Cyber Physical Systems: The Next Computing Revolution

Insup Lee
PRECISE Center
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania
www.cis.upenn.edu/~lee/

Adream, LAAS-CNRS
June 15, 2010

Computing Revolution History

- Mainframe computing (60’s-70’s)
  - Large computers to execute big data processing applications
- Desktop computing & Internet (80’s-90’s)
  - One computer at every desk to do business/personal activities
- Ubiquitous computing (00’s)
  - Numerous computing devices in every place/person
  - “Invisible” part of the environment
  - Millions for desktops and billions for embedded processors

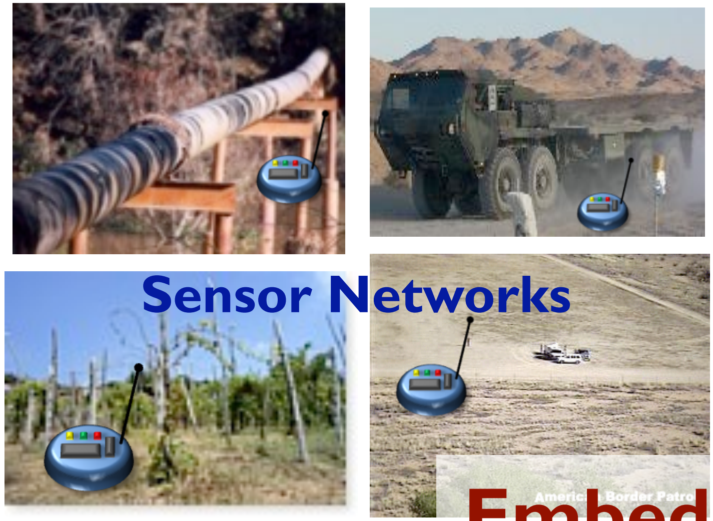
The Next Computing Revolution…

Cyber Physical Systems

driven by …

Trend 1: Data/Device Proliferation (By Moore's Law)

Unattended multihop adhoc wireless



Sensor Networks

Medical Devices

Embedded Everywhere!

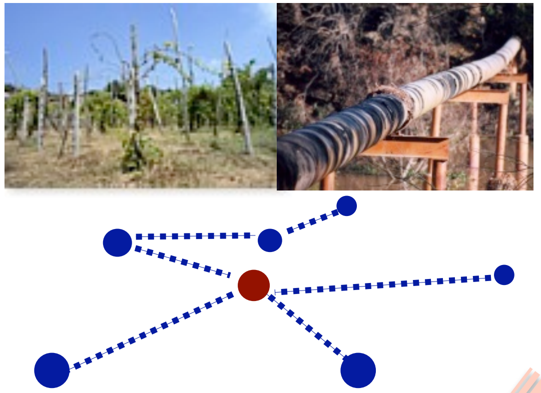
Industrials

Cargo, machinery, factory floor

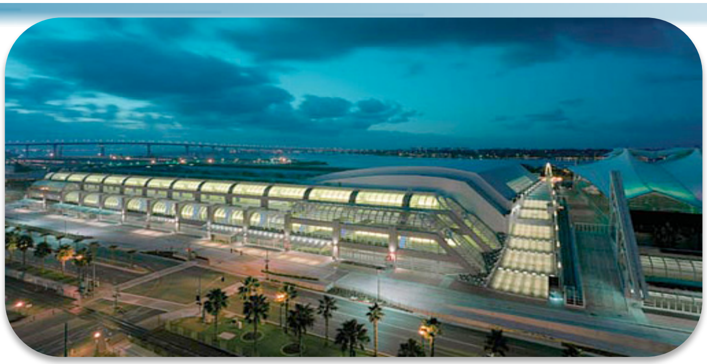
Smart Space

Smart space
Assisted living

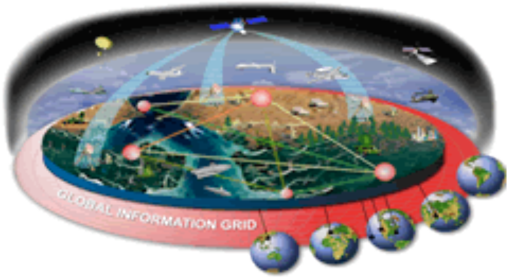
Trend 2: Integration at Scale (Isolation has cost!)



World Wide Sensor Web



Smart Building Environment



Future Combat System

Low End

Integration & Scaling Challenges

High End

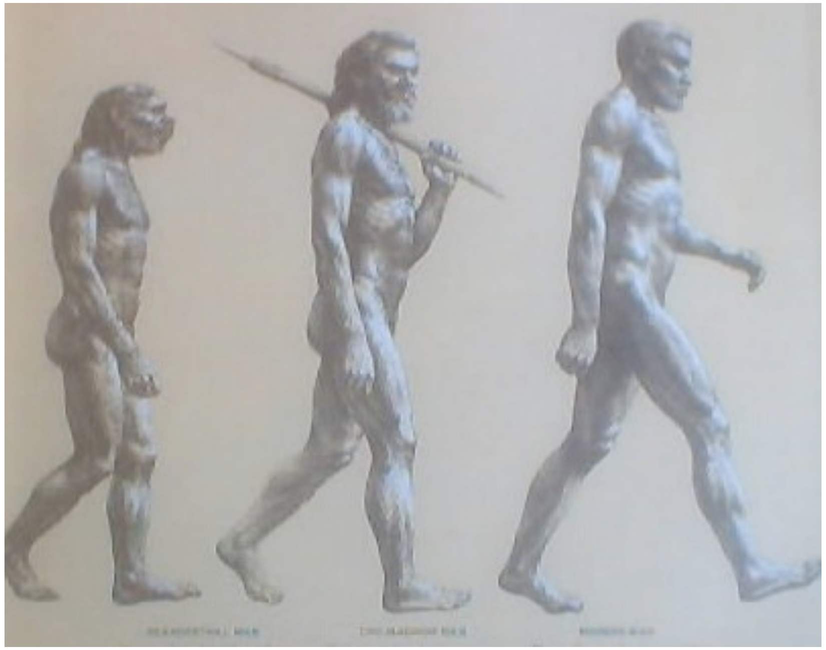
Ubiquitous embedded devices

- Large-scale networked embedded systems
- Seamless integration with a physical environment

