Systems Engineering at the Point of Care

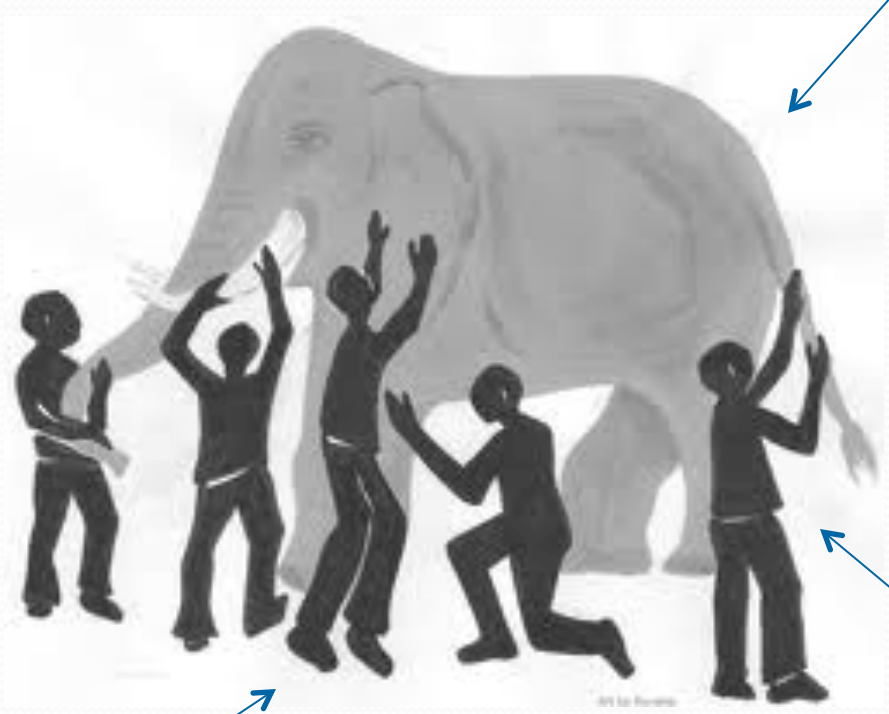
Has the time finally come?

Rick Schrenker
Systems Engineering Manager
Department of Biomedical Engineering
Massachusetts General Hospital
raschrenker@partners.org

A Bit About My Favorite Topic…

- Educational background is in EE
- 33 years in and/or around CE
  - Johns Hopkins (1979 – 1990)
  - MGH (1990 – Now)
- Variety of interests (not necessarily in order of importance)
  - Systems and software engineering
    - Requirements, Validation, Assurance
    - Safety
  - Fishing, dancing, piano, history of engineering…

The Clinical Engineering Perspective



Healthcare System

Clinical Engineering

Allied Health Professionals

PBME - Introduction

Partners Biomedical Engineering (PBME) is comprised of the Departments of Biomedical Engineering at Massachusetts General Hospital (MGH) and Brigham and Women's Hospital (BWH) and also serves the biomedical engineering needs at Dana Farber Cancer Institute (DFCI).

Our Mission

In partnership with clinicians, researchers and other engineering groups, Partners Biomedical Engineering ensures that technology is used appropriately and safely, performs properly and is managed cost-effectively. *It is our goal that no patient is harmed by the application of a medical device within our Partners' sphere of influence.* We strive to improve and develop devices and instrumentation for healthcare delivery and for innovative medical and scientific research and to assist others at Partners who are working toward the same objectives. We are committed to supporting quality and compassionate care to patients.

Our Staff

- Technical support personnel are organized as customer-focused teams of biomedical equipment technicians.
- Clinical Engineers at each hospital are available for special projects.
- The Model Shop fabricates custom-designed devices for clinical and research purposes.
- The Systems Engineering Group provides central support for the other groups in that it administers the technology database that forms the core of the department's service activities. This group also develops and manages the PBME website.
- Medical Advisors at each hospital give critical clinical guidance for addressing patient care needs.
- We have a close relationship to the Center for Integration of Medicine and Innovative Technology (CIMIT).

