Safety of Interoperable Systems

Sandy Weininger, Dave Arney
FDA, CDRH, OSEL
MD PnP (www.mdpn.org) / MGH, UPenn
Safety of Interoperable (Medical) Systems

• We want safe, interoperable systems of medical devices.

• Interoperability = The ability of two or more medical devices and other equipment, which are intended by their manufacturers to exchange information via an electronic data interface (EDI), to safely perform a clinical function with a specific intended use, and in a assembled configuration not necessarily foreseen by the manufacturers.

• This presentation represents our initial experiments and first pass applying STAMP to this domain, not necessarily correct

• Medical devices are designed and regulated as stand-alone devices, not as system components

• But they are being used in very complex systems.

Disclaimer: None of this is in any way official commentary from FDA
Safety of Interoperable (Medical) Systems

• Medical devices are different from other communities
  – Many stakeholders: hospitals, regulators, patients, clinicians
  – No single system integrator
  – No process model

• Every integration effort is an individual, one-off exercise

• Every day, clinicians have ideas about how to implement safer systems, but these can't be implemented

• Medical devices are already part of the patient care system, whether or not they're good players. Clinicians manually coordinate device usage.

• A standardized approach with defined, reusable components across the industry will lead to easier integration

• The system can be safer than the device (e.g., PCA) if we can address the known significant system hazards and common PCA failure modes. Need contextual info + sensor info + supervisory system to enhance safety.

• The system may detect/compensate for device safety shortcomings (e.g., PCA fails in free flow or drug library has error)
RESOLVED, That our American Medical Association (AMA) believes that intercommunication and interoperability of electronic medical devices could lead to important advances in patient safety and patient care, and that the standards and protocols to allow such seamless intercommunication should be developed fully with these advances in mind. Our AMA also recognizes that, as in all technological advances, interoperability poses safety and medico-legal challenges as well ...

as of July 2009:

Anesthesia Patient Safety Foundation
Society for Technology in Anesthesia
Society of American Gastrointestinal Endoscopic Surgeons

American Medical Association
World Federation of Societies of Anesthesiologists
American Society of Anesthesiologists
Massachusetts Medical Society
Each box is a system component.
Apps are components with intended uses.
ASTM F2761 (ICE) architecture and AAMI/UL 2800 – interoperable medical device interface safety

Reducing Interface Complexity is Key

AAMI/UL 2800 Deterministic Interface for Risk Management
AAMI/UL 2800 in the “big picture”

- Clinical Scenario
- Interoperable Scenario
- System Safety / Interoperability (HL7, IEEE, Continua, etc...)
- Connectivity / Interoperability (Wi-Fi, Bluetooth, Zigbee, Ethernet, etc...)
- Enabling Technologies (Wi-Fi, Bluetooth, Zigbee, Ethernet, etc...)

AAMI/UL 2800
Environment for which medical devices are designed and regulated

program

Infusion Pump

Flow of fluid
Stand-alone device development

• System-level Accidents, Hazards, Safety Constraints are minimally considered in current development and regulatory practice.
• Intended use may include sending data to an EMR
• Very few devices allow control inputs through their network connection
• So of course we see unintended interactions all the time.
NIBP-SpO₂ Interaction
Real use environment for medical devices
Clinical care: Is not neat and tidy. Poor access to data, only manual coordination of devices.
Hospital IT system

- Hospital IT is highly balkanized
- Typically, each manufacturer has a VPN and gateway server
- Integration is up to each hospital
PCA Clinical Scenario

• **Clinical Scenario Narrative Description**
• **Scenario Current State**
  • A 49-year-old woman underwent an uneventful 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) infusion pump. A few hours after leaving the post-anesthesia care unit (PACU) 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 by providers implicated a PCA overdose (1)

• **Scenario Proposed State**
  • While on the PCA infusion pump, the patient is monitored with a respiration rate monitor and a pulse oximeter. If physiological parameters move outside the pre-determined range, the infusion can be stopped and alarms sent to notify the clinical staff and restart the infusion if appropriate. The use of two independent physiological measurements of respiratory function (oxygen saturation and respiratory rate) enables a smart monitor to optimize sensitivity to detecting respiratory compromise while reducing false alarms.

• One Clinical Scenario of NIH “Quantum Medical Device Interoperability” [www.mdpnp.org/quantum.html] research project
Patient-Controlled Analgesia (PCA) system safety concerns

- Patient presses button to receive intravenous pain medication
- Patients can call to request more analgesia, but, cannot call for help when over-medicated.
- Over-medication can cause respiratory and cardiac arrest
- Comprehensive monitoring is not typically used due to high false/nuisance alarm rate
- How can we improve safety of this system?
Why is optimizing the safety and effectiveness of PCA difficult?

