Assurance Cases for Medical Devices

"Integration of Safety and Security Risk and considerations for remote monitoring environments"

A presentation to the Assurance Case Workshop

Paul Hopkins & Mark-Alexander Sunjan
Warwick Digital Laboratory and Warwick Medical School

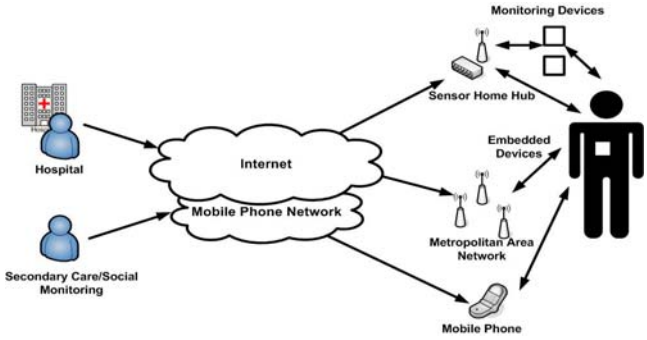
Date: 25th September

Contents

- A Scenario
- Issues
- Challenges

A Scenario

Consider the following 'fictional' & 'incomplete' scenario:



Issues: Risk Management Issues?

Who owns and manages the risk?

- Does ownership transition?
- What risk and why is it being managed (Security and/or Safety)?

How do they manage the risk?

- Large system?
- Multiple system users?
- Multiple Combinations?
- Unknown Provence of components?

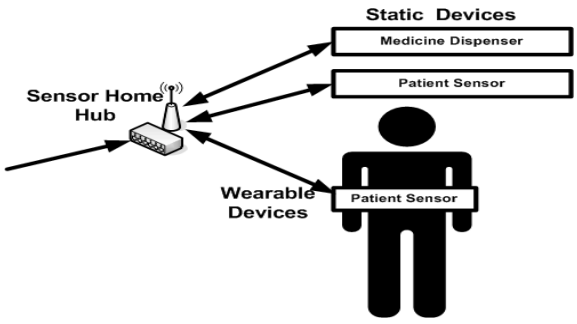
Risk Management: Where are we?

Manufacturers guidance is king.

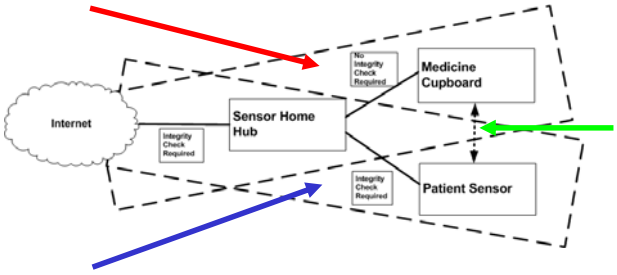
Standards

- IEC 80001: 2007 Application of Risk Management to IT networks including medical devices.
  - Process Framework that recognises the need but no guidance
  - Network Topology but what about software architecture/stack.
  - Leans on…..
- ISO 14971: 2007 Application of Risk Management to medical devices
- ….others embedded…

Another Example



Another Example: Issues



Ref: Concepts and Principles of Compositional Safety Case Construction: COMSA/2001/1/1; Tim Kelly , University of York

Options: 'Structured' Assurance Cases

Safety – number of 'critical' system examples using notations …..GSN

Security – very little 'evidence' of their use practically…

Integration of Safety and Security:

- DTI Forward: An investigation into system security requirements for next wave information provision services: (Creese et Al, QinetiQ, 2005)
- SafSec Methodology: integration of Safety and Security Certification (Praxis 2006)
- Unifying MANET Safety and Security. (Clark, Chivers, Murdoch, McDermid 2007)
- Combining Security and Safety Principles in Practice (Cockram and Lautieri, Praxis, 2008)

Potentially different (and the same) Issues

- Pre-operational Accreditation/Certification? More Dynamic?
- Scale of components (modules) & Number of permutations (modules)?
- Treatment of none technological methods (human performance/process)?
- Risk communication? (who is being convinced of what)?

Ref: Structured Assurance Cases: Three Common Standards: T. Scott Ankrum, Alfred H.Kromholz, Mitre, 2005

'Structured' Assurance Cases /cont

So there are potentially a number of existing/new issues:

1. Have we decomposed/constructed the modules or arguments at the right level?
2. Considering we have manufacturers guidance are they in a common vocabulary/ontology. Which elements are difficult to do – but critically need to be combined and understood (context and evidence?)
3. Other factors could get affected by the combination of systems – such as QoS – what if both take over half the bandwidth….its not only safety and security
4. How do we handle un-trusted components?

Challenges

1. What is the acceptability or success criteria of any methodology for assuring the safety and security of a medical system to the medical community (device's; ,integrators; operators, regulators)?
2. What techniques need to be developed for creating a security and safety assurance case specifically for a medical environment?
   - Dynamic v Lifecycle (Frequency of change)
   - Complexity v Modularity (Depth of analysis, Number of interconnections)
   - Communication & shared understanding of risk v timeliness (Audience)

How do these proposed techniques differ from those in other fields (nuclear, railways, etc)?

WDL Digital Innovation

Any Questions?