Penn Engineering

University of Minnesota

Assuring the Safety, Security, and Reliability of MDCPS (Medical Device Cyber Physical Systems)

Insup Lee (PI)
PRECISE Center
Department of Computer and Information Science
University of Pennsylvania

NSF CPS Large Meeting
January 31, 2012

MD PnP™ Getting connected for patient safety

Penn Medicine

Team members

- Penn, SEAS
  - Insup Lee (PI)
  - Rajeev Alur
  - Rahul Mangharam
  - George Pappas
  - Rita Powell
  - Oleg Sokolsky
- Penn, UPHS/SoM
  - William Hanson, III, MD
  - Margaret Mullen-Fortino, RN
  - Soojin Park, MD
  - Victoria Rich, RN, PhD
- Penn, Sociology, SAS
  - Ross Koppel
- MGH/CIMIT
  - Julian Goldman, MD
- Minnesota
  - Mats Heimdahl
  - Nicholas Hopper
  - Yongdae Kim
  - Michael Whalen
- Waterloo
  - Sebastian Fischmeister
- Collaborators
  - John Hatcliff, KSU
  - Paul Jones, FDA
  - Sandy Weininger, FDA
  - Zhang Yi, FDA

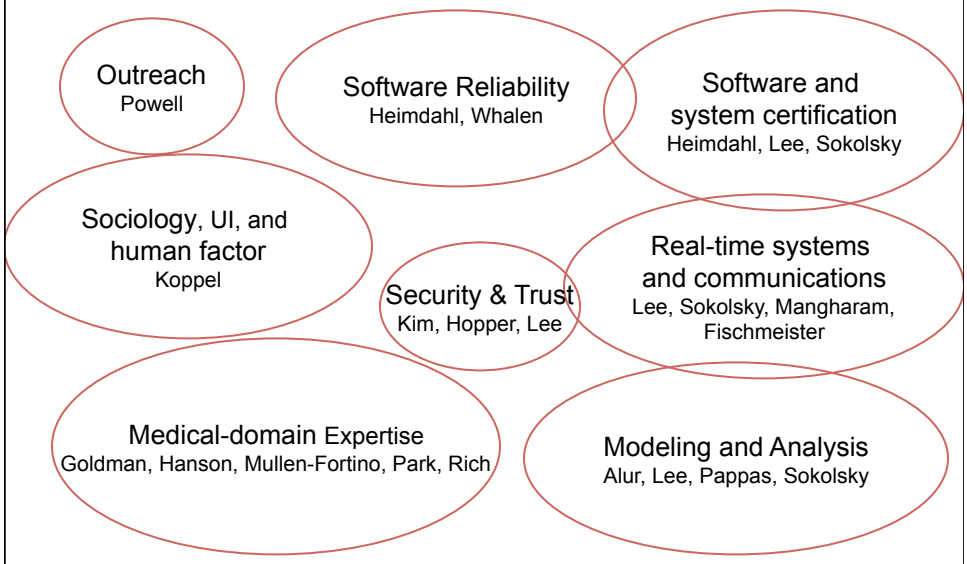
CPS: Large: Assuring the Safety, Security and Reliability of Medical Device Cyber Physical Systems (NSF CNS-1035715)

Affiliated Project:
- Medical Device NIH/NIBIB Quantum Grant: Development of a Prototype Healthcare Intranet for Improved Health Outcomes (PI: Julian Goldman)

Penn Engineering

PRECISE

Team Composition



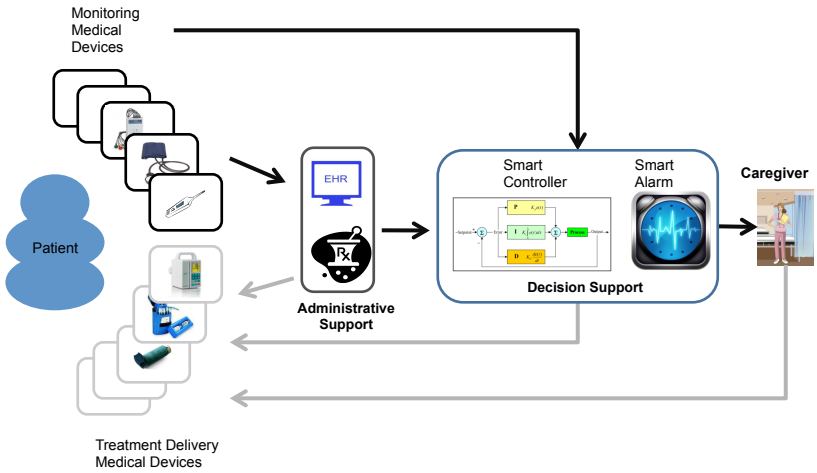
Penn Engineering PRECISE

MDCPS Project Goal

- Develop a new development paradigm for the effective design and implementation of MDCPS that are *safe*, *secure*, and *reliable*:
  - A compositional development framework for safe and secure MDCPS
  - 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
  - An approach to evidence-based regulatory approval and incremental certification of MDCPS

