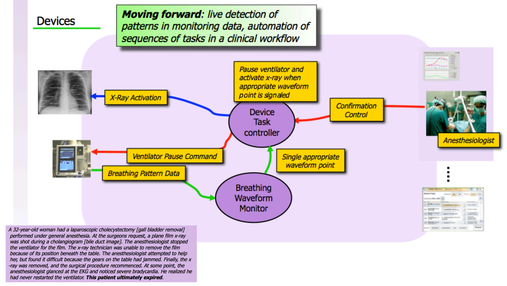
### Safety Interlocks

Fully leverage device data streams and the ability to *control* devices



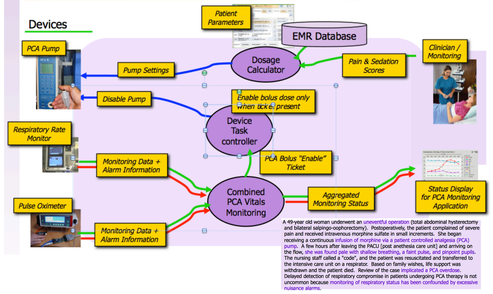

### Workflow Automation / Control

Fully leverage device data streams and the ability to *control* devices




### Closed Loop Control

Fully leverage device data streams and the ability to *control* devices

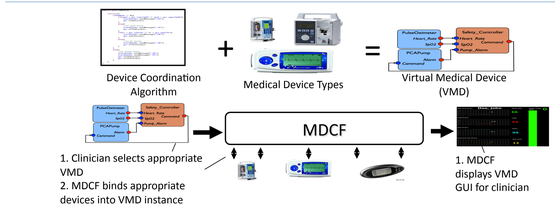



Technology Solutions

## Medical Application Platforms (MAPs)

### The Medical Device Coordination Framework (MDCF)

- Our project is developing an open source *Medical Device Coordination Framework* – a *medical application platform (MAP)* for integrating medical devices into systems
- The MDCF provides…
  - Publish-subscribe real-time middleware for integrating devices
  - A component-based application (app) environment for developing and running algorithms that coordinate the device data flows and actions
- Together the platform, app, and connected devices form a Virtual Medical Device – a composite system device composed of individual devices

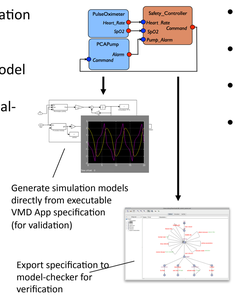



### Research Issues

**Real-time support Via MIDAS Middleware**

- Hard real-time communication infrastructure
- Light-weight
- Pub/sub programming model
- Support for programming clinical-algorithms with real-time constraints
- Event driven
- Time triggered
- Admission control
- Guarantee performance specified by VMD App or prevent clinician from instantiating VMD

**VMD App Validation & Verification**



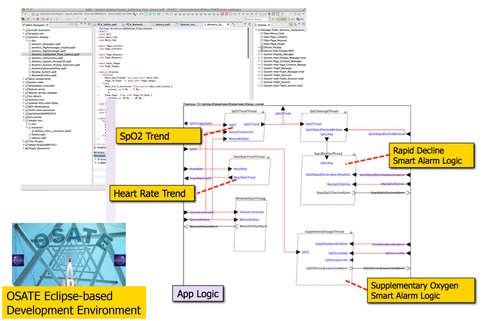

**MDCF Platform Verification**

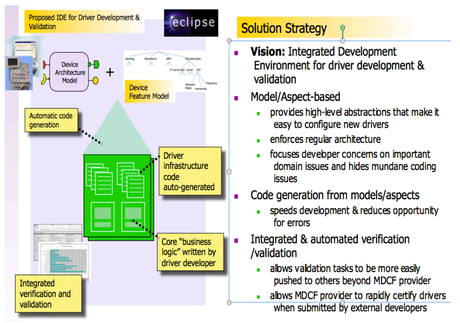
- Device connection protocols
- Device configuration protocols
- VMD setup/tear-down algorithm
- Verify that platform:
  - Correctly implements admission control
  - Correctly implements protocols

The MDCF aligns with the ASTM standard for an *Interoperable Clinical Environment* (ICE) developed by the CIMIT MDPnP project.

## Component-based Development for Coordination Apps

Apps are developed in a model-based development environment based on the industry standard Architecture and Analysis Definition Language (AADL)

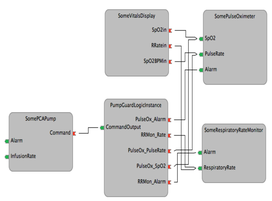



**Solution Strategy**

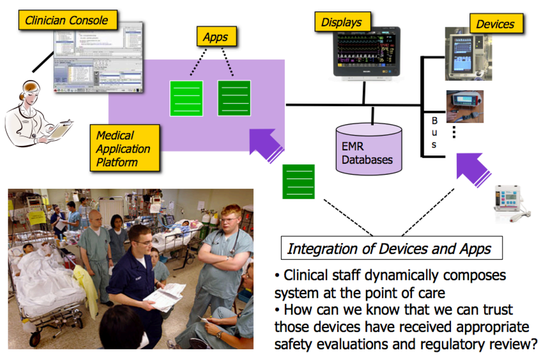
- **Vision:** Integrated Development Environment for driver development & validation
- Model/Aspect-based
  - provides high-level abstractions that make it easy to configure new drivers
  - enforces regular architecture
  - focuses developer concerns on important domain issues and hides mundane coding issues
- Code generation from models/aspects
  - speeds development & reduces opportunity for errors
- Integrated & automated verification /validation
  - allows validation tasks to be more easily pushed to others beyond MDCF provider
  - allows MDCF provider to rapidly certify drivers when submitted by external developers