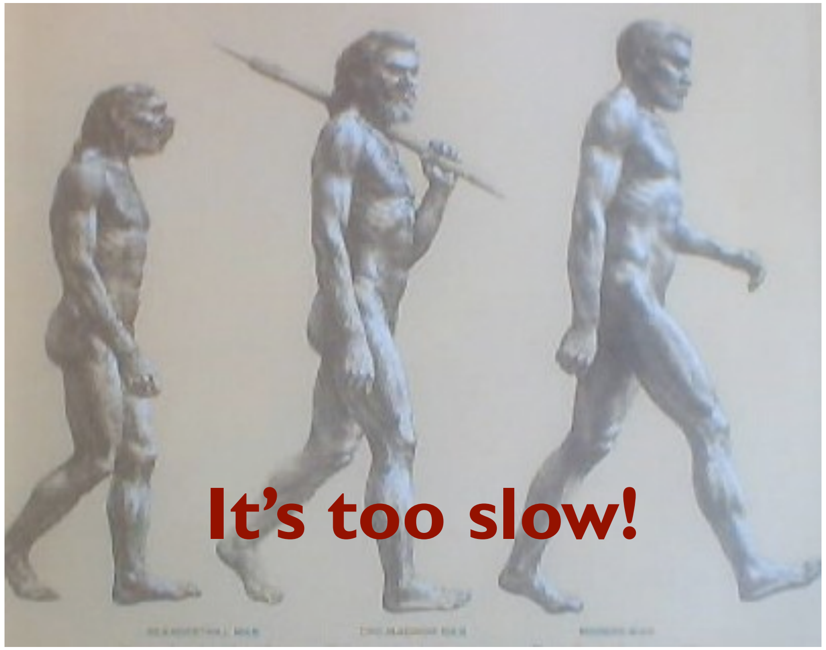
Complex systems with global integration

- Global Information Grid
- Smart Building Environment

Trend 3: Biological Evolution



Trend 3: Biological Evolution



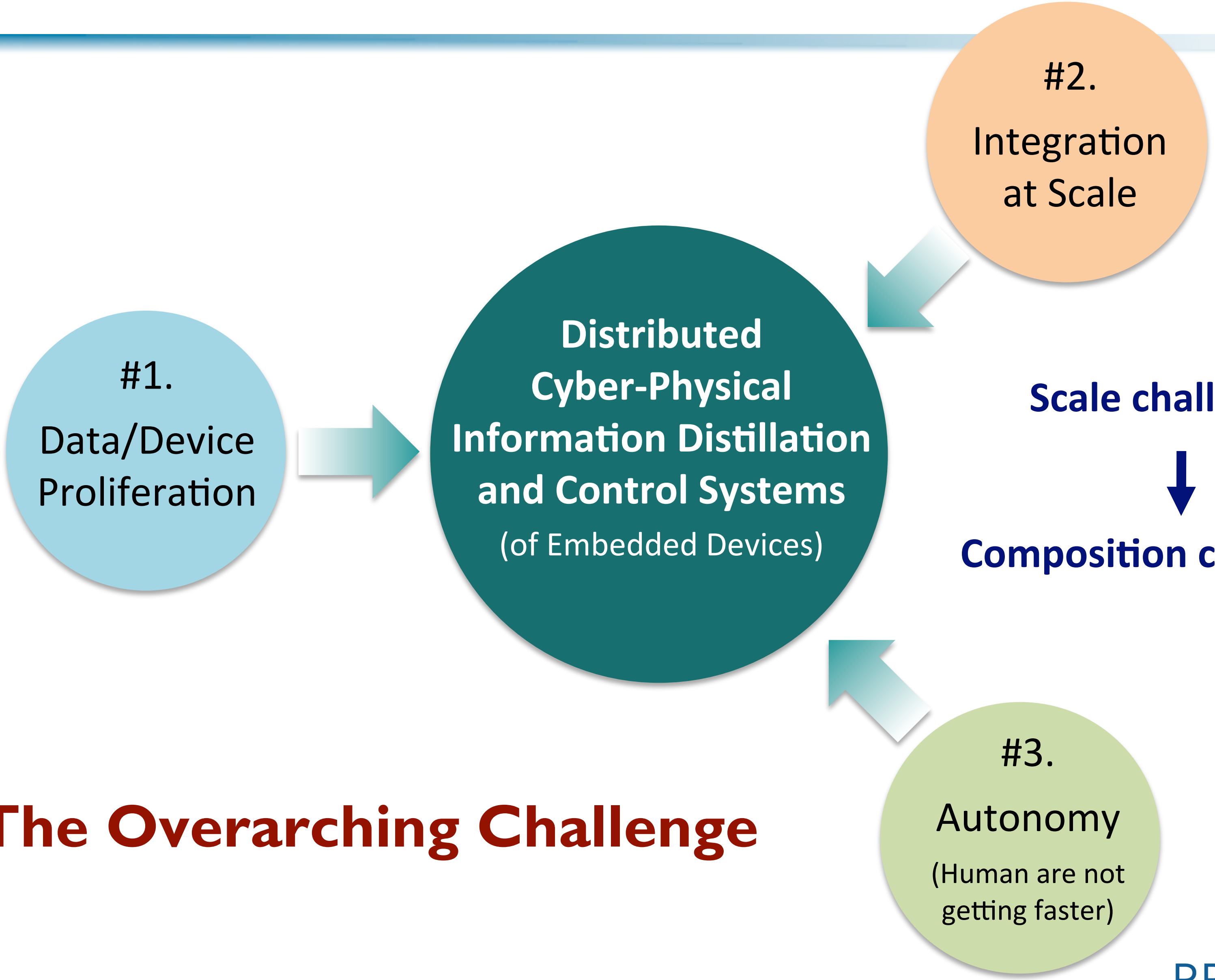
It’s too slow!

The exponential proliferation of embedded devices (afforded by Moore’s Law) is *not* matched by a corresponding increase in human ability to consume information!

↓

Increasing autonomy (human out of the loop), direct world access

Confluence of Trends



#1.

Data/Device Proliferation

#2.

Integration at Scale

#3.

Autonomy

(Human are not getting faster)

Distributed Cyber-Physical Information Distillation and Control Systems

(of Embedded Devices)

Scale challenges

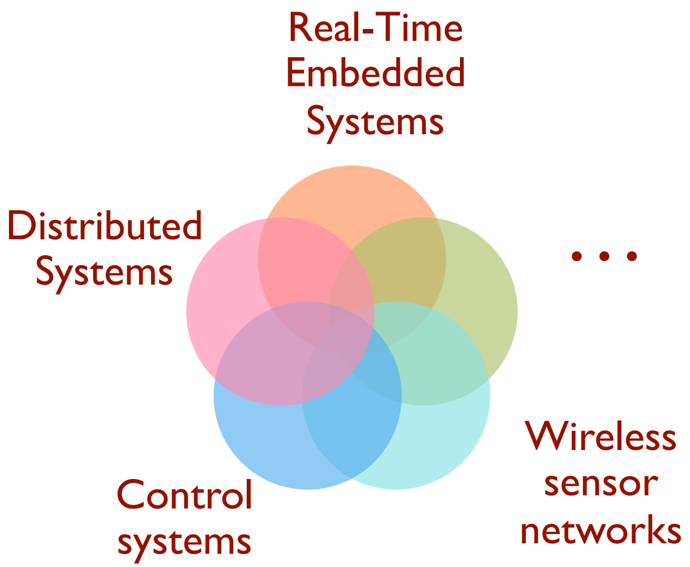
↓

Composition challenges

The Overarching Challenge

What are Cyber-Physical Systems (CPS)?

- Physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core.
- Tight conjoining of and coordination between computational and physical resources.
- Exceeds today's systems in adaptability, autonomy, efficiency, functionality, reliability, safety, and usability
- Convergence of computation, communication, information, and control