Penn Engineering PRECISE

Vision of MDCPS



Penn Engineering

PRECISE

MDCPS Research Projects

- High-confidence medical software systems
  - Model-based development
  - GPCA (Generic Patient-Controlled Analgesia) infusion pump
  - Pacemaker
- Medical device interoperability
  - MDCF/MIDAS, VMD (virtual medical device)
  - Security and Privacy
- Smart alarms & clinical decision support
- Physiological closed-loop systems
- Assurance and Certification
  - Evidence-based certification
  - Blackbox recorder for medical device

Penn Engineering

PRECISE

Infusion Pump Safety

- During 2005 and 2009, FDA received approximately 56,000 reports of adverse events associated with the use of infusion pumps
  - 1% deaths, 34% serious injuries
  - 87 infusion pump recalls to address safety problems
- The most common types of problems
  - Software Defect
  - User Interface Issues
  - Mechanical or Electrical Failure

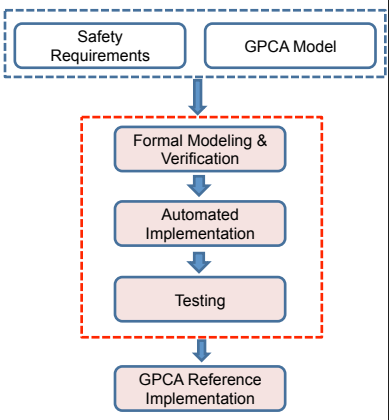
U.S. Food and Drug Administration, Center for Devices and Radiological Health. White Paper: Infusion Pump Improvement Initiative, April 2010

Penn Engineering

PRECISE

GPCA reference implementation

- FDA initiated
  - GPCA Safety Requirements
  - GPCA Model (Simulink/Stateflow)
- Develop a GPCA reference implementation
- Provide evidence that the implementation satisfies the safety requirements
  - Compositional verification
  - Code generation
- Organize evidence for certification
  - Safety cases
  - Confidence cases
- All artifacts to be available as open source
  - http://rtg.cis.upenn.edu/gip.php3



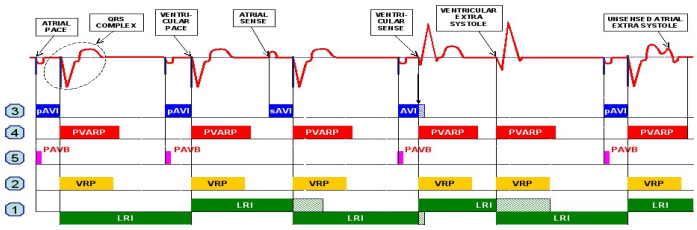
Model-Based Development of GPCA Reference Implementation

Penn Engineering

PRECISE

The Pacemaker Challenge

- The formal method challenge problem issued by the Software Certification Consortium (SCC)
  - The system specification for a previous generation pacemaker from Boston Scientific
- Goals:
  - Provide a traceable model-based design path from requirements to executable code
  - Evidence that code adheres to the formal models
  - Study assurance case construction for MDD
  - Heart modeling

