Assuring Confidence in Predictable Quality of Complex Medical Devices: Quality from a Customer Perspective

July 16, 2008

Rick Hampton
Wireless Manager
Partners HealthCare Information Systems
Quality from my perspective

- Quality means the devices operate as required, each and every time, in the same manner, each and every time. In other words; the device
  - Performs it's intended function
  - Responds the same each time
  - Fails “gracefully”
    - Gives the operator viable options for use
      - May required some type of work-around
    - Minimizes risk to the patient
Quality from my perspective

- Quality for networked devices should include some type of hazard analysis for hospitals to examine and include in their 80001 efforts
- Be prepared to work, to some degree, with each hospital
- For wireless networking, should consider:
  - Wireless Coverage
  - Security requirements
  - Frequency Coordination
  - Incompatibility problems
  - Network Architecture
  - Ongoing Support
  - Ownership of the verification & validation process

Uses of Wireless Devices

- Voice devices
  - Cellular telephones, wireless VoIP, hand-held radios
- Data devices
  - Laptop computers, PDAs, two-way pagers, RFID tags/readers, wireless LAN access points (APs)
- Integrated devices (RIM Blackberrys®)
- Real-Time Location devices
  - Active/passive RFID tags
- Medical Telemetry
  - WMTS and wireless LANs
- Accessory devices
  - Cordless headsets, keyboards, mice, printers, etc.
FCC Services Utilized

- ISM (Industrial, Scientific, Medical)
- WMATS (Wireless Medical Telemetry Service)
- PLMRS (Private Land Mobile Radio Service)
  - Public Safety
  - Bio-medical Telemetry
  - Industrial/Business
  - Private Land Mobile Paging
  - Radiolocation
- Paging
- MURS (Multi-Use Radio Service)
- FRS (Family Radio Service)
- GMRS (General Mobile Radio Service)
- MICS (Medical Implant Communications Service)
- Part 15
  - Medical Telemetry
  - RFID
  - Spread Spectrum
  - U-NII (Unlicensed National Information Infrastructure)
  - UWB (Ultra WideBand)
    - Medical Imaging
- Cellular Radio Service
- SMRS (Specialized Mobile Radio)
- AWS (3G) - Advanced Wireless Services Spectrum
- PCS (Personal Communications Service)
- Amateur Radio
- Private Operational Fixed Microwave

Wireless Application Map

7/23/2008
Overlapping wireless technologies in the 2450 MHz ISM band

- 802.11b/g
  - 2412
  - 2437

- 802.15.3
  - 2412
  - 2437

- 802.15.1
  - 2412
  - 2437

- 802.15.4
  - 2412
  - 2437

Non Interfering Sub Channels
Effective Management of Wireless

- Hospitals need to establish multi-disciplinary groups to define a wireless roadmap, assess technologies for appropriateness, and ensure implementation meets hospital standards for security and risk management.
- Hospitals need to identify a wireless manager who can ensure compatibility between medical devices and other wireless systems.
- Hospitals need to ensure vendors understand their environments are different than warehouses or offices.
- **Hospitals need to ensure vendors use systems that adhere to published standards. Failure to do so can lead to disruption of multiple systems.**

Converging Networks

- Many devices now operate on the wireless LAN with more coming.
- If the WLAN is planned only for coverage and does not address scalability or capacity issues, a large number of client devices can interfere with each other through network congestion.
- Though technically EMI, wireless network congestion is best managed through proper planning and implementation of WLAN concepts, not spectrum analyzers and frequency charts.
- Since the device manufacturer has no control over the IS wireless and wired LAN, it is prudent for the IS department to begin assessing and ensuring the extra level of reliability required by the addition of medical devices.
- It is IMPERATIVE that Clinical/Biomedical Engineering departments begin working with IS departments to address these issues.
IEC 80001 & Wireless Medical Devices

- **IEC 80001 Draft Standard – Title: Application of risk management for IT-networks incorporating medical devices**
  - Expected to be ratified in 2010
  - Addresses IT/Medical integration “head on”
  - Requires risk analysis and mitigation to be done on an ongoing basis for networked medical systems

### Relevant Players

- **Medical Device Vendor** (GE, Welch Allyn, etc.)
- **IT Network Vendor** (Cisco, Aruba, etc.)
- **Integration Risk Manager** (MGH, BWH, etc.)
Device Vendors Are at Apex

- The *medical device manufacture must initiate the process* – they must specify the characteristics of the IT networks on which they can safely operate
- The hospitals can’t do anything until they take this step
- The hospital then can demand the IT vendor provide specs & instructions on how to make their network perform to these requirements
- The hospital then needs to make sure the network is installed and maintained to these specs

IT Involvement Needed

- Several “subtle” issues must be worked out:
  - Wireless Coverage
  - Security requirements
  - Frequency Coordination
  - Incompatibility problems
  - Network Architecture
  - Ongoing Support
- IT and the medical device vendor must work together to ensure everyone is working with the same plan… and the sooner, the better.
Wireless Network Issues

- Security
  - Within medical systems themselves
  - Within the wireless LAN
  - Within the wired LAN

Wireless Coverage

- May require more coverage than anticipated
  - Patient Care Areas
  - Biomedical Engineering
  - Central Supply/Processing
  - Training Classrooms
Wireless Coverage Questions

- In what areas will your application/device/system be used?
- What signal levels are required?

