Risks, Challenges and Opportunities of Wireless Technologies in Healthcare: Wireless Testing in a Hospital

4-5 October, 2012, Herndon, VA

Phil Raymond
Wireless Architect, Philips Healthcare
Steven D Baker, PhD
Sr. Principal Engineer, Welch Allyn

Agenda

- Gap between medical device mfr (MDM) testing and hospital IT testing

- Using risk analysis in designing and testing a wireless Medical IT Network

- General Purpose IT Network → Medical IT Network
  - Why test
  - When to test
  - What to test
  - Where to test
  - How to test

Gap analysis: MDM & Hospital IT Testing

What an MDM can do

- Define system level performance specification (latency, traffic types, etc.)
- Characterize device and radio performance specification (QoS, security, etc.)
- Establish RF environment requirements (RSSI, SNR, etc.)
- Provide device specific intended use(s)
- Test to some specific WLAN vendor configurations

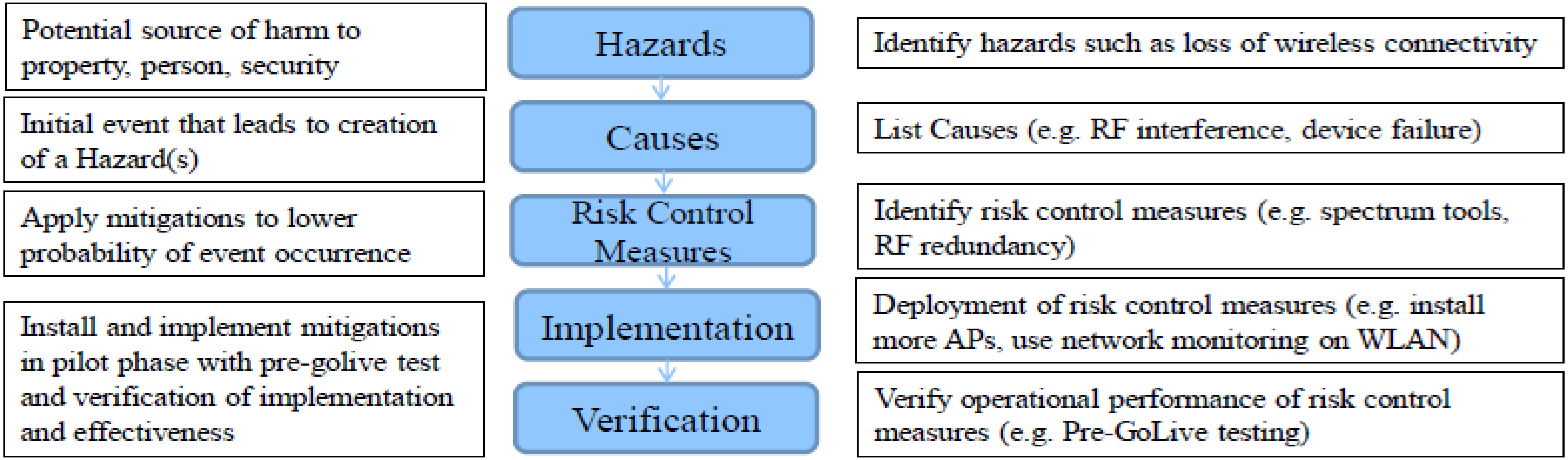
What an MDM cannot do

- Test to a specific hospital RF environment
- Test every network topology
- Create replica environment of hospital devices (co-existence)
- Test to every variation of WLAN vendor configuration (standard and proprietary)

What hospital IT should do

- Apply risk management umbrella within the design, deployment and management of medical IT network
- Understand clinical use, networking performance and characteristics of end devices
- Know your WLAN vendor (read the manual…)
- Test to hospital RF environment, network topologies, configurations, device coexistence

IEC/ISO/AAMI 80001-2-3: Risk Analysis Applied to Wireless Networks



RA Terms & Definitions		RA applied to WLAN
Potential source of harm to property, person, security	Hazards	Identify hazards such as loss of wireless connectivity
Initial event that leads to creation of a Hazard(s)	Causes	List Causes (e.g. RF interference, device failure)
Apply mitigations to lower probability of event occurrence	Risk Control Measures	Identify risk control measures (e.g. spectrum tools, RF redundancy)
Install and implement mitigations in pilot phase with pre-golive test and verification of implementation and effectiveness	Implementation	Deployment of risk control measures (e.g. install more APs, use network monitoring on WLAN)
	Verification	Verify operational performance of risk control measures (e.g. Pre-GoLive testing)

Risk management is a valuable tool in identifying the networking requirements of your hospital and the **best practices** and network management processes that are key in providing the medical IT network that meets these requirements

Wi-Fi Best Practices: www.wi-fi.org/knowledge-center/white-papers

Practical Example

From predefined risk acceptability criteria, our risk is High.