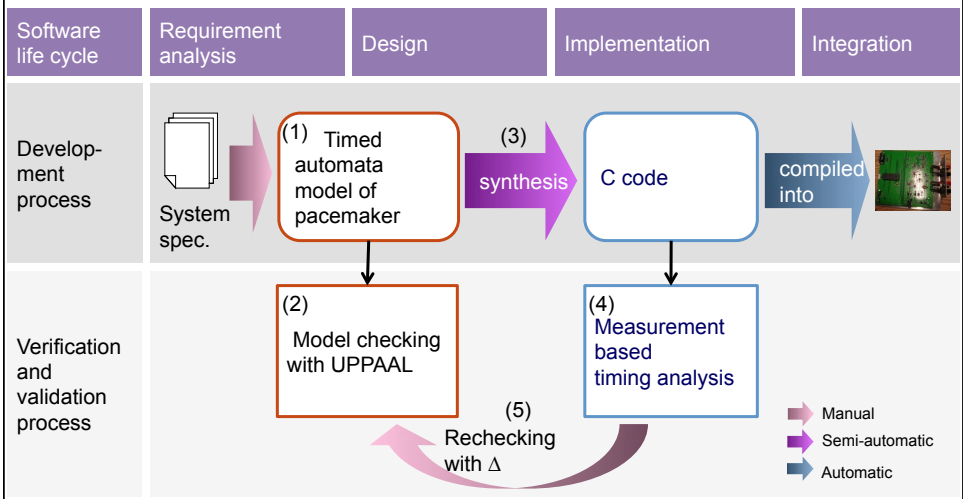


Penn Engineering

PRECISE

Methodology for Safe Medical Device Software

Model-Driven Development + Timing Analysis



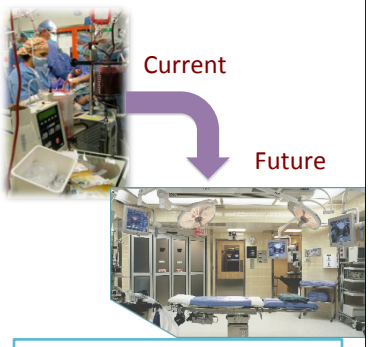
Penn Engineering

PRECISE

Medical-Device Interoperability

Characteristics

- Medical devices gaining communication capabilities
- Devices still operate independently
- Standardized interaction between devices non existent
- Full benefit of communication capabilities not being realized



MD PnP: Interoperable medical devices based on plug-n-play!

Vendor neutrality based on open medical device interfaces

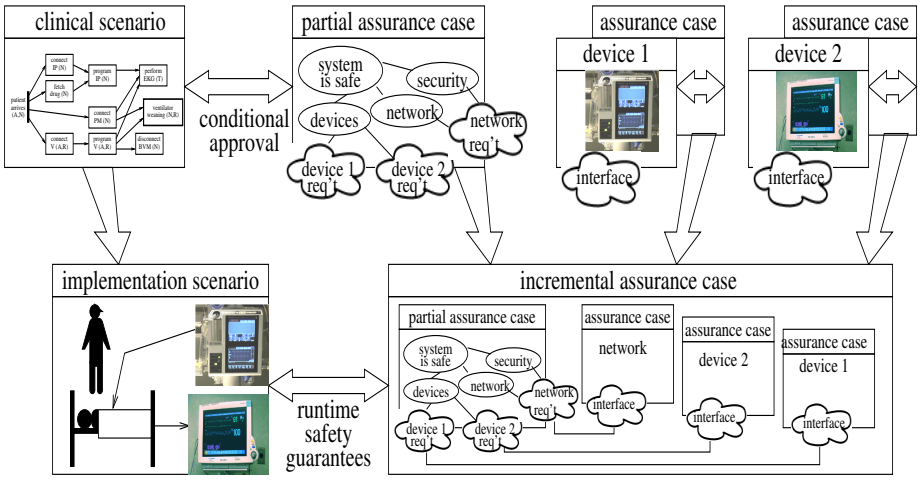
Advantages

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

Penn Engineering

PRECISE

Compositionality Challenge



Penn Engineering

PRECISE

Virtual Medical Devices (VMD)

- **MD PnP** (initiative for medical devices interoperability) enables a new kind of medical device, a **Virtual Medical Device (VMD).**
- VMD is a set of medical devices coordinating over a network for clinical scenario.
- VMD does not physically exist until instantiated at a hospital.
- The Medical Device Coordination Framework (MDCF) is prototype middleware for managing the correct composition of medical devices into VMD.