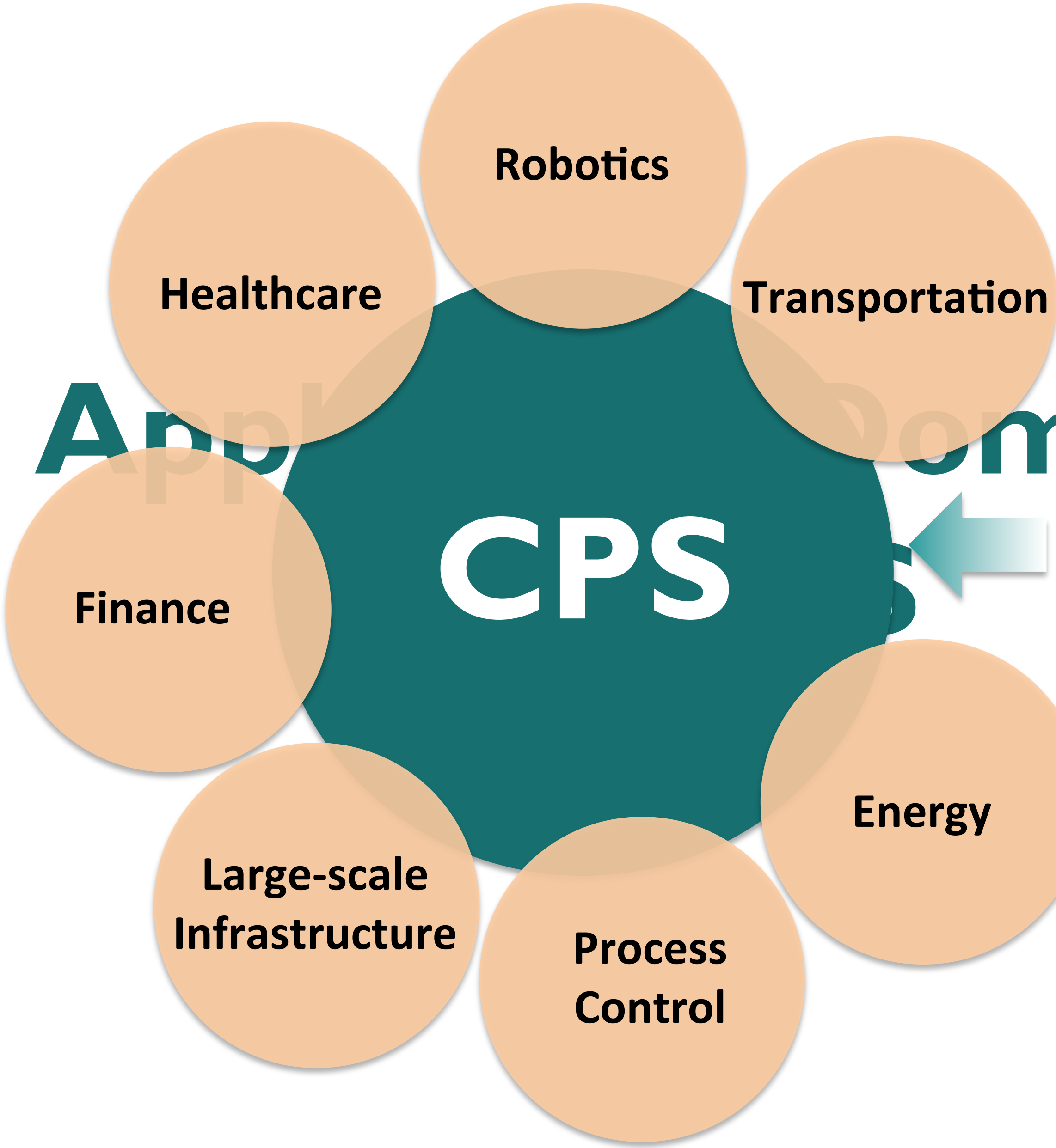


Characteristics of CPS

- Cyber – physical coupling driven by new demands and applications
  - Cyber capability in every physical component
  - Large scale wired and wireless networking
  - Networked at multiple and extreme scales
- Systems of systems
  - New spatial-temporal constraints
  - Complex at multiple temporal and spatial scales
  - Dynamically reorganizing/reconfiguring
  - Unconventional computational and physical substrates (Bio? Nano?)
- Novel interactions between communications/computing/control
  - High degrees of automation, control loops must close at all scales
  - Large numbers of non-technical savvy users in the control loop

Characteristics of CPS

- Ubiquity drives unprecedented security and privacy needs
- Operation must be dependable, certified in some cases
- Tipping points/phase transitions
  - Not desktop computing
  - Not traditional, post-hoc embedded/real-time systems
  - Not today’s sensor nets
  - Internet as we know now, stampede in a moving crowd, …



X by wire(less)

X = anything physical in nature

Ex1. Automotive Telematics

- 30-90 processors per car
  - o Engine control, Break system, Airbag deployment system
  - o Windshield wiper, door locks, entertainment systems

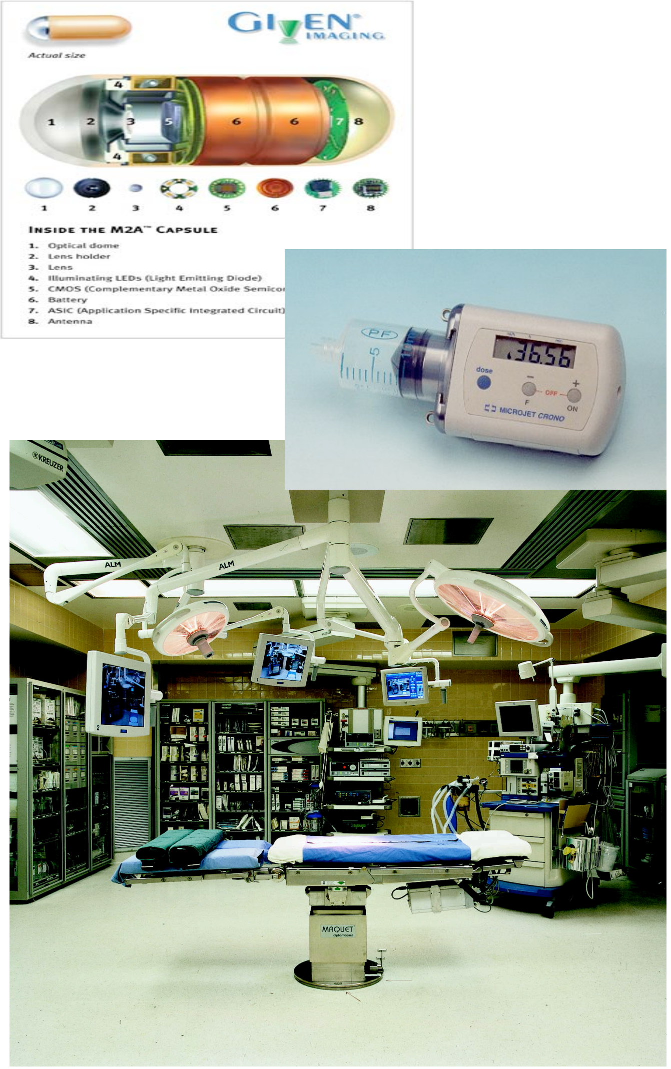
BMW 745i:

2,000,000 LOC,
Window CE OS
Over 60 microprocessors
53 8-bit, 11 32-bit, 7 16-bit
Multiple networks

- Cars are sensors and actuators in V2V networks
  - o Active networked safety alerts
  - o Autonomous navigation

Ex2. Health Care and Medicine

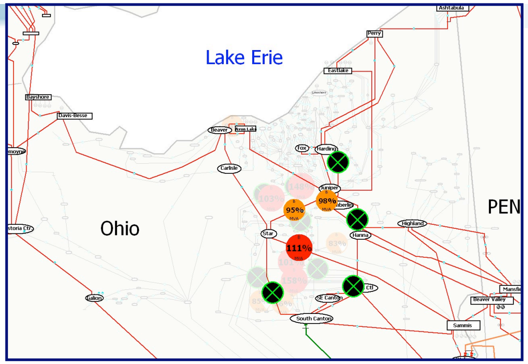
- National Health Information Network, Electronic Patient Record initiative
  - Medical records at any point of service
  - Hospital, OR, ICU, …, EMT?
- Home care: monitoring and control
  - Pulse oximeters (oxygen saturation), blood glucose monitors, infusion pumps (insulin), accelerometers (falling, immobility), wearable networks (gait analysis), …
- Operating Room of the Future
  - Closed loop monitoring and control; multiple treatment stations, plug and play devices; robotic microsurgery (remotely guided?)
  - System coordination challenge
- Progress in bioinformatics:
  - gene, protein expression; systems biology; disease dynamics, control mechanisms
  - Personalized medicine

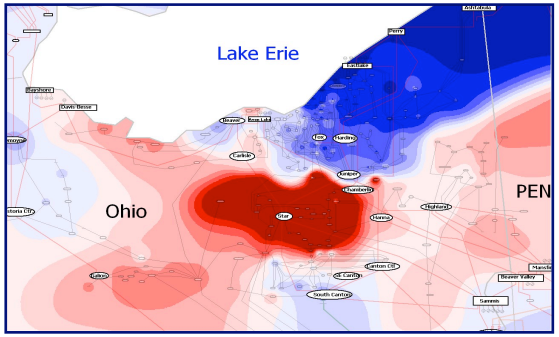


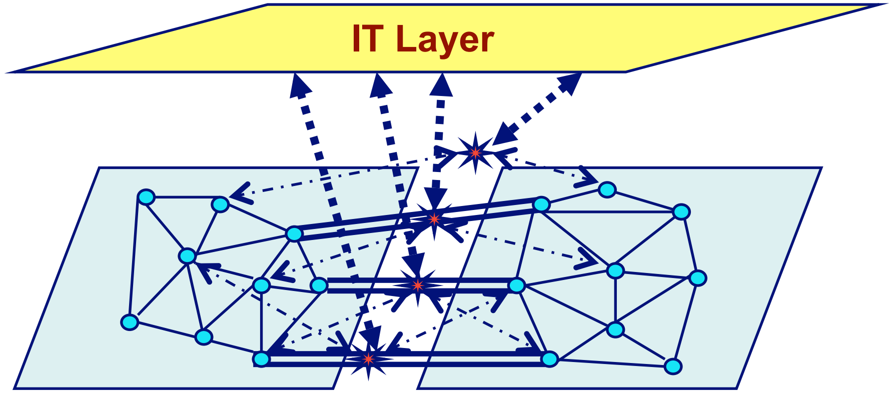
Ex3. Electric Power Grid

- **Current picture**
  - Equipment protection devices trip locally, reactively
  - Cascading failures: E.g., Aug (US /Canada) and Oct (Europe), 2003

