This article is part of the IEEE Reliability Society 2008 Annual Technology Report.

Trustworthy Medical Devices

John Harauz
Email: j.harauz@computer.org

Advances in health information systems and healthcare technology present opportunity to improve quality of healthcare while reducing healthcare costs. The Healthcare Market in The US is roughly $2 trillion/year in 2006 and projected to reach $4 trillion (or 25% GDP) by 2015. Since the current trends are unsustainable; US and worldwide governments are "changing the game" by building National Healthcare Information Networks (NHINs), essentially bring eCommerce and automated manufacturing tools and techniques to healthcare.

There is a proliferation of diagnostic and therapeutic devices due to advances in computing, networking, sensing, and medical device technology. They have revolutionalized patient monitoring allowing small teams of nurses to monitor larger numbers of patients. They now extend to more active intervention including programmable infusion systems and surgical robots.

What is a Medical Device?
According to the Food and Drug Administration (FDA), a medical device is "any product (or portion of a product) that affects a patient's diagnosis or therapy of". In a recent 2008 FDA proposed ruling, *data communication or storage devices or networks that merely transmit or store patient data will become "medical devices". There is a s*trong movement now occurring inside and outside government to include a new class of "consumer health/medical devices" and associated communication, storage, and computing accessories" such as heart monitors used with treadmills as non-regulated, but still *partially valid*, sources of medical data. Low cost products suit Medicare plans to reduce costs.

Medical Device Incidents
Adverse medical incidents due to innovative technologies are estimated at 45,000 – 100,000 fatalities per year in the US and at 850,000 adverse events in the UK. (*C.W. Johnson, Univ. of Glasgow, 2002).* IOM/National Academies of Engineering report in 2005 for the healthcare market stated that errors are running at 2-3 Sigma levels and that medical errors are killing 70-100,000 patients each year.

The number of devices recently recalled due to hardware and software problems is increasing at an alarming rate. FDA Analysis of 3140 medical device recalls between 1992 and 1998 showed 242 (~8 %) attributable to software (FDA Guidance on Software Validation 2002) (79% of those caused by software defects introduced when changes were made to the software after initial production and distribution.). Of 23 recalls in 2007 that the FDA classified as life-threatening, three involved faulty software

"Research on medical errors suggests that the frequency and consequences of medical device use errors may far exceed those arising from device failures". (R Kaye and J Crowley, FDA Guidance on Human Factors and Use Error Risk Management, 2000). Recent FDA reports show that more than 1/3 of medical device incident reports involve use error, and more than 1/2 the recalls due to design problems can be traced to design of the user interface. (Comments from FDA Spokesperson at AAMI Conference, June 2005, Washington DC.)

State of Practice

The medical industry as whole does reasonably well in developing and approving stand-alone devices with moderate complexity, based on mature technology. However designing bug free code is difficult, especially in complex devices that might be used in unanticipated contexts. Large scale complex devices require extensive validation and certification. The development of high confidence medical devices has not kept pace with software assurance techniques practiced in other safety critical domains, due to time-to-deliver pressures and a shortage of properly trained software engineers. The number of medical devices to be networked and integrated is increasing significantly and there are no standards or regulations yet for their integration or interoperation. Medical devices are embedded not only in information networks but also in human patients; the design of medical devices must also include the devices interaction with the patient and the environment and the context in which they coexist. The development and certification processes effectively need to undergo a paradigm shift in order not to stifle innovation in medical devices.

What Standards Govern Medical Devices in the US?

Unlike Europe the FDA has no standards for medical devices. FDA chooses to regulate quality and safety by pre-market screening and post-market surveillance. The furthest FDA goes is to provide a few "guidance documents" for manufacturers:

- FDA 21 CFR 820 (Title 21, Code of Federal Regulations (CFR), Part 820) Medical Devices Quality System Regulation (QSR).
- FDA Final Guidance, General Principles of Software Validation : 2002.
- FDA Guidance for Off-the-Shelf Software Use in Medical Devices: 1999.
- FDA Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices: 2005.
- FDA Guidance, Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management: 2000.

AAMI, an industry association, develops consensus clinical, technical, and safety standards for specific medical devices like IV Pumps. AAMI is now "importing" European standards from IEC and other sources. IEC 60601 and some ISO standards cover European medical devices. Key medical device standards include:

- ISO 13485:2003, Medical devices—Quality management systems—System requirements for regulatory purposes
- ISO/TR 14969:2004, Medical devices – Quality management systems - Guidance on the application of ISO13485:2003
- ISO 14971:2007, Medical devices – Application of risk management to medical devices
- AAMI TIR32:2004, Medical device software risk management
- IEC 60601-1-4, Medical Electrical Equipment – Part 1 General Requirements for Safety, 4 Safety Requirements for Programmable Electronic Medical Systems
- IEC 62304:2006, Medical device software – Software life cycle processes

Standards have been established for best practices in human interface design and training techniques as follows:

- ANSI/AAMI HE74: 2001 Human factors design process for medical devices
- ANSI/AAMI HE48:1993 Human factors engineering guidelines and preferred practices for the design of medical devices

- ANSI/AAMI HE-75: 2008? *Human Factors Engineering -- Design of Medical Devices* (released for public review).
- ISO/IEC 62366:2007 Ed 1, Medical devices - Application of usability engineering to medical devices
- IEC 60601-1-6:2004 Medical electrical equipment - Part 1- 6 General requirements for safety: Collateral Standard: Usability.

Professional Responsibility Needs

People developing any safety critical software systems should be adequately trained in basic software development and they should understand their limitations. Software developers as responsible professionals have responsibility for minimizing the risk of failure and ensuring public safety and security. Certification of software safety engineers is becoming an increasingly important consideration in the development of safety-critical systems. Just as in other fields where the consequences of failure are very high, there is a need to ensure that practitioners are properly monitored by their colleagues, independent auditors and government regulators.