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

MDCF displays VMD GUI for clinician

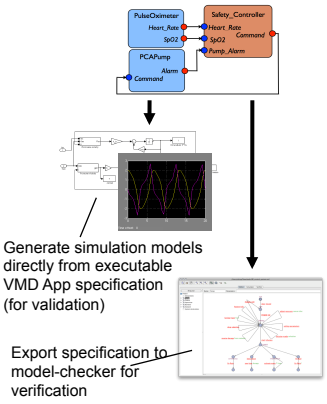
Penn Engineering

PRECISE

VMD Research Issues

- **Real-time support for VMD Apps**
  - Real-time communication infrastructure
  - Pub/sub programming model
  - Support for programming clinical-algorithms with real-time constraints
  - Event driven & Time triggered
  - Guarantee performance specified by VMD App or prevent clinician from instantiating VMD
  - Temporal isolation guarantees
- **MDCF/MIDAS Platform**
  - Device connection protocols
  - Device configuration protocols
  - VMD setup/tear-down algorithm
  - Verify that platform:
    - Correctly implements protocols
    - Instantiation of VMD is safe
    - Non-interference between VMD Apps
    - Runtime verification

VMD App Validation & Verification



Generate simulation models directly from executable VMD App specification (for validation)

Export specification to model-checker for verification

Co-Developed with
NSF CNS-0930647 (PI: John Hatcliff)
Medical Device NIH/NIBIB Quantum Grant (PI: Julian Goldman)

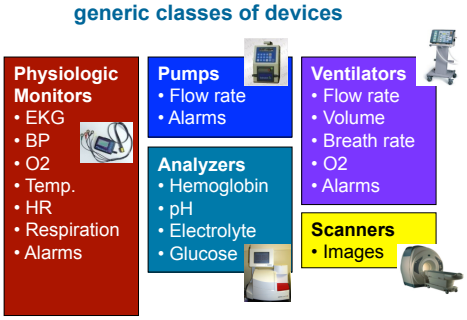
Penn Engineering

PRECISE

Security

- Motivation
  - Devices store personal/ sensitive health information
  - Devices are wireless with increasing access range
  - Connecting to existing IT infrastructure (Internet) for easy access
  - Use of COTS software which might not be designed with security in mind
  - Physiologic monitors might be vulnerable to interference
  - HIPAA requirements

Sensitive information collected by generic classes of devices



Medical devices today, either do not have any inbuilt security features or have proprietary features that are not disclosed.

Penn Engineering

PRECISE

Problem Statement and Approach

- Problem Statement
  - Protect medical devices' data and operation from attackers
- Approach
  - FOUR broad categories of **targets** to be protected:
    - Patient
      - prevent physical harm to the patient
    - Data
      - protect patient data privacy/integrity
    - Device
      - prevent denial of service and damage to devices
    - Institution
      - prevent targeting of medical institution

Attacker Categories

- Operational Categories:
  - **Passive**
    - Eavesdrop on communication
    - Do not actively engage in the system's operations
  - **Active**
    - Actively engage in the system's operations
    - Can flood, modify, delay, replay information
    - Can physically compromise systems
- Contextual Categories:
  - **Insiders**
    - Attackers that are part of the system and have inside information
  - **Outsiders**
    - Attacker that do not belong to the system
- Cohesiveness Categories:
  - **Coordinated**
    - Active attacker nodes that work in a coordinated manner to attack a system
  - **Uncoordinated**
    - Lone-wolf
    - Large number of independent attackers

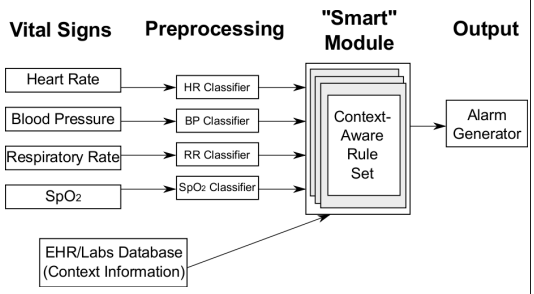
Current Work: Analysis of the ICE Architecture and its variants' communication stack for potential information security vulnerabilities

Penn Engineering

PRECISE

Smart Alarms

- **VMD** of multiple devices and central "smart" controller
  - Filter, combine, process, and present real-time medical information
  - Suppress clinically irrelevant alarms
  - Provide summaries of the patient's state and predictions of future trends
- Benefits
  - Improves patient safety
  - Reduces clinician workload
  - Facilitates practice of evidence-based medicine



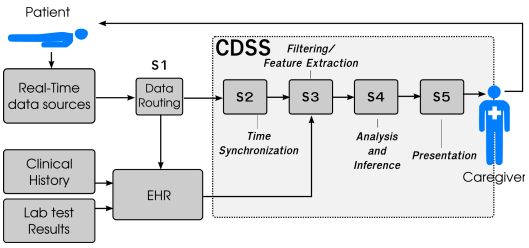
- Challenges
  - Filtering and combining data streams from multiple devices (clock synch?)
  - Developing context-aware patient models
  - Encoding hospital guidelines, extracting experts' models, learning models statistically
  - Presenting data concisely and effectively