Security requirements

- HIPAA compliance requires securing the entire network, not just one vendor’s application
  - Security must be built around the hospital’s needs, not those of the medical device vendor
- Two criteria determine wireless security
  - Authentication – ensures you allow only authorized users on the network
  - Encryption – secures sensitive data from prying eyes
Security requirements (cont.)

- Open
- WEP: Broken before it was released
  - EAP-styles: early Enterprise-grade (802.1x)
- WPA & WPA2
  - Enterprise-grade (802.1x)
  - WPA - Moderately strong encryption scheme
  - WPA2 - Capable of meeting FIPS requirements
- Multiple combinations, not all of which may be supported

Security Questions

- What is the architecture of your security system?
- What security protocol do you support?
- Are you willing to devote resources to WPA2 EAP-TLS?
Frequency Coordination

- Some medical device vendors want a wireless channel dedicated only to them… not practical
- Medical devices, computers, and bar code scanners can use different wireless protocol and may cause interference when in close proximity
- Most vendors focusing on 802.11b/g at 2.4 GHz – 3 non-overlapping channels
- Need to consider 802.11a at 5.8 GHz – 23 channels

Frequency Coordination Questions

- What frequencies and protocol does your system use?
- What are your requirements for sharing frequencies and bandwidth with other applications and devices?
- Do you have any special operational requirements?
- How does your system respond to interference or disrupted communications links?
Incompatibility Problems

- Current wireless standards are written for consumers, not enterprise healthcare environments
- Bluetooth Version 1.0 – notorious interferer
- 802.11n, Zigbee, Wibree, and other “standards” coming and not all may be useful in hospitals
- IT Manufacturers use proprietary features
  - May not be compatible with one another
  - Need to work with “generic” devices and be transparent

Compatibility Questions

- What standards are met by your system?
- What is the make and model of your wireless equipment?
  - Need technical specs
    - Output power, receiver sensitivity, etc.
- With which IT vendor’s equipment does your system work?
  - Manufacturer
  - Model
  - Software version
  - Specific settings
  - Peculiar failure modes
  - List other systems known to cause problems
Network Architecture

- Need to compare network architectures/diagrams between IT and medical device vendors
  - Many vendors want to operate only on their own “Virtual LAN” (VLAN)
    - Many individual VLANs may become a maintenance nightmare
  - Many medical device vendors want an unsegmented LAN to cover the entire campus
    - Large hospitals may require a segmented LAN for stability and robustness
- Need to get manuals beforehand to ensure IT can meet installation requirements

Network Architecture (cont.)

- Industry IT goals often do not take into account clinical/biomedical goals – conflict may result
  - VoIP, RFID, etc., may required different/conflicting wireless architecture (QoS, deployment, security, etc.)
- Consider installing “limited wireless” to get a flavor of challenges to be faced
Network Architecture Questions

- Describe your data and bandwidth requirements
  - How large are the packets you send?
  - How many packets to you send per unit time?
  - Do you send unicast, multicast, or broadcast packets?
  - Which protocol do you send, TCP or UDP?
- Describe your latency requirements
- Describe your reliability requirements
- Other requirements?

Ongoing Support

- Who will be responsible for server and anti-virus updates?
- How will you assess effects of IT network changes on these systems, especially when they incorporate real-time alarms or programming capability?
- Are there ongoing operational costs from Nursing, Biomed, or IT?
Wired Network Issues

- Wired Infrastructure Considerations
  - Medical networks & HIS networks usually separate
  - Wireless network = common element?
  - Need for increased reliability
  - Fail-over redundancy
  - Management tools to monitor capacity and quality of service

Regulatory Concerns of Wireless Medical Devices

- FDA does not yet regulate the IS LAN as a medical device.
- If connecting a medical device to the IS LAN adds functionality to the device, the LAN could become part of the device and additional regulatory requirements (510k) would likely be required.
- Since the device manufacturer has no control over the IS LAN, it is prudent for the IS department to begin assessing and ensuring the extra level of reliability required by the addition of medical devices.
Regulatory Concerns of Wireless Medical Devices (cont.)

- Software as a Medical Device
  - Wireless access has driven programmers to create more software for medical systems.

- Primary vs. Secondary Alarms
  - Makes sense from a regulatory approach
  - Do users expectations invert the definitions?

- Programming Control
  - Who enters programming parameters?
  - Who verifies programming parameters?

Regulatory Questions

- Software as a Medical Device
  - Is your system regulated by FDA?

- Does your system incorporate alarms or alerts?
  - How do you define the alarm or alert function? Primary or Secondary?

- Programming Control
  - Who enters programming parameters?
  - Who verifies programming parameters?
Contact Information

Rick Hampton
Wireless Communications Manager
Partners HealthCare System
One Constitution Center, OCC210
Charlestown, MA  02129
Office: 617-726-6633
Cell: 617-968-2262
RHampton@Partners.org