Medical CPS (MCPS) Architecture *

Insup Lee, University of Pennsylvania
John Hatcliff, Kansas State University

March 26, 2014
NSF CPS Reference Architectures Workshop

** In Collaboration with David Arney, Andrew King, Julian Goldman, Oleg Sokolsky*

Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

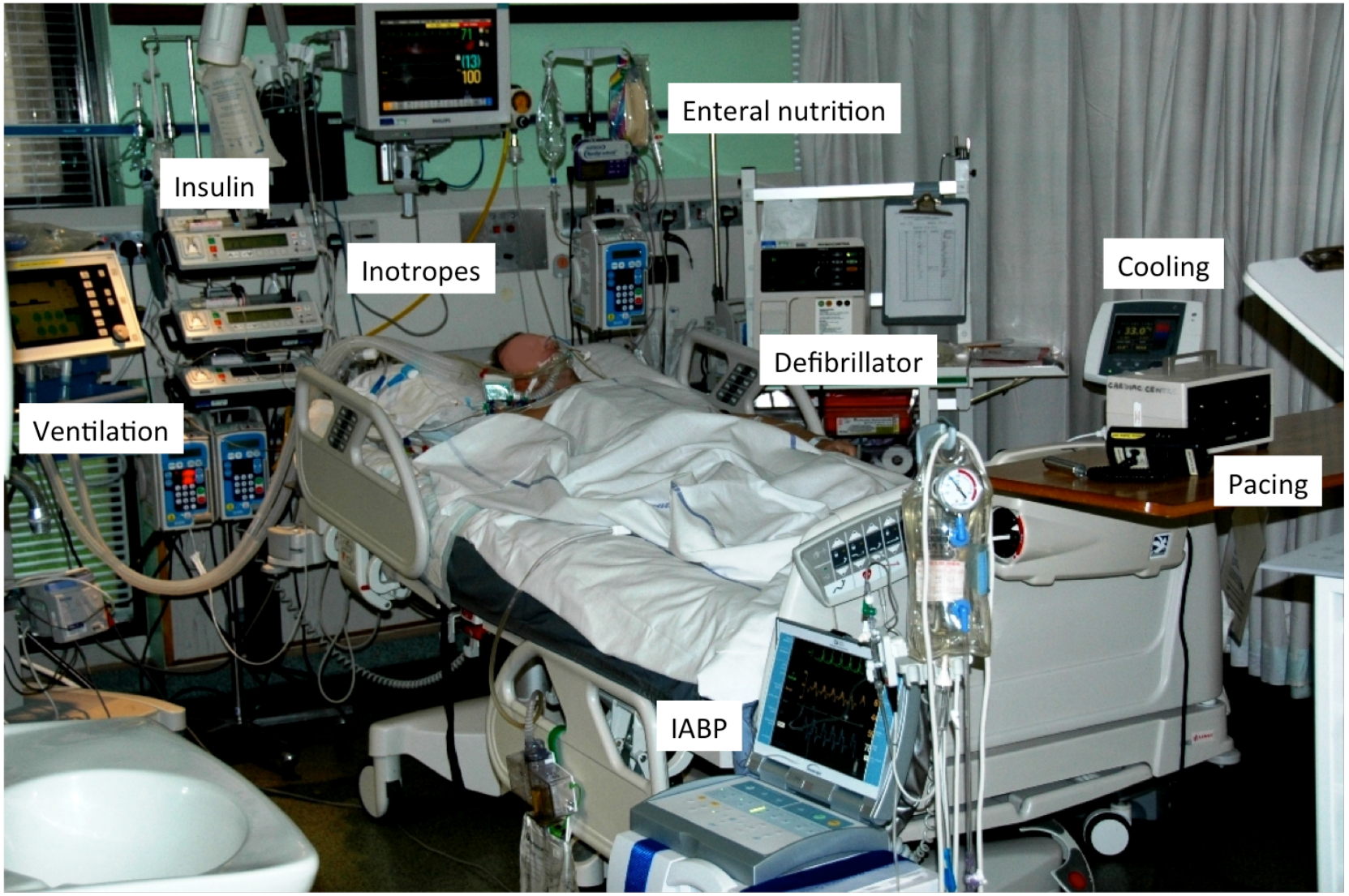
Outline

- MCPS Architecture
  - Characteristics
  - Needs
  - Requirements
- MCPS Architecture Components
  - MAP, Data Logger, Integrated Alarm Systems
- Challenges
- ICE Standard/Architecture