Penn Engineering

PRECISE

G-CDS Architecture

- Generic Clinical Decision Support Architecture
  - Modular: flexible and configurable
  - Preprocessing, inference, visualization
  - 3-pronged approach



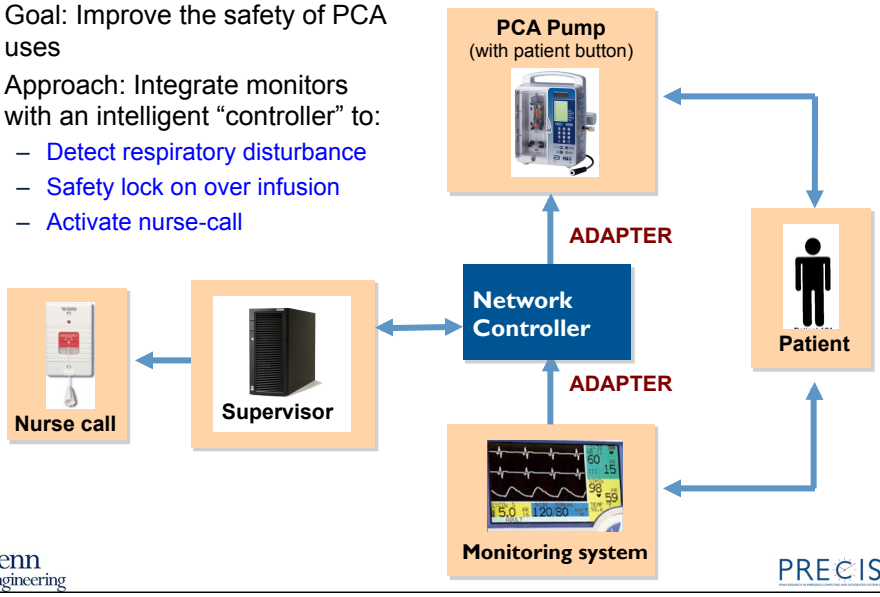
- Case Studies
  - Smart alarm for CABG patients
    - Post-CABG surgery patients produce many false alarms
    - Simple classification with nurse-generated rules: 57% reduction in false alarms
  - Vasospasm decision caddy
  - Sepsis early warning system
- Issues
  - Simplify design to ease workflow integration
  - Understand and establish safety in these systems

Penn Engineering

PRECISE

PCA Closed-loop System

- Goal: Improve the safety of PCA uses
- Approach: Integrate monitors with an intelligent "controller" to:
  - Detect respiratory disturbance
  - Safety lock on over infusion
  - Activate nurse-call

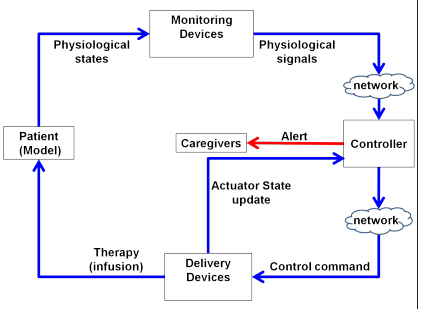


Penn Engineering

PRECISE

Networked Physiological Closed-Loop Systems

- Benefits
  - Improved patient safety
  - Improved clinical outcomes
  - Reduced deployment cost
    - Networking existing medical devices
- Clinical Use Cases
  - Closed-loop PCA
  - Closed-loop Blood Glucose (BG) Control
  - Ventilator weaning procedure
- Challenges
  - Hazard identification and mitigation
    - Network packet delay/drop, sensor disconnection, out-of-sync between controller and devices
  - System modeling and analysis
    - Hybrid (continuous physiology + discrete controller) system simulation & formal verification



Penn Engineering

PRECISE

Certification

- In the U.S., FDA approves medical devices for specific use
  - Safety and effectiveness are assessed
  - Evaluation is process-based: ISO 9001 (quality management) and ISO 14971 (risk management)
  - FDA's 510(k) requires "substantially equivalent" to devices on the market
- Process standards are just one part of the picture
  - Evidence about the product should play a larger role, which provides a reasonable assurance of safety and effectiveness
- Certification of interoperable medical devices in MDCPS
  - Currently, each collection of interconnected devices is a new medical device to be approved. Unsustainable!
  - Can we approve virtual medical devices or clinical scenarios?