Components are composed to form coordination apps




Applications

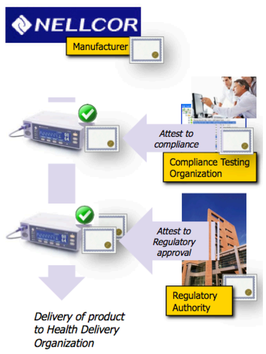
## Authentication Framework for Trusted Composition



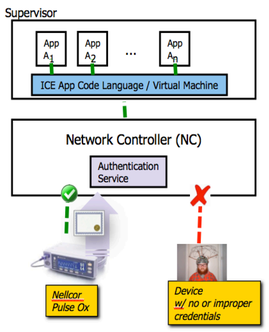



- Clinical staff dynamically composes system at the point of care
- How can we know that we can trust those devices have received appropriate safety evaluations and regulatory review?

**Solution (Part 1):** At critical steps in development/ certification, components are given digital certificates that attest to their safety and compliance with platform architecture

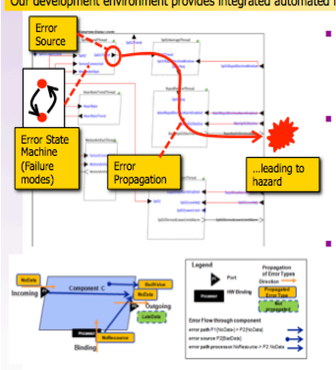



**Solution (Part 2):** When components are integrated, platform automatically checks that components have the appropriate digital credentials



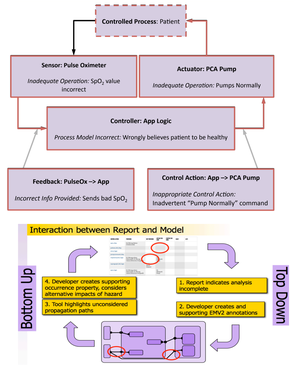

## Component-wise Hazard Analysis and Risk Management

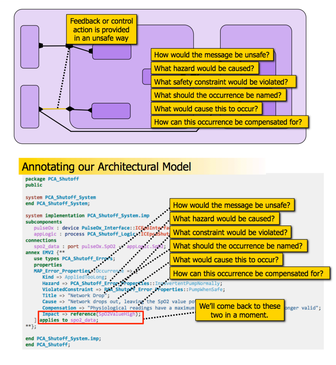
Current risk management activities are highly manual and not well-integrated with formal development artifacts. Our development environment provides integrated automated formal support for risk management activities.




- AADL includes an Error Modeling language dedicated to modeling errors and propagation leading to hazards
- Provides the core of formal architecture-integrated risk management activities from which steps in common hazard analysis such as FEMA, FTA, can be automatically derived.
- Allows engineers to compositionally model aspects of system as it is experiencing faults failures.
  - Necessary for supporting compositional approaches to system safety

Our novel approach involves integrating Leveson's STPA Hazard Analysis with formal architecture models in AADL. Due to our auto code generational from models, hazard analysis is directly traceable to source code and architecture infrastructure components.




Outreach/Impact

## Industry Collaboration

Demo for NIH with CIMIT, Anakena Solutions, DocBox

U Penn Ph.D. student Andrew King explains demo scenario to FDA engineer Paul Jones

## Standards & Regulatory Policy

PIs are members of the AAMI / UL 2800 standard committee tasked with writing a family of standards for safety/security of medical device interoperability

- Safety/security requirements of architectures for Medical Application Platforms (MAPs)
- Framework for compositional certifications of MAPs
- Guidelines for evaluating compliance to requirements

We are actively engaged with FDA engineers to develop science-based inputs for forming regulatory policy for interoperable medical systems

- Safety evaluation eco-system for medical device interoperability platforms
- Example hazard analyses, mock 510(k) regulatory submissions for apps and other MDCF components
- Guidelines for development of third-party certification regime

## Educational Material

The MDCF is open source and is designed to support a variety of interesting class projects and graduate research projects

- A collection of mock (software simulated) medical devices including blood pressure monitor, pulse oximeter, infusion pump, electrocardio-gram (ECG)
- A collection of example apps illustrating how to use the MDCF app development environment
- Illustrations of how to interface with real medical devices
- Suggested student projects
- Detailed requirements and development artifacts for Patient-Controlled Analgesic (PCA) Pump
- Lectures on safety-critical system development – requirements, hazard analysis, assurance cases, etc.

## Team


**Kansas State University**

John Hatcliff
Robby
Eugene Vasserman
Steve Warren
Venkatesh Ranganath

Yu Jin Kim
Brian Larson
Sam Procter
Kim Fowler

**University of Pennsylvania**

Insup Lee
Oleg Sokolsky
Andrew King

**Collaborators**

**Center for Integration of Medicine and Innovative Technology (CIMIT)**

Dr. Julian Goldman
David Arney, Jeff Plourde

**FDA & Underwriters Lab**

Paul L. Jones (FDA)
Sandy Weininger (FDA)
Anura Fernando (UL)