- **Better future?**
  - Real-time cooperative control of protection devices
  - Or -- self-healing -- (re-)aggregate islands of stable bulk power (protection, market motives)
  - Ubiquitous green technologies
  - Issue: standard operational control concerns exhibit wide-area characteristics (bulk power stability and quality, flow control, fault isolation)
  - Technology vectors: FACTS, PMUs
  - Context: market (timing?) behavior, power routing transactions, regulation

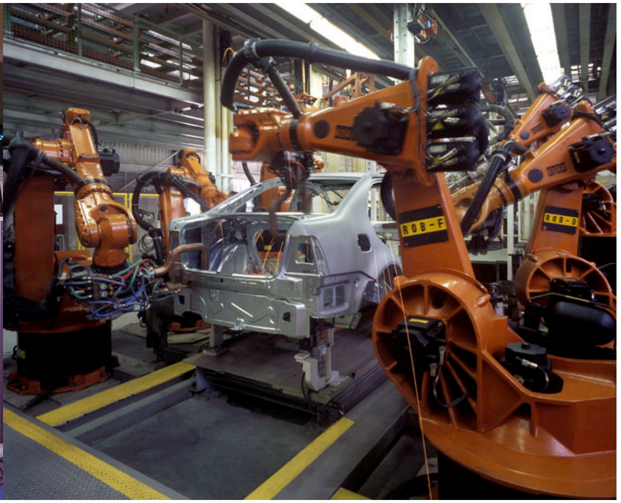






Ex4. Robotics

Robotic Surgery



Factory Automation

Military Robot Vehicles

- Manufacturing and Logistics Robotics
- Medical and Healthcare Robotics
- Service Robotics
- A Roadmap for US Robotics from Internet to Robotics, CCC CRA, May 2009

CPS Everywhere

- Expectations
  - 24/7 availability, 100% reliability, 100% connectivity, instantaneous response, remember everything forever
- Classes
  - Young to old, able and disabled, rich and poor, literate and illiterate
- Numbers
  - Individuals, special groups, social networks, cultures, populations

Societal Responsibility/Challenge

How can we provide people and society with CPS that they can trust their lives on ?

Trustworthy:
reliable, safe, secure,
privacy-preserving,
usable, etc.

- **Partial list of complex system failures**
  - Denver baggage handling system ($300M)
  - Power blackout in NY (2003)
  - Ariane 5 (1996)
  - Mars Pathfinder (1997)
  - Mars Climate Orbiter ($125M,1999)
  - The Patriot Missile (1991)
  - USS Yorktown (1998)
  - Therac-25 (1985-1988)
  - London Ambulance System (£9M, 1992)
  - Pacemakers (500K recalls during 1990-2000)
  - Numerous computer-related incidents with commercial aircrafts (*http://www.rvs.uni-bielefeld.de/publications/compendium/incidents_and_accidents/index.html*)

R&D Needs for High-Confidence CPS

- **Engineering design techniques and tools**
  - Modeling and analysis, requirements capture, hybrid systems, testing
  - Capture and optimization of inter-dependencies of different requirements
  - Domain-specific model-based tools
- **Systems Software and Network Supports**
  - Virtualization, RTOS, Middleware, …
  - Predictable (not best-effort) communication with QoS, predictable delay & jitter bounds, …
  - Trusted embedded software components
    - To help structured system design and system development
    - To reduce the cost of overall system development and maintenance efforts
    - To support the reuse of components within product families
- **Validation and Certification**
  - Metrics for certification/validation
  - Evidence-based certification, Incremental certification

Scientific Challenges

- **Computations and Abstractions**
  - Computational abstractions
  - Novel real-time embedded systems abstractions for CPS
  - Model-based development of CPS
- **Compositionality**
  - Composition and interoperation of cyber physical systems
  - Compositional frameworks for both functional, temporal, and non-functional properties
  - Robustness, safety, and security of cyber physical systems
- **Systems & Network Supports**
  - CPS Architecture, virtualization
  - Wireless and smart sensor networks
  - Predictable real-time and QoS guarantees at multiple scales

Scientific Challenges

- Computations and Abstractions
- Compositionality
- Systems & Network Supports
- **New foundations**
  - Control (distributed, multi-level in space and time) and hybrid systems - cognition of environment and system state, and closing the loop
  - Dealing with uncertainties and adaptability - graceful adaptation to applications, environments, and resource availability
  - Scalability, reliability, robustness, stability of system of systems
  - Science of certification - evidence-based certification, measures of verification, validation, and testing

Application domain dependent!

Penn Engineering

High Confidence Medical Device Software Systems (HCMDSS)

Challenges & Opportunities

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

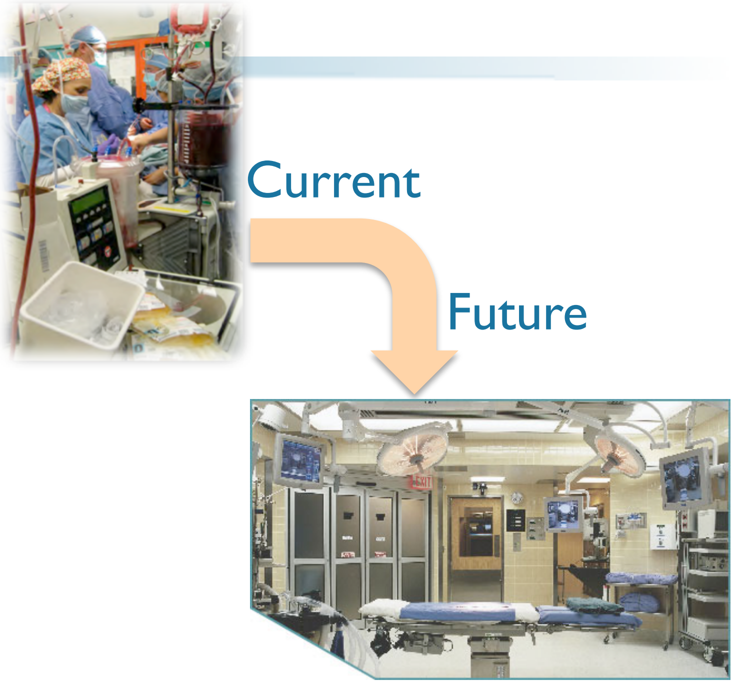
Needs for Healthcare Systems

- Integration techniques for systems of systems
  - Interoperation of medical devices, EHR systems, ...
  - High-confidence systems
- Secure, dependable, real-time communication networks with GoS (Guarantee of Service)
  - Internet service
  - Interference-resilient wireless networks
- Validation and evidence-based certification

Interoperability

Characteristics

- Over the years medical devices gaining communication capabilities
- Devices still operate independently
- Standardized interaction between devices non existent
- Full benefit of communication capabilities not being realize



MDPnP:

Interoperable medical devices based on plug-n-play!