Penn Engineering PRECISE

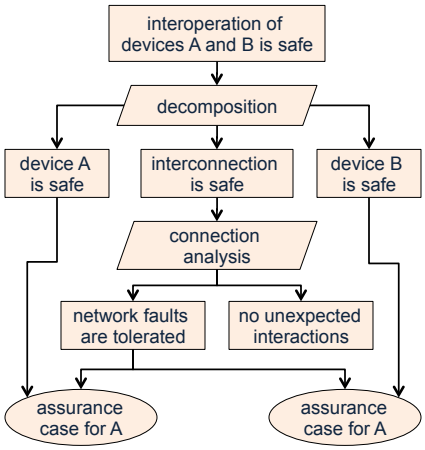
Assurance and Certification

- In search of an evidence-based regulatory regime
  - Suggested by: *Software for Dependable Systems: Sufficient Evidence? D. Jackson, M. Thomas, and L.I. Millett, Eds., National Academies Press, 2007*
  - Assurance cases have been suggested as the basis for evidence-based certification
    - Means of organizing argument
    - Goal-Structured Notation
  - Assurance cases
    - Safety cases
    - Confidence cases
    - Security cases
  - Industry day on assurance cases for medical devices, U. Minnesota, July 28, 2011
- Incremental and compositional assurance and certification

Penn Engineering PRECISE

Compositional Certification?

- A collection of interconnected medical devices is a new medical device
  - Reuse assurance cases for individual devices and concentrate on safety of interconnection?
- Interoperability enables *ad hoc* device assemblies
  - Approve clinical scenarios and interoperability infrastructure?

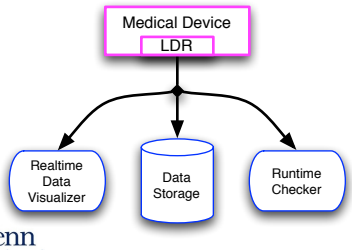


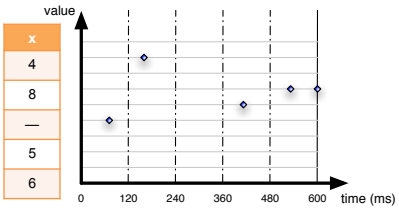
Penn Engineering

PRECISE

Life Data Recorder

- Life Data Recorder (LDR)
  - Blackbox for medical device
  - Proposed by FDA researcher
  - Preliminary prototype design for evaluationHighly configurable
  - Multiple purposes
  - Compact data format design
  - Adaptation to existing or new devices
- Trade-offs and Challenges
  - Timing uncertainty
  - Space limitation
  - Interleaving information about events unknown
  - How to check if a system property is true?
  - How to capture and analyze interactions between medical devices?





Penn Engineering

PRECISE

Posters during lunch

- Safety-Assured GPCA Reference Implementation
- From Verification to Implementation: A Model Translation Tool and a Pacemaker Case Study
- Closed-Loop Pacemaker Testing and Verification Test-Bed Real-Time Heart Model on a Chip

- Middleware Assurance Substrate
- Medical Device Dongle: An Open-Source Standards-Based Platform for Inter-operable Medical Device Connectivity

- Clinical Decision Support for Integrated Cyber-Physical Systems: A Mixed Methods Approach
- Model-Driven Safety Analysis of Closed-Loop PCA Systems
- Modeling and Analysis of Closed-loop Glucose Control Systems

- A Safety Case Pattern for Model-Based Development Approach
- Life Data Recorder and Three-Valued Runtime Checking Semantics

Penn Engineering PRECISE

On-going Collaborative Projects

- GPCA (Generic Infusion Pump)
  - Lee, Jones, Whalen, Koppel
- Pacemaker
  - Alur, Mangharam, Heimdahl, Lee, Sokolsky
- Infrastructure of MD PnP (MIDAS, MDCF, RT communication, security)
  - Lee, Goldman, Hatcliff, Fischmeister, Kim, Hopper
- Smart Alarms and Clinical Decision Support
  - Lee, Mullen-Fortino, Park, Lee, Koppel
- Closing the loop
  - Pappas, Lee, Sokolsky, Mangharam, Goldman, Mullen-Fortino, Park
- Assurance cases
  - Sokolsky, Heimdahl, Lee