MCPS Domain Characteristics

- Safety & Security Critical
- Multi-Mission
  - Medical devices (sensors / actuators) used simultaneously for multiple therapies and purposes
- Dynamic / Open
  - Medical devices are added and removed based on current needs
- Multiple scales of integration
  - Single Patient: ICU room or OR
  - Populations: Ward to Floor to Hospital to whole Health System…
- Economics of medicine and health IT mean single vendor for all systems unlikely… major integration challenges

Example: ICU


Enteral nutrition
Insulin
Inotropes
Cooling
Defibrillator
Ventilation
Pacing
IABP

Current Problem

Little to no integration of Devices with each other:

- Humans must automate even simple clinical workflows
- Unnecessary burdens placed on human caregivers
- Few opportunities for “sensor fusion” (better alarms and diagnostics)

Medical Device Interoperability

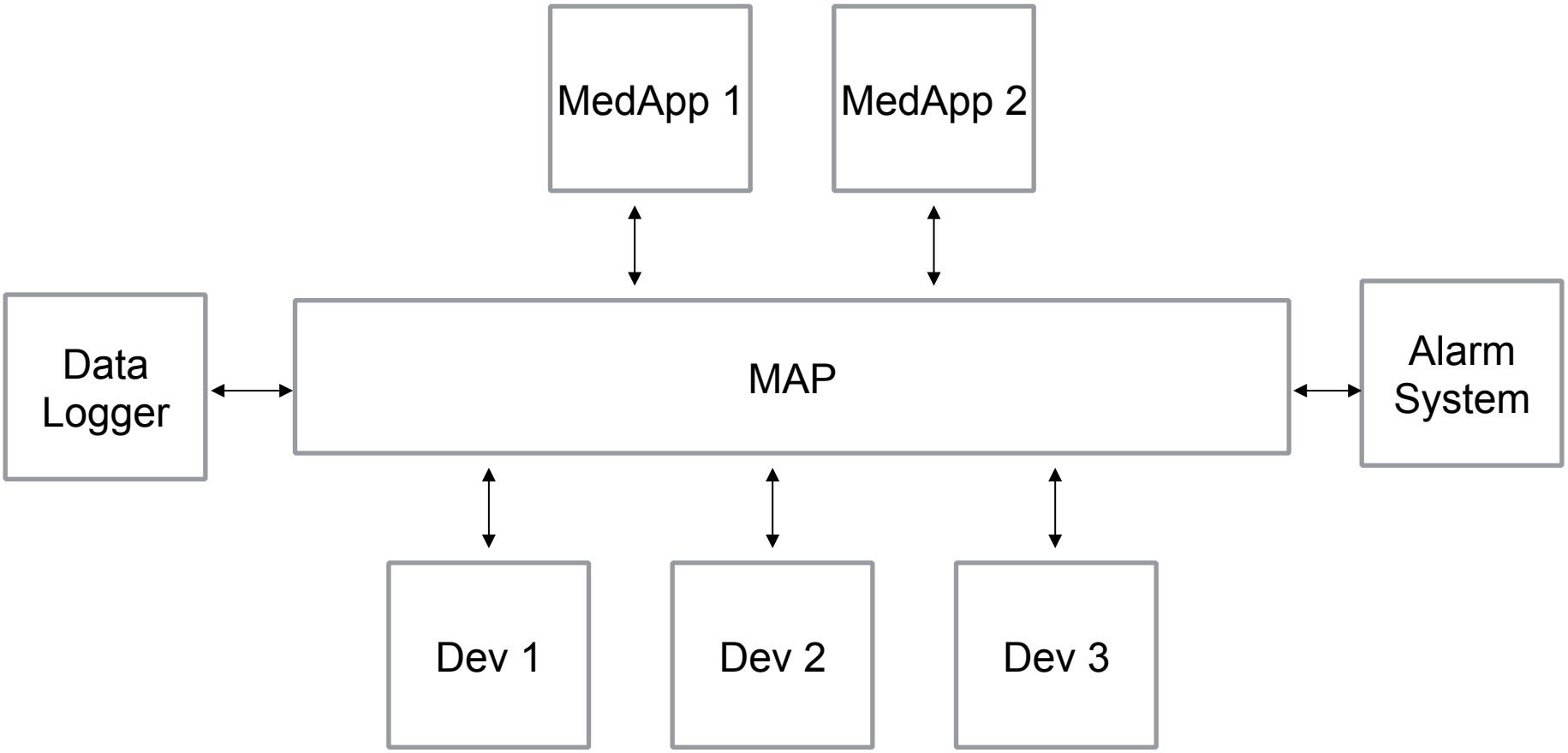
- A patient is treated using a variety of medical devices
  - Coordination between devices can increase safety or enhance functionality
  - Currently, caregivers coordinate devices