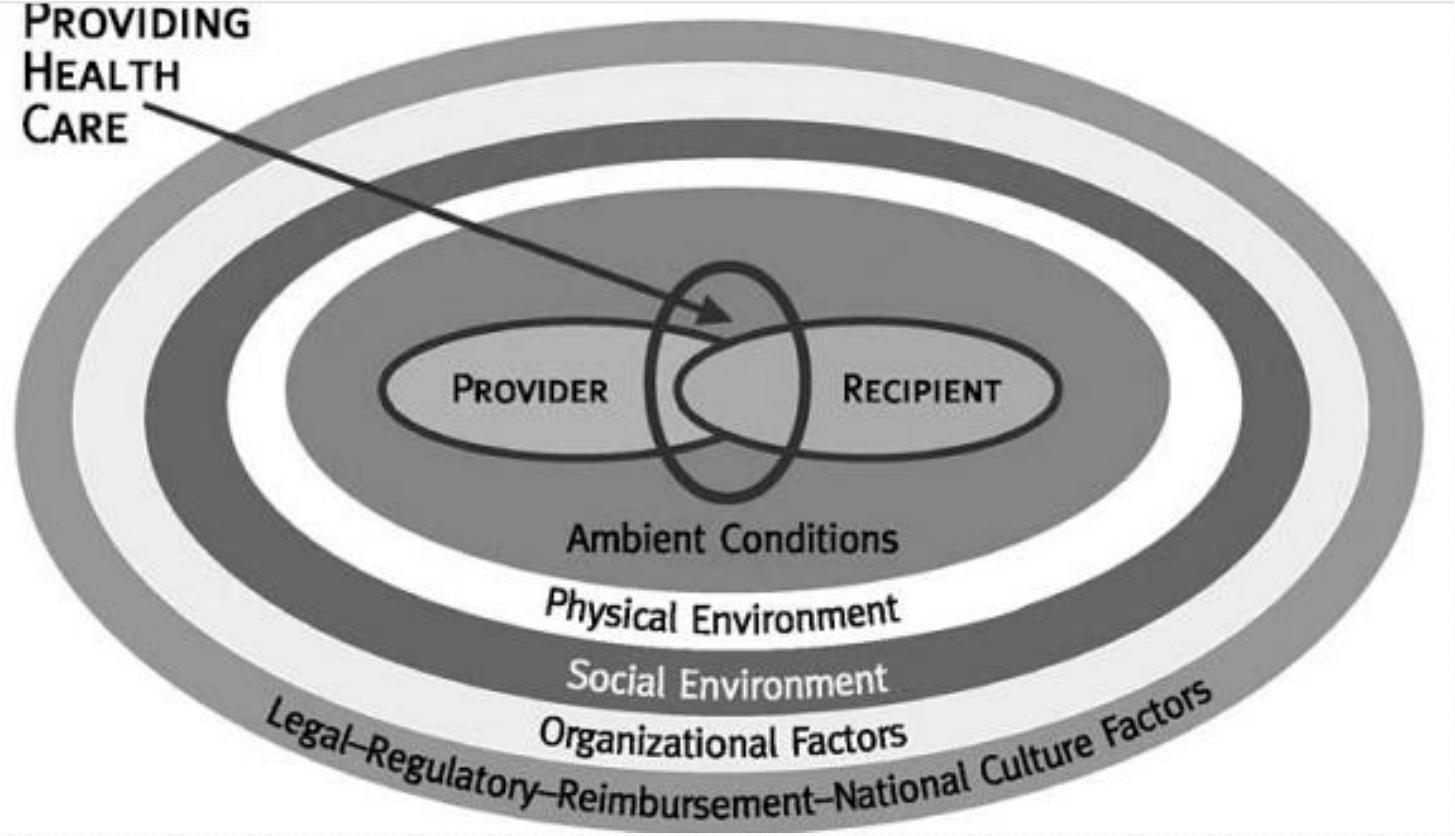
Our Medical Equipment Management Functions

- Technology acquisition and development
- Equipment repair, maintenance, and inspectiion
- Technology evaluation
- System installation
- System modification
- User Training
- Custom device development
- System problem solving
- Device failure investigation
- Recall management
- Regulatory requirements management

Some PBME Statistics (End 2008)

- Active medical devices: > 47,000
- Number of manufacturers: > 700
- Number of models: > 3,100
- Number of device types: > 400
- Devices with software version: > 10,000
- Equip work orders, 2008: > 49,000

Zooming back from the Point of Care



Bogner MS, Misadventures in Health Care – Inside Stories, 2004

The Point Of Care Subsystem - Dynamic Properties

"…Patient status follows a trajectory that is not fully deterministic, and the associated dynamics both impact and are impacted by environmental, operational, and situational contexts that evolve with time.

System components may be added or removed, clinical experts come and go, and patients move between more or less technology-intensive environments.

Over time, events emerge that can only be discerned through system understanding (a ventilator is off that should be turned on, a requested dose of narcotic pain relief should not be administered).