Penn Engineering PRECISE

Collaboration & Outreach

- Collaboration
  - Regular virtual meetings
    - Biweekly meetings
  - Regular physical meetings
    - Exchange of researchers, students
    - CPSWeek 2011,
    - Joint workshop in HCMDSS/MDPnP 2011
- Outreach
  - Minnesota Summer software symposium
  - Healthcare IT (Cerner) and medical device industries (St Jude, Medtronic, Boston Scientific)
  - Interaction with FDA approval process
  - Research exchange with S. Patek, J. Lach, J. Stankovic at Virginia
  - Collaboration with U. Mass, Amherst and South Carolina on medical device security

Penn Engineering PRECISE

More Outreach Activities

- Co-Chair, joint workshop on High-Confidence Medical Device Software & Systems and Medical Device Plug-n-Play, CPSweek 2011
- Co-Chair, Analytic Virtual Integration of CPS Workshop, RTSS 2011
- Demonstrated Real-Time Heart Model at CPSWeek Demos
- Talk Modeling and verification of embedded software at Programming Languages Mentoring Workshop, POPL, Jan 2012 (Audience: 150 students from undergrads at community colleges to PhD students at research universities)
- Co-Program Chairs, ICCPS 2011, CPSWeek 2011
- Co-General Chairs, ICCPS 2012, CPSWeek 2012
- Co-Organizer, Workshop on Systems of Systems of Medical Devices, SoSMD 2012
- Chair, CPSWeek Steering Committee
- Leader, CPS-VO Medical Cyber-Physical Systems

Penn Engineering PRECISE

Invited/Keynote Talks

- R. Alur, Formal verification of hybrid system, EMSOFT, Taipei, Taiwan, October 2011
- R. Alur, Interfaces for control components, FORMATS, Aalborg, Denmark, September 2011
- M. Heimdalh, Assurance Cases and Software: Is there any evidence? 2nd Software Certification Consortium Workshop: Theoretical Basis for System and Software Engineering Practices and Certification (at IBM CASCON 2011). November 2011. Toronto, Canada.
- M. Heimdalh, Software Certification and Tool Qualification. Software Development Productivity (SPD) Cross Agency National Needs Summit. September 2011. NASA Ames Research Center, Moffet Field, CA
- M. Heimdalh, Formal Model-Based Development in Medical Devices: Promises and Pitfalls. Joint Workshop on High Confidence Medical Devices, Software, and Systems \& Medical Device Plug-and-Play Interoperability (HCMDSS/MDPnP 2011). April 2011. Chi
- \M. Heimdalh, Model Based Development (MBD) for Medical Devices: Promises and Pitfalls. LifeSciecne Alley, Minneapolis, March 2011.
- I. Lee, Medical Cyber-Physical Systems, EU-US Workshop on Networked Monitoring & Control/CPS, Brussels, Belgium, June 2011
- I. Lee, Cyber Physical Systems: 21st Century Embedded Systems, ISET 2011, Jeju, South Korea, May 2011
- I. Lee, Compositional scheduling and analysis techniques for real-time embedded systems, CPS Day @DGIST, Deagu, South Korea, May 2011
- I. Lee, Medical Cyber Physical Systems, Dept. of Computer Science, Washington University, Dec 2010
- R. Mangharam, Computer Methods for Medical Devices: Validation of Computer with Nonclinical Models, FDA/NHLBI/NSF Workshop, September 2011
- M. Whalen, Proving the Shalls in Practice: Experience with Industrial Formal Analysis, Keynote address at the 19th Annual Requirements Engineering Conference, August, 2011
- M. Whalen, Next-Generation V&V Techniques for Medical Devices, OPAL MedicalDevice Summit, March, 2011

Penn Engineering PRECISE

Recent Publications

- W. Visser, M. B. Dwyer, and M. W. Whalen, The Hidden Models of Model Checking. Journal of Software and Systems Modeling, [submitted - under review]
- A. Ayoub, B. G. Kim, I. Lee and O. Sokolsky, A Safety Case Pattern for Model-Based Development Approach. NASA Formal Methods Symposium, Norfolk, VA, April 2012.
- D. Cofer, A. Gacek, S. Miller, M. W. Whalen, and B. LaValley, Compositional Verification of Architectural Models. Proceedings of the Fourth NASA Formal Methods Symposium, Norfolk, VA, April 2012.
- T. Kahsai, P. L. Garoche, C. Tinelli, and M. W. Whalen, Incremental Verification with Mode Machine Invariants in State Machines. Proceedings of the Fourth NASA Formal Methods Symposium, Norfolk, VA, April 2012 .
- M. Pajic, Z. Jiang, I. Lee, O. Sokolsky, and R. Mangharam, From Verification to Implementation: A Model Translation Tool and a Pacemaker Case Study. 18th IEEE Real-Time and Embedded Technology and Applications Symposium, April 2012.
- Z. Jiang, M. Pajic, S. Moarref, R. Alur, and R. Mangharam, Modeling and Verification of a Dual Chamber Implantable Pacemaker. 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, March 2012.
- I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. G. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. Venkatasubramanian, Challenges and Research Directions in Medical Cyber-Physical Systems. Special Issue on Cyber-Physical Systems, IEEE Proceedings, Jan 2012.
- Z. Jiang, M. Pajic, S. Moarref, R. Alur, and R. Mangharam, Modeling and verification of a dual chamber implantable pacemaker. 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, 2012.
- D.F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, Location leaks on the GSM air interface. ISOC Network & Distributed System Security Symposium, 2012.