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Challenge</th>
</tr>
</thead>
</table>
| A. PCA is **safe** because patient must be alert to “request” each dose | 1. Patients may have marked variation in sensitivity. Requirements vary across patients and over time, co-morbidities (OSA, ARF), and use of other medications. In some patients **one** dose may cause overdose.  
2. Use of basal infusion rate is controversial  
3. PCA by proxy (especially in pediatrics, also adults)  
4. Device and delivery problems can overestimate dosage requirements |
| B. PCA is **effective** because patients can dose on demand | 1. PCA protocols are optimized for “average” patient  
2. Fear of iatrogenic respiratory arrest delays aggressive, effective pain management especially in opioid-tolerant patients |
| C. Q 4-hour recommended reassessment is appropriate to achieve analgesic efficacy | Pain scoring requires awakening/disturbing patient and possibly their family members. Automated continuous analgesic assessment may be possible. |
Why is optimizing the safety and effectiveness of PCA difficult?

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Challenge</th>
</tr>
</thead>
</table>
| D. Current monitoring is adequate to provide detection of respiratory compromise | 1. **Current** detection of respiratory compromise is not sufficiently sensitive and specific to prevent harm. **Earlier** detection of respiratory distress may avoid harm. Algorithm development is challenging due to lack of historical, comprehensive, baseline data.  
2. Use of supplemental O2, placement of monitors, and monitor response time must be considered  
3. Comprehensive monitoring has been shown to reduce/prevent “dead in bed” events, but not early detection of respiratory compromise and associated morbidity. In addition iatrogenic response is to undertreat pain in these settings. optimization of analgesic therapy. |
| E. Stopping PCA pump after detection of respiratory distress will be a sufficient intervention | 1. Cessation of therapy is a poor and painful solution. Adaptive dose titration may be a better response.  
2. Adaptive system requires reliable Integration of monitors and clinical data, deployment of personalized alarms, AND ability to adjust rate of IV opioid delivery |
Why is optimizing the safety and effectiveness of PCA difficult?

<table>
<thead>
<tr>
<th>Assumption</th>
<th>Challenge</th>
</tr>
</thead>
</table>
| F. Current vital signs monitors provide accurate, complete, and timely data for real-time decision support. Information about nursing interventions, patient activity, time-of-day, co-morbidities, and concurrent medications can be easily documented and used to create optimum monitoring algorithms | 1. Comprehensive PCA observational data set is not available. Useful data set may require customized electronic data interfaces and expert observation.  
2. Performance (accuracy, sensitivity, specificity) of conventional non-invasive monitors may be inadequate. Specialized monitoring strategies may be required. |
| G. Relevant Co-morbidities are known                                       | Obstructive sleep apnea is under-diagnosed and may be an important factor in PCA safety. PCA Safety System may also be able to screen for OSA. |
Analyzing Interoperable Medical Devices with STAMP

• We need a defined, controlled development process

• Manufacturers must build in safety as opposed to testing at end

• We’re here to figure out what that means from practical perspective
Component-level

- Component only introduced into system if it meets conditions of acceptability
- Components are (typically) FDA cleared devices that can maintain basic safety and essential performance while functioning in a heterogeneous networked environment
- Interface standard is intended to be applied early in the product development process to help establish a baseline set of safety constraints to be implemented during the design phase, and which we hope to determine as a function of system hazards (clinical workflow driven) with the aid of STPA/STAMP.
- Many system level hazards are mitigated by the controller app component
System-level

System goal: Identify entities (and boundaries) that have a responsibility in assuring the safety of the patient, determine the monitoring or control action, and provide a means of assessing what happens if …

1. required action not provided or followed
2. incorrect or unsafe control action is provided
3. potentially safe control action is provided too early or too late
4. correct control action is stopped too soon

• And what happens if one of the entities doesn’t do its job.
• Hope to provide template as starting point for instantiations designs that are compatible with this control loop notion
Black Box Level Process Model

Only a very few elements are captured here to illustrate that influence can go in both ways from each box, and that there are interactions that need to be made explicit for both entities and devices.

For example, the training material for the HDO and from the manufacturer are related. Problems found in one need to be communicated to the other.
High Level Safety Control Structure

- Health Delivery Organization Safety Control
- Regulatory Oversight
- Standards Development
- Patent + Devices
- Accreditation / Certification
  - System Development (Manufacturer)
    - Risk management
    - Systems Engineering
      - Design control
      - Life cycle phases
  - Authorities having jurisdiction
    - Congress
    - Executive
    - FDA/CDRH
    - OSHA
    - State boards
    - Local code authority
    - HDOs
    - Professional societies

Note – the role of each stakeholder from the MDICC subgroups should be considered.
First attempt at understanding the functions in a health delivery organization; note that no interactions have been drawn in yet.
Conclusions

- STAMP is a tool for identifying and thinking through the safety and regulatory issues for plug and play interoperable medical devices.
- The current STAMP exercise is only a first attempt at getting experience using the STAMP process.
- STAMP process looks useful, particularly for identifying roles and responsibilities and interactions - we are trying to apply it to our issues.
- We will be analyzing the outcomes looking to see how it can guide our work.
- Several standards activities are underway; would like a means for understanding how their work products fit into the broader environment to assure safe and effective devices, and safe delivery of health care (promote and protect public health)