		Probability				
		Improbable	Remote	Occasional	Probable	Frequent
Severity	Catastrophic	🟨	🟥	🟥	🟥 High	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Medium	🟩	🟨	🟨 Moderate	🟨	🟥
	Low	🟩 Low	🟩	🟨	🟨	🟥
	Negligible	🟩	🟩	🟩	🟨	🟨

#	Hazard	Hazardous Situation	Cause(s), Contributing Factors	Harm	Initial Risk			Mitigation/Risk Control Measures	Reference to RO specifications, policies	Residual Risk		
					Severity	Probability	Risk			Severity	Probability	Risk
1	Delay in Treatment	Loss of alarm at Nurse Station	RF Interference	Minor or major injury, medical intervention required	High	Moderate	🟥 High	Spectrum monitoring, spectrum usage policies, device database mgmt				

Why Test

- Patient safety, clinical effectiveness, ePHI…
- Significant investment in hospital networks
- Even Congress gets it…
  - “Both FDA and FCC have publicly discussed efforts to make possible wireless “test beds” for the important purpose of better understanding how wireless health devices coexist in healthcare settings and advancing medical device interoperability. Please provide an update on these efforts…[†]”

[†] http://blackburn.house.gov/UploadedFiles/Letter_from_Congress_to_FDA_and_FCC_-_3Apr2012.pdf

When to test

- Changes to the network & devices
  - WLAN configuration
  - New device(s) introduction
  - WLAN physical layout
  - New construction (RF environment changes)
- Consider Risk Management as a tool to identify the "when"
  - If the RISK level is high and testing decreases the probability or severity of unintended consequences, then test
- Compare the difficulty in testing vs. the difficulty in recovering from network failure
- Examples:
  - Test failover recovery on a redundant controller

What to Test (1 of 2)

- Depends on what has changed (Risk Review)

- Include regression testing
  - Existing devices included for interoperability

- Both medical and non-medical devices
  - New VoIP devices added to hospital WLAN
  - WLAN vendor software upgrade
  - WLAN configuration changes (vendor recommended, QoS implementation, security upgrade to RADIUS)
  - APs added or AP location changed

- Interoperability between WLAN and Device configs

What to Test (2 of 2)

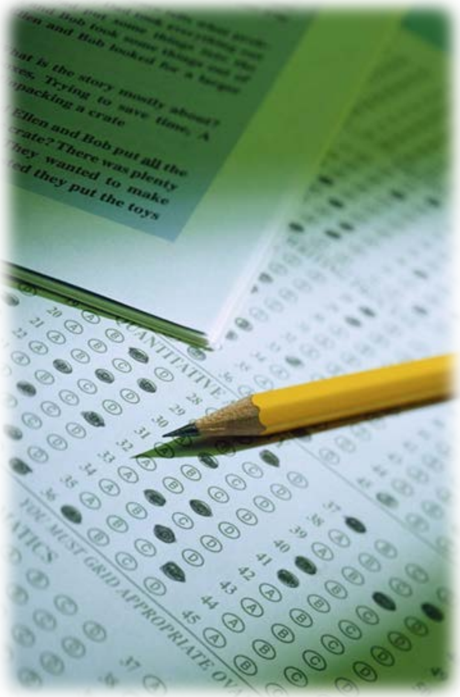
- Basic connectivity of all devices
  - Example. IT security certificates SNAFU
  - From device to server, not just “on” the network
  - Test procedures *are not just a set* of check boxes!
- Long-term operation
  - 24 to 96 hours
- Roaming or device handover
  - AP to AP, ward-to-ward
- WLAN Load
  - Particularly with new devices, test on single AP if not actual network

Where to Test

- Small clinic or IT network in a non-patient area of the hospital
  - Pros:
    - Isolated physically and logically: Eliminate direct risk of connected patients
    - Uses IT network configurations
    - Includes both medical and non-medical traffic
  - Cons:
    - Requires changes (adds, modifications) to IT network configuration
      - Consider a permanent test subnet/VLAN to mitigate this
    - May need to coordinate scheduling with IT and hospital admin
    - Test traffic pathways require definition: Routing, etc.
- A stand-alone lab
  - Pros:
    - Test when needed with full control over network configurations
    - Higher costs due to dedicated network
  - Cons:
    - Smaller network footprint (less network devices, less complex)
    - Device numbers not representative of IT network loading
- Use a phased approach
  - Isolated testing ⇨ IT network testing ⇨ live-patient, high-confidence testing

How to Test

- Not on patients! Most devices have demo modes, etc.
- Collaborative effort
  - In hospital – CE and IT
  - External to hospital – MDM and Network Mfr
- Understand device-level networking requirements
- Understand and duplicate current production configuration
  - Device config
  - WLAN config – duplicate hospital network configs
- Proper tools
  - Site survey tool (RSSI, SNR, Interference)
  - Wireless packet capture (wired too)
  - WLAN and device mfr built-in performance monitoring tools
- Test device, WLAN, configurations
  - Pre go-live



Summary: Building *your* test lab

- Risk Analysis: determine required testing
  - Closely emulate production network (PHY+L2/L3 boundaries)
  - Use network loading tools
  - Actual medical and non-medical devices
  - Client to server connections
  - Production network and device configurations
  - Implement and understand performance monitoring tools
- Organization! CE/Biomed and IT joint effort
- Follow industry & vendor specific best practices
- Document everything!
  - Device database
  - Consistent test protocols and reports

Thank You!