Penn Engineering PRECISE

More Publications (2011)

- Z. Jiang, M. Pajic, and R. Mangharam, Cyber-Physical Modeling of Implantable Cardiac Medical Devices. IEEE Proceedings, Special Issue on Cyber-Physical Systems, November 2011.
- B. G. Kim, A. Ayoub, O. Sokolsky, I. Lee, P. Jones, Y. Zhang, and R. Jetley, Safety-Assured Development of the GPCA Infusion Pump Software. Proceedings of the International Conference on Embedded Software (EMSOFT 2011), Taipei, Taiwan, October 2011
- O. Sokolsky, I. Lee, and M. Heimdahl, Challenges in the Regulatory Approval of Medical Cyber-Physical Systems. Special session on software certification, EMSOFT, ESWeek, Oct 2011.
- D. Arney, K. Venkatasbramanian, O. Sokolsky, and I. Lee, Biomedical Devices and Systems Security. Proceedings of 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2011), Boston, MA, August 30 - September 3, 2011
- C. Murphy, M.S. Raunak, A. King, S. Chen, C. Imbriano, G. Kaiser, I. Lee, O. Sokolsky, L. Clarke, L. Osterweil, On Effective Testing of Health Care Simulation Software. Proceedings of the 3rd International Workshop on Software Engineering in Health Care (SEHC 2011), Honolulu, Hawaii, May 2011.
- R. Alur, Formal verification of hybrid systems. 11th International Conference on Embedded Software, 2011.
- R. Alur and A. Trivedi, Relating average and discounted costs for quantitative analysis of timed systems. 11th International Conference on Embedded Software, 2011.
- Z. Jiang and R. Mangharam, Modeling Cardiac Pacemaker Malfunctions with the Virtual Heart Model. 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2011.
- S. Park, A. Roederer, R. Mani, S. Schmitt, P. LeRoux, L. Ungar, I. Lee, S. Kasner, Limitations of Threshold-Based Brain Oxygen Monitoring for Seizure Detection. NEUROCRITICAL CARE: Volume 15, Issue 3 (2011).

Penn Engineering

PRECISE

More Publications (2010)

- A. King, A. Roederer, D. Arney, S. Chen, M. Fortino-Mullen, A. Giannareas, C. W. Hanson III, V. Kern, N. Stevens, J. Tannen, A. V. Trevino, S. Park, O. Sokolsky, and I. Lee, GSA: A Framework for Rapid Prototyping of Smart Alarm Systems. Proceedings of the 1st ACM International Health Informatics Symposium (IHI '10), Arlington, Virginia, USA, November 2010.
- E. Jee, I. Lee and O. Sokolsky, Assurance Cases in Model-Driven Development of the Pacemaker Software. Proceedings of the 4th International Symposium On Leveraging Application of Formal Methods, Verification and Validatio, Part II, LNCS 6416, Amirandes, Heraclion, Crete, October 2010.
- E. Jee, S. Kim, S. Cha, and I. Lee, Automated Test Coverage Measurement for Reactor Protection System Software implemented in Function Block Diagram. Proceedings of the 29th International Conference on Computer Safety, Reliability and Security, LNCS 6351, Vienna, Austria, September 2010.
- E. Jee, S. Wang, J. K. Kim, J. Lee, O. Sokolsky, and I. Lee, A Safety-Assured Development Approach for Real-Time Software. Proceedings of the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, August 2010.

Penn Engineering

PRECISE

Penn Engineering

The rest of the day

http://rtg.cis.upenn.edu/MDCPS/2012jan_meeting.html