High-Assurance Medical Device Systems

Insup Lee
PRECISE Center
School of Engineering and Applied Science
University of Pennsylvania

PRECISE Center Open House
May 18, 2012
Our MCPS Research

• High-confidence medical software systems
  – Infusion pump software
  – Pacemaker systems
• Medical device interoperability platform
  – Compositional safety platform
  – Security & Privacy
• Smart alarms & clinical decision support
• Physiological closed-loop control
• Assurance and Certification
  – Evidence-based certification
  – Blackbox recorder for medical device
Some Software-related Failures

• Therac-25 (1985-1988)
  – Failure to understand software fault tolerance

• Numerous problems with radiation treatment
  – Failures in the generation of treatment plans

• Pacemakers (500K recalls during 1990-2000)

• St Jude pacemaker programmers (2006)
  – Incorrect reporting of pacemaker state

• Difibtech external defibrillators (2007)
  – Self-test resets low-battery status

• Baxter’s Colleague Infusion Pumps (2010)
  – Software update triggers buffer overflow, stops pump
Example: Infusion Pumps

- Involved in many clinical accidents
  - 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
Generic PCA (GPCA) Project

- PCA Infusion Pump
- GPCA Model
- Assurance Case
- Hazard Analysis
- Model-Based Implementation
- Safety Requirements
- Reference Model

GPCA Hazard Analysis

GPCA Safety Requirements
GPCA reference implementation

- FDA initiated
  - GPCA Safety Requirements
  - GPCA Model (Simulink/Stateflow)

- Develop a GPCA reference implementation
  - Model-based development

- Provide evidence that the implementation satisfies the safety requirements
  - Safety cases
  - Confidence cases

- All artifacts to be available as open source
  - [http://rtg.cis.upenn.edu/gip.php3](http://rtg.cis.upenn.edu/gip.php3)
Interoperability and Compositionality

**Problems**

- Standardized interaction between devices nonexistent
- Full benefit of communication capabilities not being realized

**Advantages**

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

*WE ARE THE FUTURE*

- Developing technology to enable safe interoperability of medical devices across manufacture boundaries.
Closed Loop Safety Interlock

Example Use-Case: PCA Monitoring

- Patients are commonly given patient-controlled analgesics after surgery
- Crucial to care, but numerous issues related to safety

A 49-year old woman underwent an uneventful operation (total abdominal hysterectomy and bilateral salpingo-oophorectomy). Postoperatively, the patient complained of severe pain and received intravenous morphine sulfate in small increments. She began receiving a continuous infusion of morphine via a patient controlled analgesia (PCA) pump. A few hours after leaving the PACU [post anesthesia care unit] and arriving on the floor, she was found pale with shallow breathing, a faint pulse, and pinpoint pupils. The nursing staff called a "code", and the patient was resuscitated and transferred to the intensive care unit on a respirator. Based on family wishes, life support was withdrawn and the patient died. Review of the case implicated a PCA overdose. Delayed detection of respiratory compromise in patients undergoing PCA therapy is not uncommon because monitoring of respiratory status has been confounded by excessive nuisance alarms.

[hatcliff]
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
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 app 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
Smart Alarms

- 85%-99% of alarms generated in ICUs are false 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 caregiver 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
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
  - Vasospasm decision caddy
  - Sepsis early warning system

- **Issues**
  - Simplify design to ease workflow integration
  - Understand and establish safety in these systems
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 MCPS
  – Currently, each collection of interconnected devices is a new medical device to be approved. Unsustainable!
  – Can we approve virtual medical devices or clinical scenarios?
  – Incremental and compositional assurance and certification
Assurance Cases

- Evidence-based certification
  - How do we organize and evaluate evidence
  - To gain adoption, we need to understand what works and what does not

- Assurance cases have been suggested as the basis for evidence-based certification
  - Means of organizing argument
  - Goal-Structured Notation

- Case Studies
  - Pacemaker, GPCA

- Future work
  - Patterns for model-based design
  - Evaluation strategies
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

- **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 Projects:**
  - CPS:Medium:Collaborative Research: Infrastructure and Technology Innovations for Medical Device Coordination, KSU (PI: Hatcliff) (NSF-0930647)
  - Medical Device NIH/NIBIB Quantum Grant: Development of a Prototype Healthcare Intranet for Improved Health Outcomes (PI: Goldman)
Posters on MCPS

• Model-base development
  – Jhihao Jiang, Closed-loop Testing and Verification of Implantable Medical Devices
  – BaekGyu Kim, Safety-Assured Development of the GPCA Infusion Pump Software
  – Miroslave Pajic, From Verification to Implementation: A Model Translation Tool and a Pacemaker Case Study

• Medical Device Interoperability
  – Sanjian Chen, Closed-loop Medical Cyber-Physical Systems: Networked Physiological Control System
  – Andrew King, Medical Device Interoperability Infrastructure & Ecosystem
  – Alex Roederer, A Generic Architecture for Building Better Clinical Decision Support Systems

• Certification
  – Anaheed Ayoub, Assurance Cases for Medical Devices
  – Shaohui (Vincent) Wang, Life Data Recorder and Three-Valued Runtime Checking Semantics
Thank You!
Questions?
High-Confidence Medical Device Software & Systems
Medical CPS

Monitoring Medical Devices

EHR

Administrative Support

Decision Support

Smart Controller

Smart Alarm

Caregiver

Patient

Treatment Delivery Medical Devices
Cast Study: CABG Smart Alarm

- **CABG** (Coronary Artery Bypass Graft)
  - Monitoring of post-CABG patients
  - 57% reduction in false alarms
  - No missed true alarms
  - Rule-based, from clinical guidelines and experts
  - Margaret Fortino-Mullen, RN

<table>
<thead>
<tr>
<th>BP</th>
<th>HR</th>
<th>SPO$_2$</th>
<th>RR</th>
<th>Alarm Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal High</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>Normal</td>
<td>Normal</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>2</td>
</tr>
<tr>
<td>Very Low</td>
<td>Normal</td>
<td>Normal</td>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Normal</td>
<td>High</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1: Small subset of the rule set.
Case Study: Vasospasm Decision Caddy

- Post-brain surgery risk
- Hard to diagnose, deadly if not caught early
- Requires combing through 15 days of data
- Provide supporting information
  - Context for alarms
  - Give clinicians access to data
- 3-pronged approach
  - Guideline driven
  - Physician driven
  - Data driven
- Soojin Park, MD

- Analyze data in new ways
  - New device sources
  - Trending
  - Waveform analysis
  - Clinician provide data
  - Cope with missing data
Key Safety Property of Closed-Loop PCA

Pump stops in time if total delay $\leq t_{\text{crit}}$

Total delay is the sum of:
- $t_{\text{POdel}}$: worst case delay from PO (1s)
- $t_{\text{net}}$: worst case delay from network (0.5s)
- $t_{\text{Sup}}$: worst case delay from Supervisor (0.2s)
- $t_{\text{Pump}}$: worst case delay from pump (0.1s)
- $t_{\text{P2PO}}$: worst case latency for pump to stop (2s)
- $t_{\text{crit}}$: shortest time the patient can spend in the alarming region before going critical