Vender neutrality based on virtualization (virtual medical device interfaces)

Advantages

- Improve Patient safety
- Complete, accurate medical records
- Reduce errors
- Context awareness
- Rapid deployment
- Safety interlocks

MDPnP Use Case: X-Ray / Ventilator

"With the advent of sophisticated anesthesia machines incorporating comprehensive monitoring, it is easy to forget that serious anesthesia mishaps still can and do occur."
APSF Newsletter Winter 2005

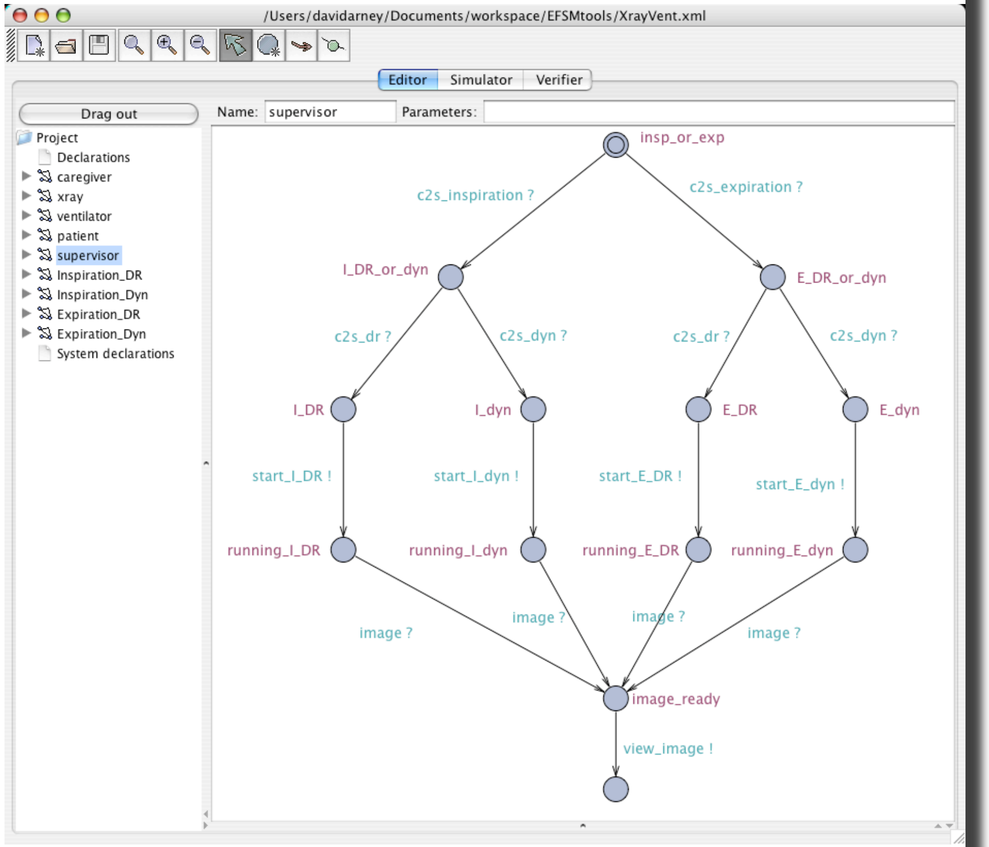
Anesthesia Machine

Portable x-ray machine

Surgeons

Modeling MD PnP Systems: Xray/Vent

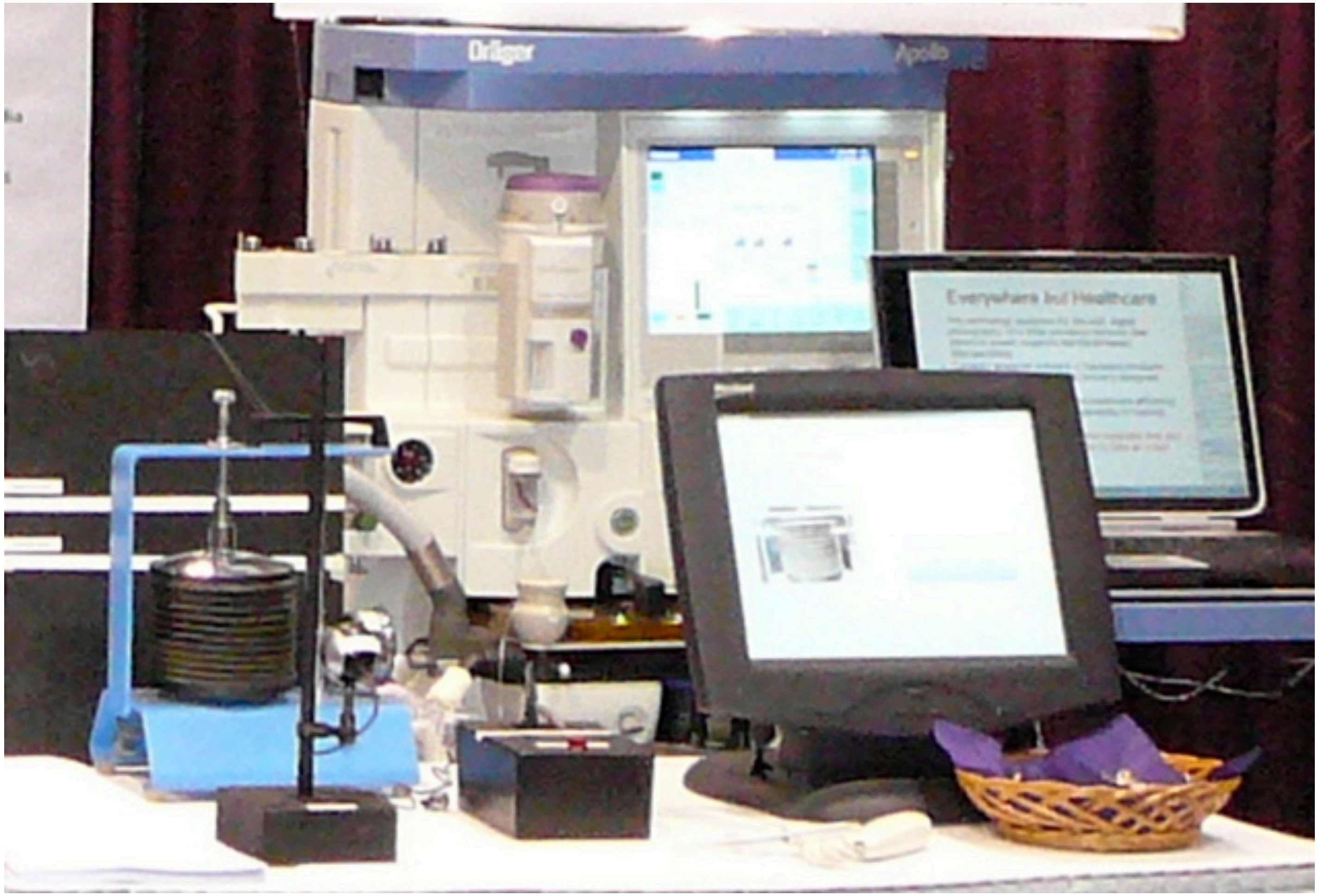
- Model of system components and interactions
- Model includes:
  - Xray
  - Ventilator
  - Supervisor
  - Caregiver
  - Patient
- Verification:
  - Correctness of inspiration dynamic algorithm
  - Feasibility of interoperation



/Users/davidarney/Documents/workspace/EFSMtools/XrayVent.xml

Name: supervisor Parameters:

X-Ray / Ventilator Demo Implementation



Interaction Complexity

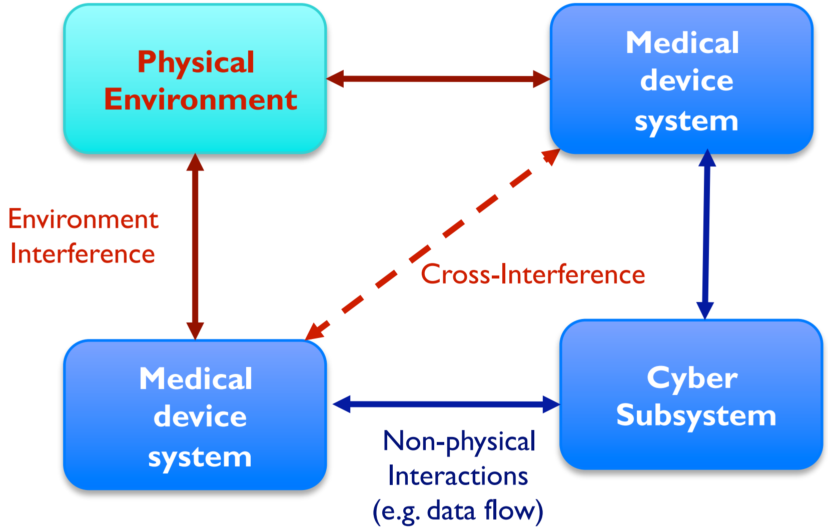
- Healthcare systems are systems of systems
- Composition of systems are about the interactions of systems
- "Normal Accidents", an influential book by Charles Perrow (1984)
  - One of the Three Mile Island investigators
  - A member of recent NRC Study "*Software for Dependable Systems: Sufficient Evidence*?"
- Posits that sufficiently complex systems can produce accidents without a simple cause due to
  - **interactive complexity** and **tight coupling**

Interference Due to Coupling

- MD systems have implanted or worn sensors/devices on the human body

- Interference
  - Explicit resource sharing /synchronization
  - Implicit coupling via shared environment

- Needs:
  - Mixed criticality
  - Mode changes
  - Environment model (e.g., patient model)



Need formal interference analysis methods for medical devices systems

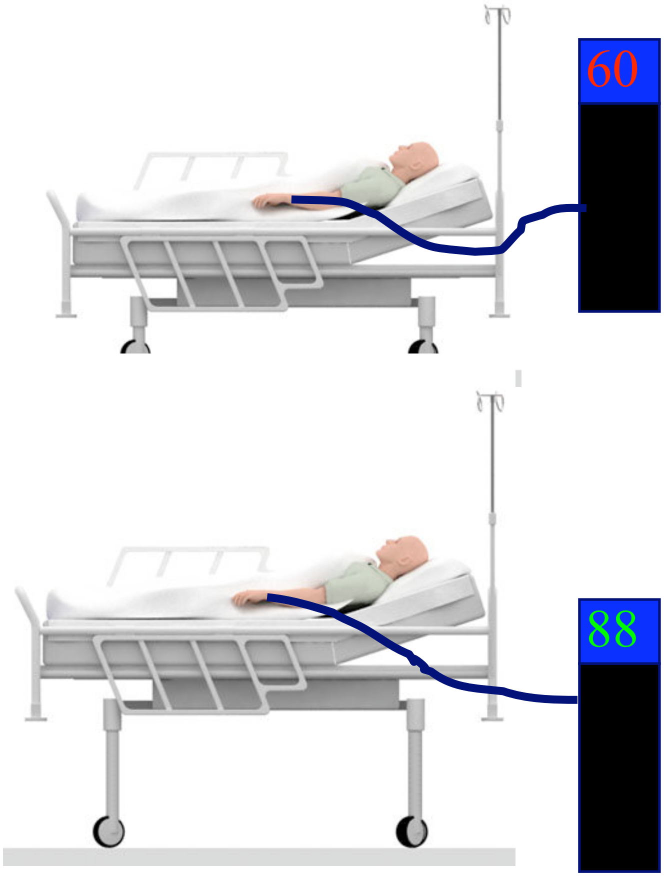
Interference Example: Bed and MAP

A patient's Mean Arterial Pressure (MAP) is measured using a transducer attached to a line in their radial artery. The transducer is mounted next to the patient's bed.

When the bed is raised, the MAP reading increases because the patient is higher than the sensor. The opposite happens when the bed is lowered.

This can mask a problem by making the pressure look OK when it's low, or cause false positive alarms.

UNH page on MD PnP project:
http://www.ece.unh.edu/biolab/hof/



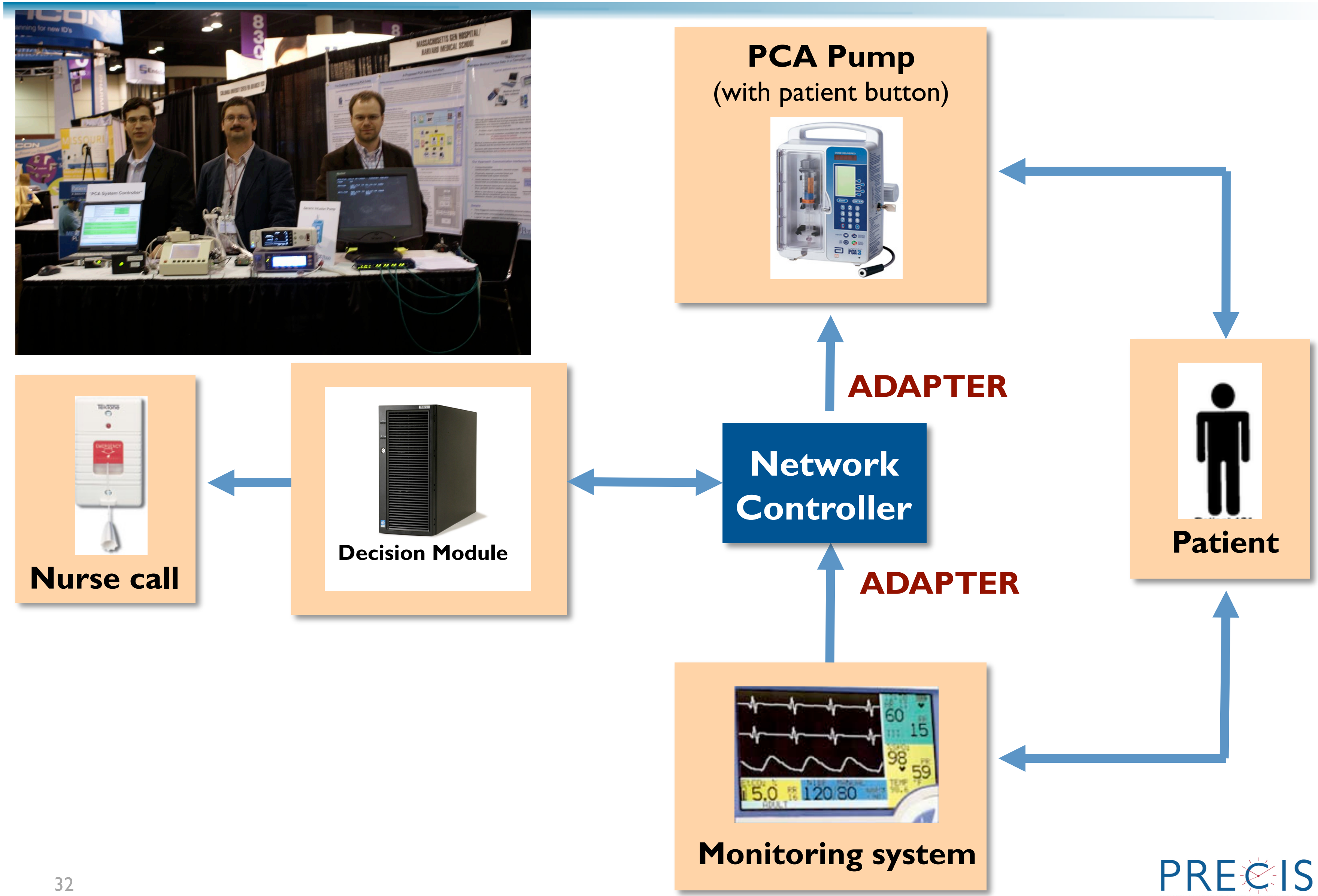
PCA Monitoring: Closing the Loop

- PCA (Patient Controlled Analgesia) infusion pumps are used to administer pain medications such as Morphine to conscious patients after surgery

- Can we use pulse oximeters and capnometers already in the hospital to monitor PCA opioids?