- Interoperable devices can self-coordinate
  - Provide continuous monitoring
  - Handle routine tasks and respond to obvious problems
  - Summon caregivers in more serious cases
  - Physiological closed-loop control in many cases

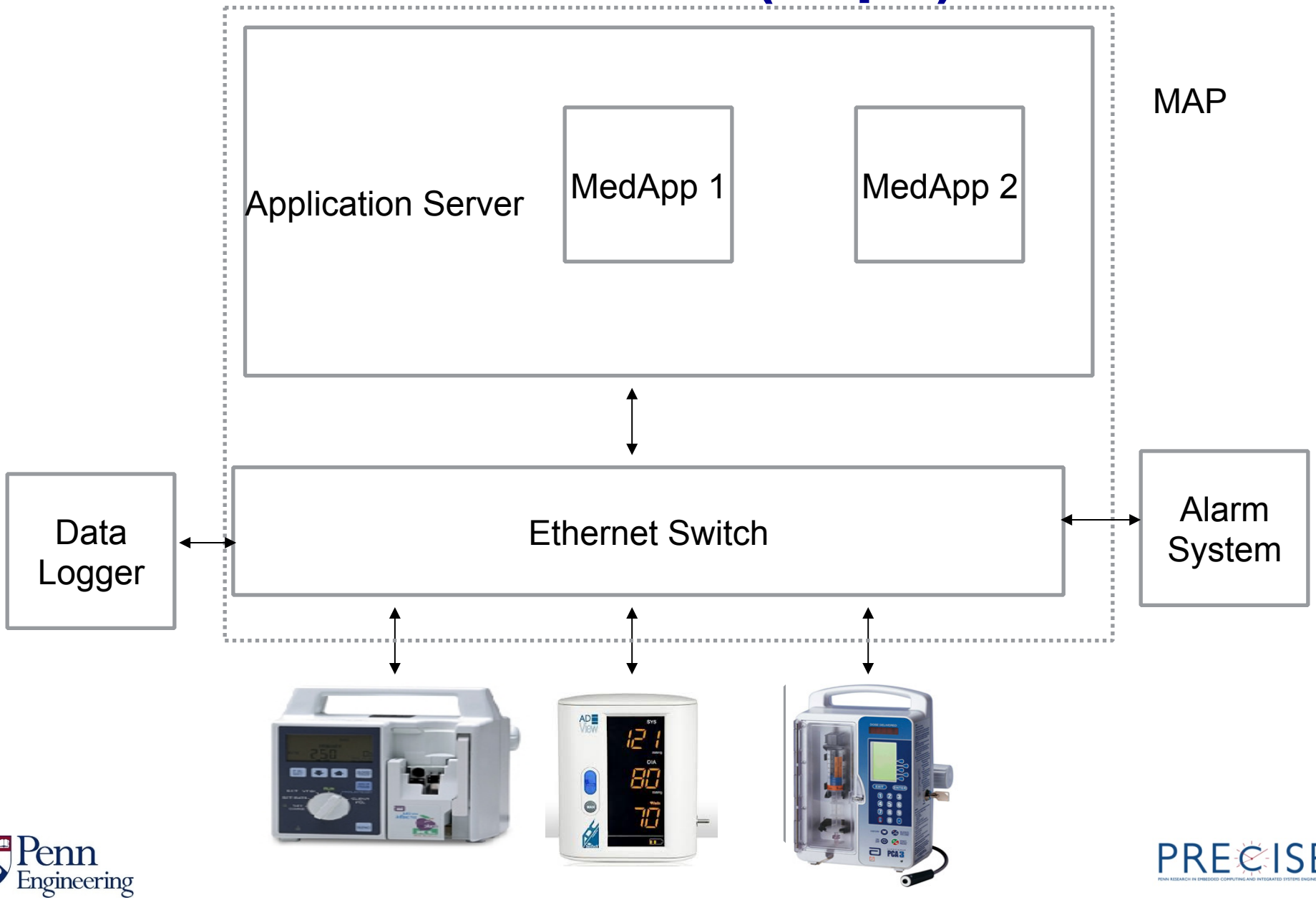
What we want

- Plug & Play Integration of Medical Systems
- Safety, security, and non-interference are emergent properties of Virtual Medical Device
- Challenges
  - How to control which emergent behaviors manifest in a Plug & Play system
    - Good behaviors lead to effectiveness
    - Bad behaviors lead to unsafe situations
- Architecture
  - The architecture should be designed to support safety arguments by providing mechanisms to control what emergent behaviors manifest...