Only by understanding the system in its situational context can these problems be appreciated and clinical requirements identified. "

And All the While, "The Singularity" Approaches…

- *Clinical Engineering and Personal Computer Maintenance*, AAMI Annual Meeting, 1986
- *The Andover Working Group: A Model for Implementing Healthcare Information Technology Standards*, AAMI Annual Meeting, 1998
- *A Perspective on the Impact on Safety of the Rate of Change of Technology Used in Patient Care,* Elektrotechnik und Informationstechnik, April 2006
- *Systems and Software Engineering Needs in Clinical Engineering: Requirements, Validation, and Assurance,* AAMI Annual Meeting, June 2009
- *IEC 80001-1 Has Arrived*, 24x7, November 2010 (co-author)
- *Formal Systems Engineering in the Clinical Space: What now? Why now?*, AAMI Annual Meeting, June 2012 (co-presenter)

Consequences of a system-blind approach…

"… Not only did each have a different user interface, but I couldn't intuit any of them…

only so much time for training, and *if a device didn't provide at least some guiding context of itself, I found it relatively more difficult to teach*… more of a concern today, given the accelerating rate of change in technology…

I [can] test drive a car within minutes, but … clinicians almost always require fundamental user training every time they encounter a new model of types of devices that have been around for 25 years. *I'm not talking about training for new features. I'm talking about just learning the user interface*."

http://www.embedded.com/columns/embeddedpulse/159400817

And yet more consequences…

Regarding upgrading medical device software, one vision:

"… Hospitals will have a lab with some number of workstations … configured to support the update of one or more types of medical devices. Technicians will … connect them to the workstation, magic will happen, and the technician will return the devices to the floor. Hopefully nothing will go wrong…

[Afterwards] *an engineer from a medical equipment manufacturer came up to me to say he'd never considered what it might be like on the receiving end of one of his upgrades*."

http://www.embedded.com/columns/embeddedpulse/159400817

What Systems Engineering Has Had to Conjure Up for Its Problems…

- Just a sample…
  - Requirements Engineering
  - Case-Based Assurance
    - Safety (and other) Cases
  - Modeling tools
    - SysML
    - Causal loops
  - Resilience Engineering
  - System Theoretic Hazard Analysis

Resilience - Good News

"Resilience is the ability to **steer the activities of the organization so that it may sail close to the area where accidents will happen** *[without getting there]…"*

A Hale and T Heijer, Defining Resilience, in "Resilience Engineering: Concepts and Precepts" Ashgate Publishing Co, 2006, p 36.

Resilience – Bad News

"Recognizing that a system is **drifting into failure** is difficult because the entire protective structure (including suppliers, regulators, hierarchies, etc.) seems to slide with the operational core towards the boundary…"

S Dekker, Resilience Engineering: Chronicling the Emergence of Confused Consensus, in "Resilience Engineering: Concepts and Precepts" Ashgate Publishing Co, 2006, p82.

System Theoretic Hazard Analysis

What if everything we know is wrong? For example…

"Old Assumption: Probabilistic risk analysis based on event chains in the best way to assess and communicate safety and risk information?

New assumption: Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis" *(N Leveson, "Engineering a Safer World", MIT Press, 2011, p 57)*

What if **medical device risk management standards are PRA based**? Well, they are…

Systems-Theoretic Accident Model and Processes (STAMP)

- "Preventing future accidents requires shifting from a focus on preventing failure to the broader goal of designing and implementing controls that will enforce the necessary constraints." *(Leveson, p 57)*
- "If we are to handle social and human aspects of safety, then our **accident causality models must include the concept of change**. In addition, **controls and assurance that the safety control structure remains effective in enforcing the constraints over time are required**." *(Leveson, p 85)*

Problem 80001
Just the First Problem

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 1: Roles, responsibilities and activities

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.

NETWORK KEY PROPERTIES

(in order of priority)

SAFETY:

*Freedom from **unacceptable risk** of physical injury or damage to the health of people or damage to property or the environment*

EFFECTIVENESS:

*Ability to produce the **intended result** for the patient and the responsible organization*

DATA AND SYSTEM SECURITY:

*An operational state of a medical IT-Network in which information assets (data and systems) are reasonably protected from degradation of **confidentiality**, **integrity**, and **availability***

[+ auditability?]