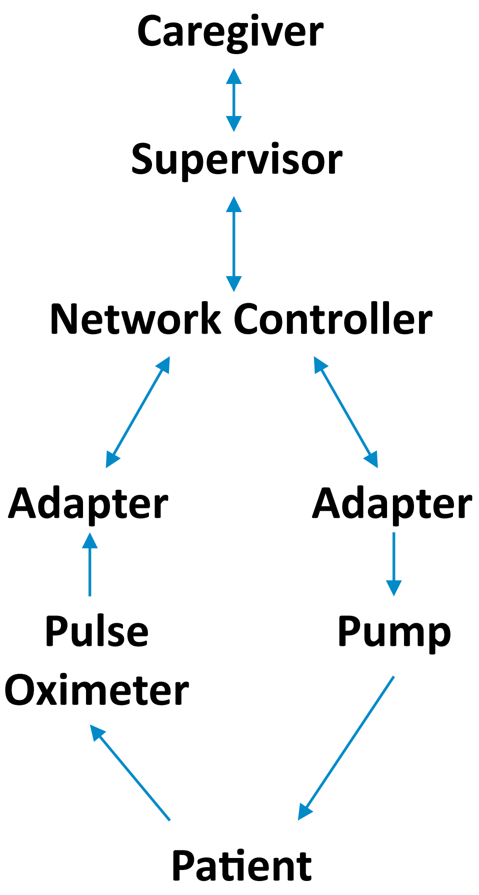
- Goal: Integrate monitors with an intelligent "controller" to:
  - Detect respiratory disturbance
  - Safety lock on over infusion
  - Activate nurse-call

PCA Monitoring System



Virtual Medical Device Scenarios

All Physical Devices



Caregiver

Supervisor

Network Controller

Adapter

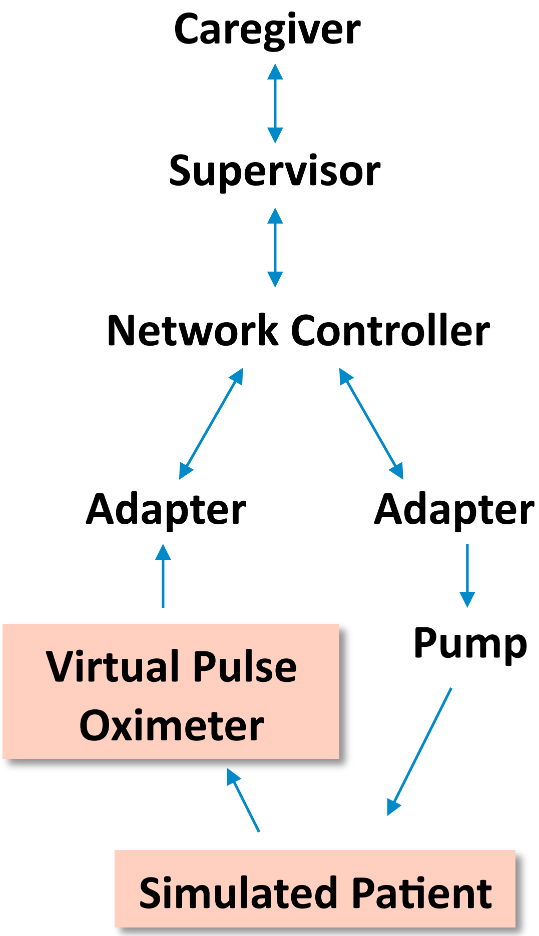
Adapter

Pulse Oximeter

Pump

Patient

Mixed Physical and Virtual



Caregiver

Supervisor

Network Controller

Adapter

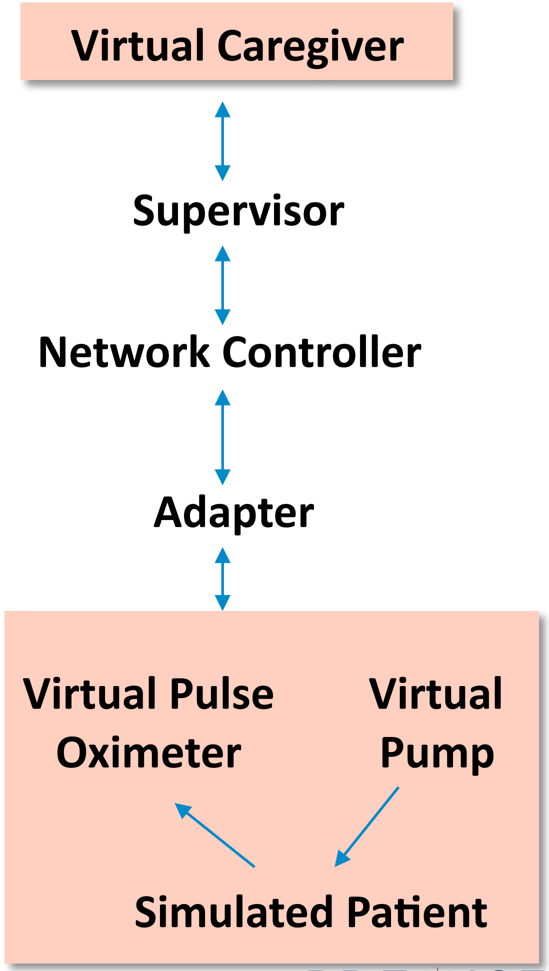
Adapter

Virtual Pulse Oximeter

Pump

Simulated Patient

All Virtual Devices



Virtual Caregiver

Supervisor

Network Controller

Adapter

Virtual Pulse Oximeter

Virtual Pump

Simulated Patient

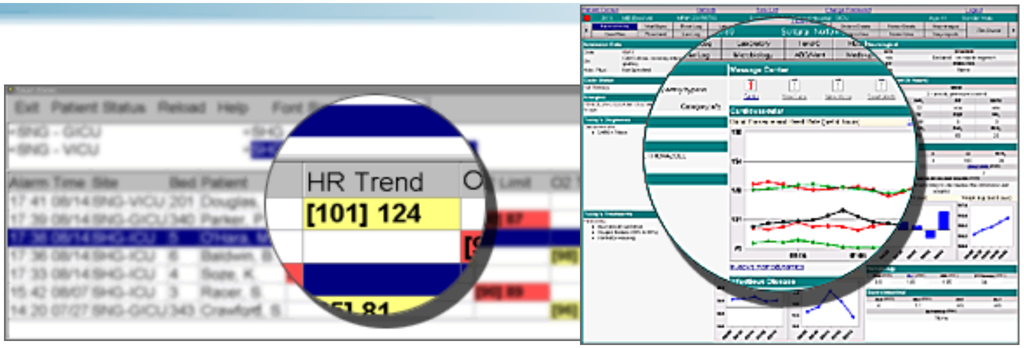
Centralized Monitoring: System of Systems

Applications

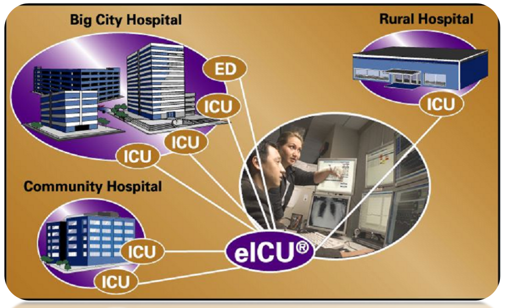
- Hospital based monitoring
- Secondary monitoring infrastructure

Features

- Patient Care Tools*
  - Patient Profile
  - Treatment Plan
  - Event Log
  - Physician note-writing capability
- Remote Health Management Tools*
  - Video-assessment
  - Remote Bedside Monitoring
  - Smart Alarms