Architecture (Logical)



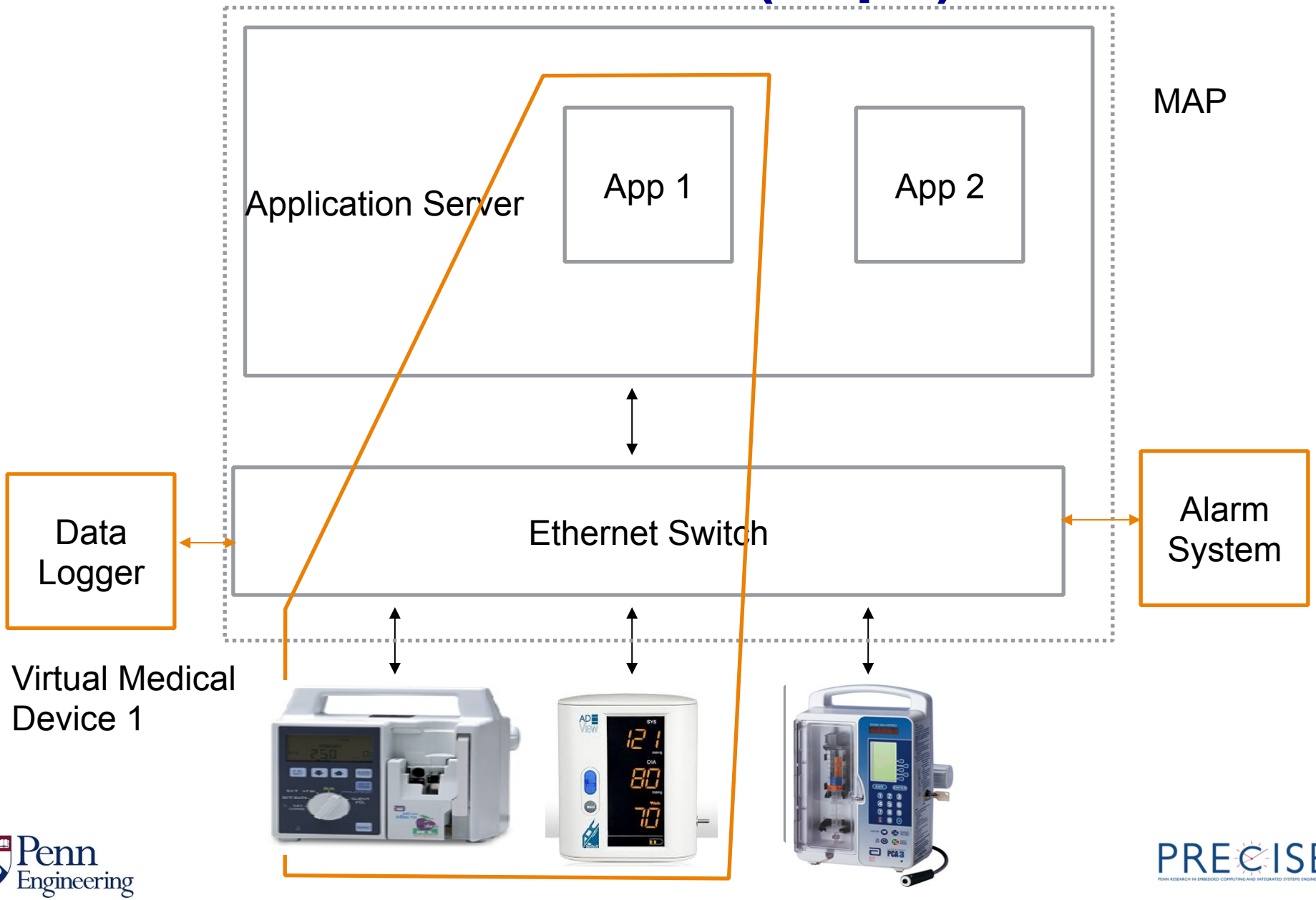
Architecture (Impl.)