Note: ***ISO 14971 for medical devices is focused on patient safety risk management***

80001-2-X EMERGING GUIDANCE

Publishing in June 2012

- ✓ **Technical "Guidance" Reports (TRs):**
  - 80001-2-1: *Step-by-Step Risk Management* (w/Examples)
  - 80001-2-2: *Communication of Medical Device Security Needs, Risks & Controls*
  - 80001-2-3: *Wireless Networking*
  - ✓ **In CD ballot …**
  - 80001-2-4: *HDO Implementation Guidance*
- ✓ **In NWIP ballot …**
  - 80001-2-x: *Guidance for Distributed Alarm Systems*
  - ✓ **Pre-NWIP development**
  - 80001-2-x: *Guidance for Responsibility Agreements*

HDO GUIDANCE KEY ASPECT:

Echoes of ISO 9001…

TOP MANAGEMENT needs to ensure the following functions are done:

- define and document the organization's RISK MANAGEMENT policy. This policy will need to address the KEY PROPERTIES;
- create and disseminate suitable RISK MANAGEMENT PROCESSES… ;
- establish RISK acceptability criteria to determine which RISKS are tolerable to the organization.
- review the suitability of the RISK MANAGEMENT PROCESSES at planned, regular intervals…

The Ten Steps…

- STEP 1. Identify HAZARDs
- STEP 2. Identify Causes and resulting HAZARDOUS SITUATIONS
- STEP 3. Determine UNINTENDED CONSEQUENCES and Estimate potential severities*
- STEP 4. Estimate the probability of the UNINTENDED CONSEQUENCE
- By estimating probability and severity of UNINTENDED CONSEQUENCE, you have estimated RISK.
- Iterate Steps 1 through 4, using both top-down and bottom-up approaches.
- There may be multiple HAZARDOUS SITUATIONS per HAZARD, multiple Causes per HAZARDOUS SITUATION, multiple HAZARDOUS SITUATIONS per Cause
- STEP 5. Evaluate RISK against pre-determined RISK acceptability criteria
- STEP 6. Identify and document proposed RISK CONTROL measures and re-evaluate RISK (i.e. return to STEP 3)
- STEP 7. Implement RISK CONTROL Measures
- STEP 8. Verify RISK CONTROL measures
- STEP 9. Evaluate any new RISKs arising from RISK CONTROL
- STEP 10. Evaluate and report overall RESIDUAL RISK

Problem 2: Problem 80001 and Responsibility Agreements

4.3.4 RESPONSIBILITY AGREEMENT

Whenever a MEDICAL DEVICE is incorporated into an IT-NETWORK, or the configuration of such a connection is changed, the RESPONSIBLE ORGANIZATION shall determine the need for one or more documented RESPONSIBILITY AGREEMENTS that define (e.g. by contract) the responsibilities of all relevant stakeholders.

The responsibility agreements shall contain (or refer to documents which contain) at a minimum:

How might we get what we're after?

Why not…

"… software is "guilty until proven innocent," [and the] burden of proof falls on the developer to convince the certifier or regulator that the software is dependable.

a software system should be regarded as dependable only if it has a credible dependability case."

Software for Dependable Systems – Sufficient Evidence, NAE, 2007

Are these sufficient to make the case?

a) the name of the person responsible for RISK MANAGEMENT for the activities covered by the RESPONSIBILITY AGREEMENT;

b) the scope of the activities covered by the RESPONSIBILITY AGREEMENT, including a summary of and/or reference to the requirements;

c) a list of the MEDICAL DEVICES and other equipment which are to be incorporated into the IT-NETWORK or changed, together with the names of MEDICAL DEVICE manufacturers or other organizations responsible for the provision of technical information necessary for the completion of the project;

d) a list of documents to be supplied by the MEDICAL DEVICE manufacturers and other equipment suppliers that contain instructions for connection to or disconnection from an IT-NETWORK;

e) technical information to be supplied by the MEDICAL DEVICE or IT manufacturers and other equipment suppliers that is necessary to perform RISK ANALYSIS for the IT-NETWORK;

f) definition of roles and responsibilities in managing potentially adverse events

g) identify the nature of the co-operation required;

h) state:

- who is responsible for requesting such co-operation;
- who is responsible for responding to such requests; and
- what criteria will be used to judge the adequacy of such response

Fair enough?

"Work as Imagined versus Work as Actually Done

One marker of resilience … is the distance between operations as management imagines they go on and how they actually go on … *Understanding the gap between the system-as-imagined and the system as actually operated* requires investment not only in understanding how the system really works but also how it is imagined to work. The latter can sometimes even be more difficult."