Penn E-lert eICU®

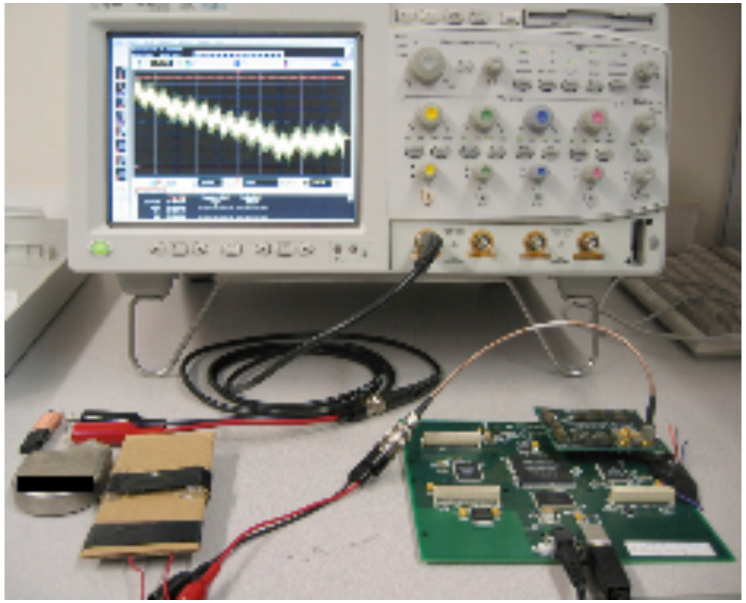


*Alerts**

- *Types*
  - *Patient Status Alerts*
  - *Care Issue Alerts*
  - *Process Reminder Alerts*
  - *Daily Management Reports*
- *Patient Parameters monitored*
  - *Heart rate (value, trend)*
  - *Mean Arterial Pressure (value, trend)*
  - *Inter-beat Interval (EKG)*
  - *O2 Saturation*

* Source:Visicu Inc.'s eICU system (http://www.visicu.com/products/index.html)

Pacemaker Hacking Example



Researchers working with an implantable cardiac defibrillator were able to remotely read telemetry data and reprogram the device.

These devices currently have no safeguards beyond an unpublished, proprietary interface.

Besides the obvious physical hazards, there are also privacy implications.

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

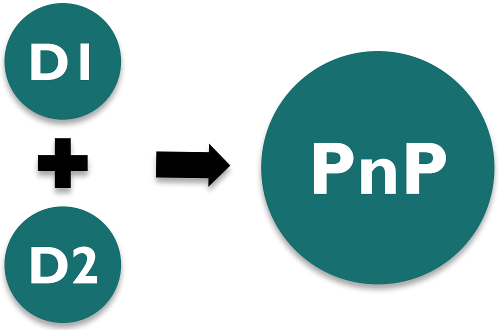
Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel
IEEE Symposium on Security and Privacy, May 2008

- "To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark, said.
- St. Jude Medical, the third major defibrillator company, said it used "proprietary techniques" to protect the security of its implants and had not heard of any unauthorized or illegal manipulation of them.

http://www.nytimes.com/2008/03/12/business/12heart-web.html?ref=business

Assurance and Certification

- **Assurance case**
  - All assurance is based on arguments that justify certain claims based on documented evidence
  - Two approaches: implicit (standards based), and explicit (goal-based)
- **Evidence-based Certification**
  - Certification is a judgment that a system is adequately safe/secure /correct/timely for a given application in a given environment
  - The judgment should be based on as much explicit and credible evidence as possible
- **Incremental certification based on evidence**
- **Blackbox recorder for medical device**

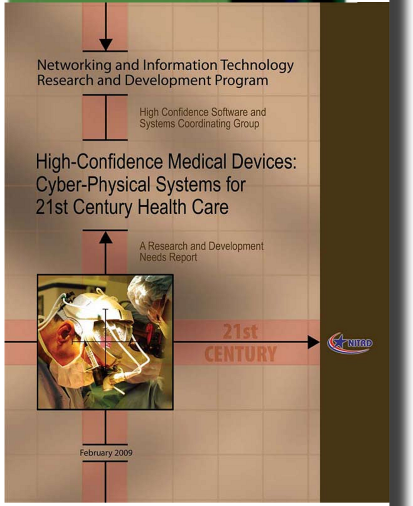


Opportunities for Real-Time Research in HCMDSS

- **System integration and interoperability**
  - Mixed critical systems, mode change protocols
  - Compositional methods with GoS (Guarantee of Service)
  - Real-time interfaces for components
  - Virtualization
- **Model-based development**
  - Patient modeling and simulation
  - Closing the loop
  - Modeling of caregivers
  - Resource-aware design
- **Adaptive patient-specific algorithms** (e.g., smart alarms)
- **Incremental validation and certification**
  - Evidence based
  - Metrics for certifiable assurance and safety
  - Blackbox recorder

Community activities

- CPS workshops sponsored by NSF and NCO/NITRD, etc.
  - HCMDSS (2005), Aviation Software /Certification (2006), SCADA (2006), HCSP -CPS (2007), Security & Privacy (2008), Transportation (2008), …
  - http://varma.ece.cmu.edu/CPS-Forum /Workshops.html
- CPS Week since 2008
  - 2008 (St. Louis), 2009 (San Francisco), 2010 Stockholm) , 2011 (Chicago)
  - Int. Conf. on CPS (ICCPS) 2010
  - www.cpsweek.org


Networking and Information Technology Research and Development Program

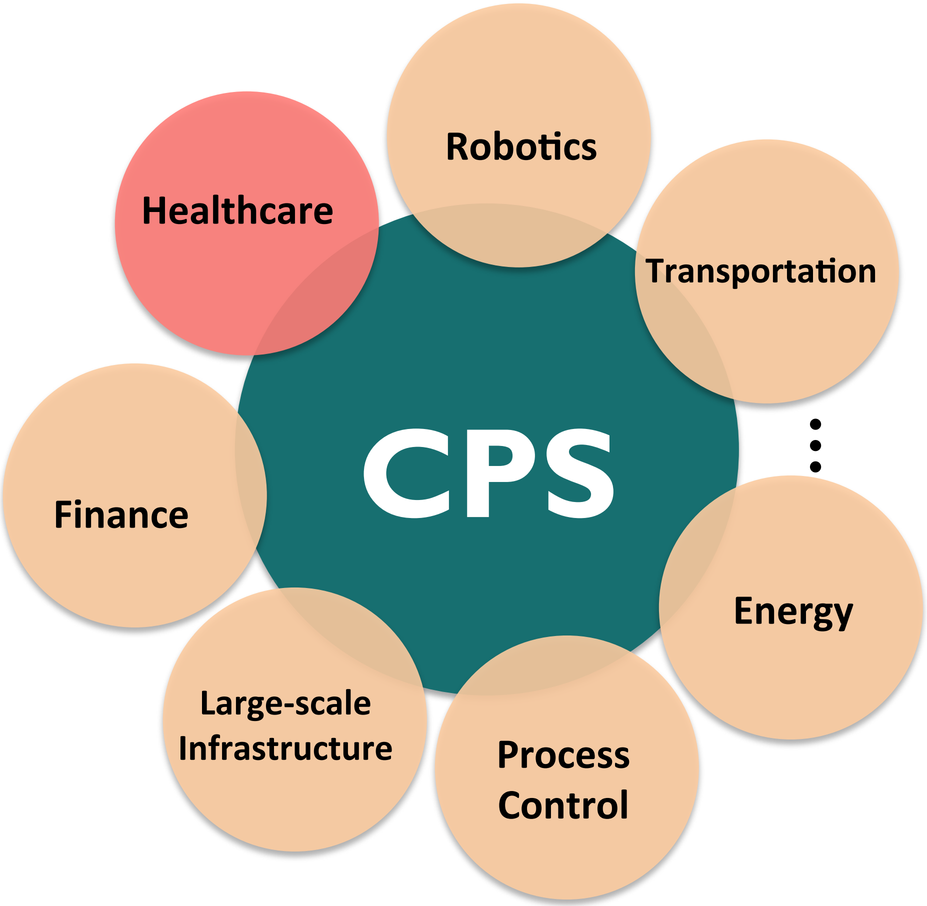
High Confidence Software and Systems Coordinating Group

High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care

A Research and Development Needs Report

21st CENTURY

February 2009



Ultimately, CPS will transform how we interact with the physical world just like the internet transformed how we interact with one another

THANK YOU!