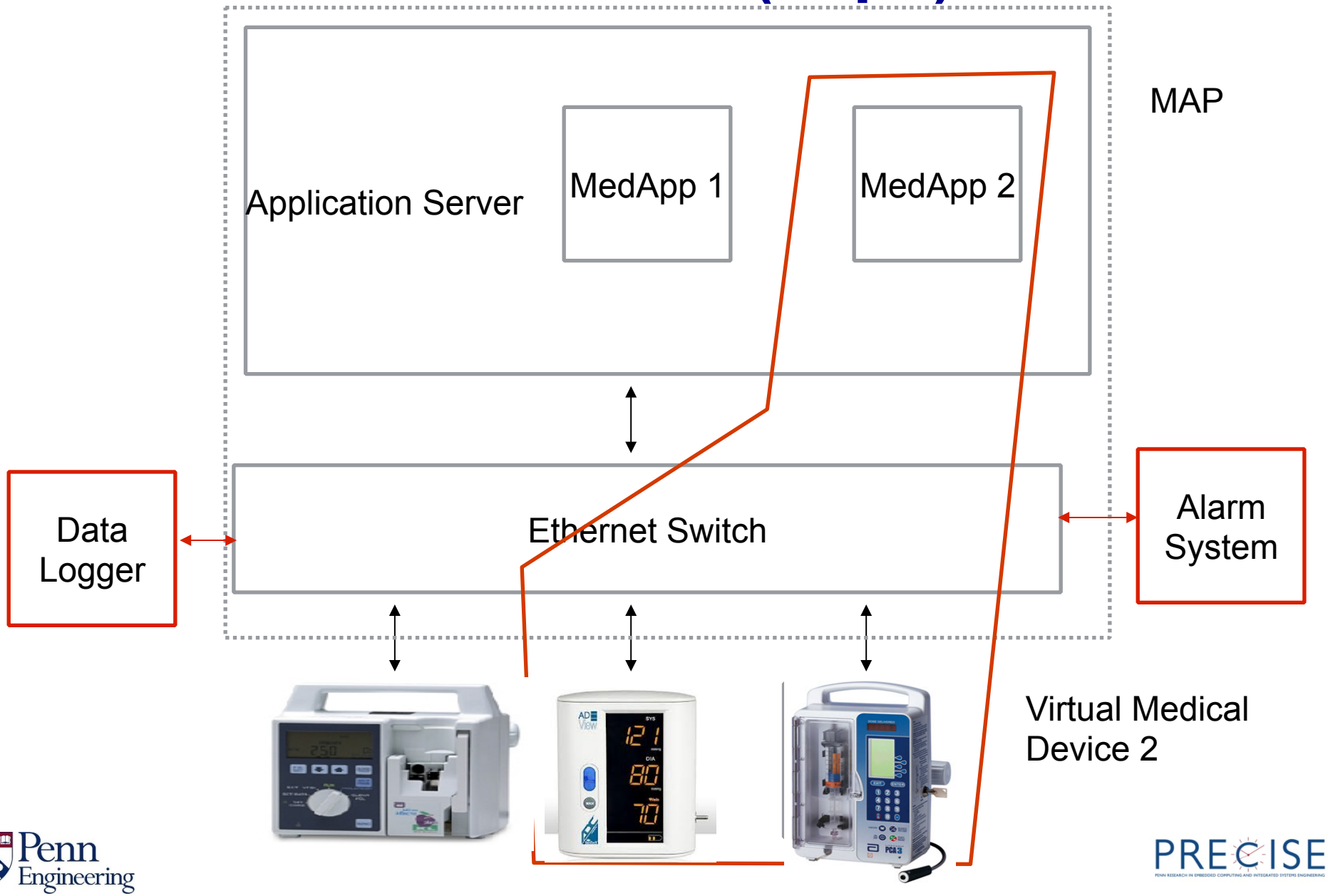
Penn Engineering

PRECISE

Architecture (Impl.)



Architecture (Impl.)