S Dekker, Resilience Engineering: Chronicling the Emerge of Confused Consensus, in "Resilience Engineering: Concepts and Precepts" Ashgate Publishing Co, 2006, pp 86, 89.

Or is it?

"Another impediment to gathering safety data is *contractual barriers (e.g., nondisclosure, confidentiality clauses) that can prevent users from sharing information about health IT-related adverse events*."

G Warden, et al, *Health IT and Patient Safety – Building Safer Systems for Better Care*, National Academies Press, 2011.

Problem 3: Medical Device Data Systems (MDDS)

FDA NEWS RELEASE: February 14, 2011

- "Medical Device Data Systems are off-the-shelf or custom hardware or software products used alone or in combination that *display unaltered medical device data, or transfer, store or convert medical device data for future use*, in accordance with a preset specification."
- "Examples of MDDS products include: devices that collect and store data from a blood pressure cuff for future use or that transfer thermometer readings to be displayed at a nursing station for future use.
- "Information technology companies that design, install or market these systems, ***and hospitals that develop them in their facilities***, must follow Class I requirements as well."

Used with permission R Hampton

Some of what that means…

- Publication in the Federal Register: ***February 15, 2011***
- All manufacturers of MDDSs, *including any health care facilities acting as manufacturers*, will be required to comply with this regulation.
- FDA expects that all MDDS manufacturers will have *established a compliant quality system and MDR system* for their devices ***within 12 months***.
- Particularly, FDA expects all MDDS manufacturers to establish and maintain adequate design controls as part of their quality system.

Used with permission R Hampton

Hoist By My Own Petard

Yes, this was the actual title of a presentation I delivered earlier this month…

And it's relevant here…

Why I Felt the Need to Do It…

"And because the next time the consequence could be worse than simple embarrassment, I share this story.

I suggest that we engineers capture more stories like this… We should keep telling stories for as long as they happen. We need to listen, learn, and change our actions based on these stories. Yet, no matter how much we do that, and how many other potential stories we will have stopped in their tracks, we'll still have more to tell."

R Schrenker, *Learning from Failure: The Teachings of Petroski*, BIT, Sept/Oct 2007

Although this was not about problems with a medical device related project….

It could have been

The Project: Replace the Medical Equipment Management Database

Existing system (at time of replacement)

- Served about 100 users in a number of Partners institutions in Eastern Massachusetts
- Developed jointly with a commercial software company; assumed maintenance and development responsibilities in June 2000
- Development and maintenance system resources
  - SQL7 server, Access 2003 clients
  - Technical Team (Systems Engineering)
    - Program manager
    - DBA
    - Two software developers

A key decision

It was proving difficult to identify detailed requirements, so in order to move forward, we settled on the following:

Our new system would have to at least be functionally equivalent to what we already were using and provide the capability to extend of those features and add new ones.

Where It All Began to Unravel

- Technically speaking
  - Communicating requirements is very difficult to do across domains
    - Consider the difference in the meaning of the word “incident” across the CE-IT divide
    - This even exists internally, e.g., our developers do not always appreciate the needs of their colleagues
  - The tool was more difficult to acquire than anticipated
- Process speaking
  - The functional equivalence constraint was gradually loosened as the capabilities of the tool became more evident

Impact

The development process became the software engineering equivalent to Whack-A-Mole, except without a buzzer to stop it.

Which Reminded Me…

"…if there were a more heightened awareness among designers that in case after case throughout history there have been surprises in extrapolatory design, then designers … might pay more attention to the warning signs that seem invariably to prefigure failure.

Such signs appear to be ignored *when the design environment rests upon an accumulation of successes rather than upon a broad-ranging awareness of failure case studies that point to common errors and lapses in design attention*."

H Petroski, "Design Paradigms", Cambridge University Press, 1994, p97

Help Needed: Problem and/or Wish List

- *… some guiding context [in] the user interface*
- *… an engineer from a medical equipment manufacturer [not knowing] what it might be like on the receiving end of one of his upgrades*
- *… medical device risk management standards are PRA based*
- *… recognizing that a system is drifting into failure*
- *… accident causality models must include the concept of change*
- *… understanding the gap between the system-as-imagined and the system as actually operated*
- *… [identify the] technical information … that is necessary to perform risk analysis*
- *… the tool was more difficult to acquire than anticipated*
- *… the development process became the software engineering equivalent to Whack-A-Mole*
- *… the design environment rests upon an accumulation of successes rather than upon a broad-ranging awareness of failure case studies that point to common errors and lapses in design attention*
- *… case studies*