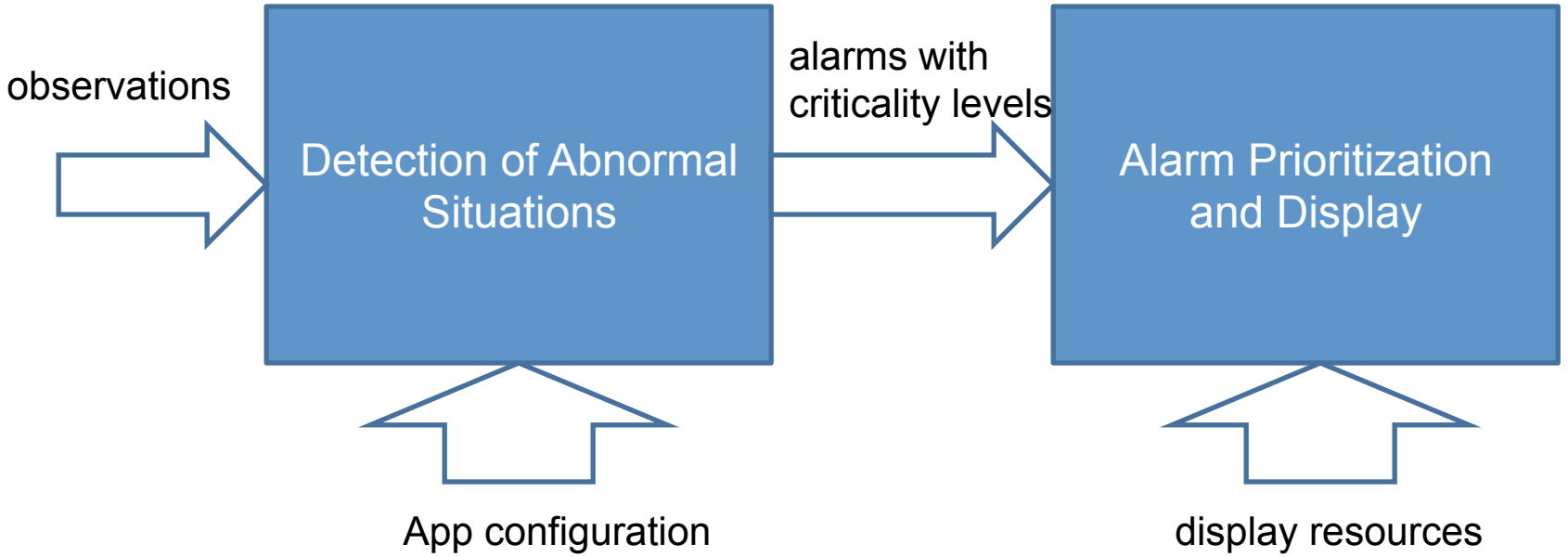
Medical Application Platform (MAP)

- Medical Device carries a capability/ behavioral specification
- Medical App contains clinical algorithms + requirements specifications on devices
- Apps are verified against intended uses and requirements specs
- MAP checks compatibility between specs and selected devices

See "Rationale and Architecture Principles for Medical Application Platforms", J. Hatcliff, A. King, I. Lee, …, J. Goldman, ICCPS '12

Integrated Alarm System (IAS)

- Goal: (Smart) Fail Loud
- Alarm criticality may depend on deployed apps
- Alarm priority depends on how alarms are presented to the user



* [Lee, Sokolksy, Sfyria, Venkatasubramanian, Yasserman, 2014]

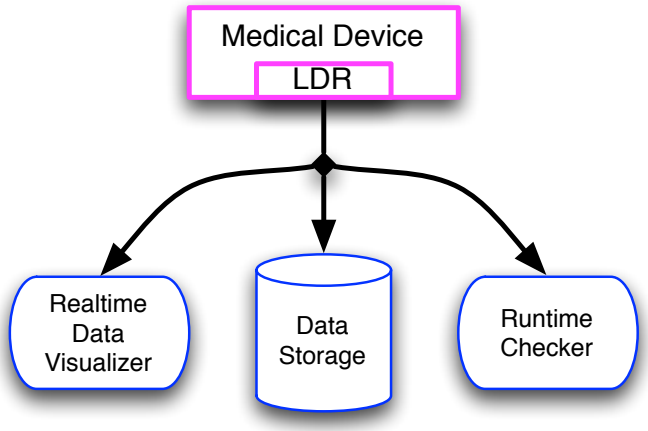
IAS Challenges

IAS alarm logic has to accommodate additional uncertainties

- It is not known at design time, what devices will be connected and what apps will be deployed
- Techniques for detecting abnormal situations may be different for different devices
- Criticality of alarms may depend on the clinical context

Data Logger/Blackbox

- Data-logging
  - forensic, failure prediction/runtime verification, regression testing for corrective actions & design evolution
- Data-logging standards
- Ownership and privacy issues
- Security/tamper resistant



- Trade-offs and Challenges
  - How/what to capture and analyze interactions between medical devices and between users and devices?
  - How to check if a system property is true?
  - Level of abstraction and granularity
    - Timing uncertainty
    - Space limitation
  - Interleaving information about events uncertain
  - Blame assignment

MCPS Architecture Requirements

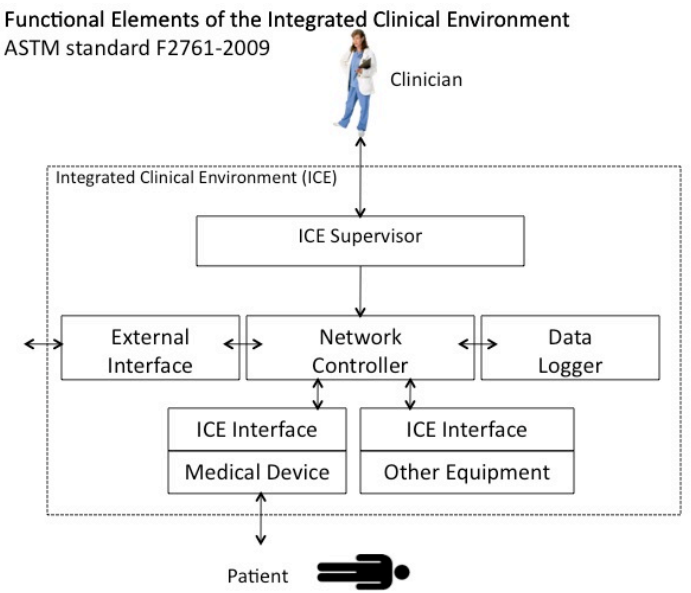
- Support Open/Dynamic systems
- Proactive compatibility checking between components
- Built-in monitoring / data logging
- Support / enforce security and data access policies
- Integrated alarm system for failures and security attacks
- Temporal / spatial guarantee and isolation for shared resources (CPU / Network)
- Support a range of component coupling protocols
- Support heterogeneous devices
  - Different models
  - Different vendors / manufacturers
  - Different functionality

MCPS Architecture Research Challenges

- How do we prove/argue that we preserve good behavior while excluding bad behavior?
  - What types of info in requirements/capabilities spec, i.e., interface?
  - What sort of isolation/guarantee mechanisms need to be in place?
  - Modeling and verification of safety, non-interference properties
- What do we do when something breaks?
- Incremental Certification

On-Demand Medical Systems

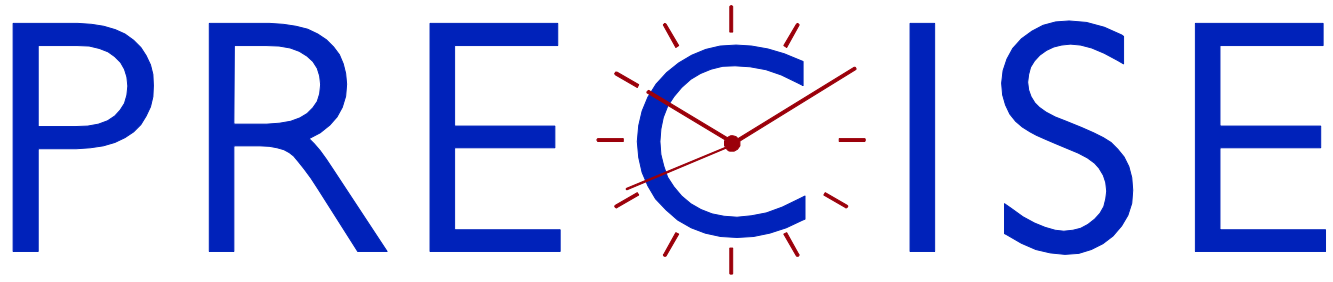
- The only way to realize the vision is to connect interoperable devices on demand
  - Clinical/medical "apps"
- Need open infrastructu support interoperability and app deployment
- Integrated clinical environment (ICE)



- Safety critical and requires high assurance

ICE Standard/Architecture

THANK YOU!



http://precise.seas.upenn.edu