The concept of applying risk analysis tools such as failure mode, effects, and criticality analysis (FMECA) to the design and development process where human safety is a factor is nothing new to many industries such as nuclear power, aviation, and the automotive industry. Safety and reliability engineers are well versed in the implementation of risk management tools as critical components of addressing human safety in their product development process. The concept of applying risk management to medical information technology (IT) networks is the focus of ANSI/AAMI/IEC 80001-1:2010, and the focus on the wireless portion of the network—the weakest link—is within the draft of an IEC technical report (TR), Application of risk management for IT-networks incorporating medical devices—Part 2-3: Guidance for wireless networks.

The governance regarding the technology convergence of medical device connectivity and the IT network is still in its infancy. Generally speaking, the focus from an IT perspective is that networking IT professionals are not expected to be trained in the concepts of risk analysis of complex systems, nor are they fully aware of all the human safety issues associated with medical device connectivity. But that precisely what is occurring when connecting medical devices (including the connected patient) to the healthcare wireless network. The draft IEC TR 80001-2-3 provides the framework by which the concepts of risk analysis can be applied to the design, deployment, and management of wireless medical IT networks in healthcare.

This paper covers two topics related to wireless medical IT networks:
1. Some of the general challenges and solutions for the design and deployment stages of a wireless medical IT network
2. The fundamental principles of applying risk management during these stages as defined in the draft TR on wireless networks

**General Challenges and Solutions**

The rapidly increasing number and variety of devices being connected to networks within hospitals presents a significant challenge to network design, deployment, and management. From infusion pumps to smart phones, the challenge of supporting an exponential growth in the number of devices and the associated varying service level agreement (SLA) requirements is daunting from a wireless integration standpoint. Add in the complexity of managing patient safety and data security with devices that operate in a regulated world and the implications of meeting these challenges is increased significantly.

**Technology Options**

One of the first steps in evaluating risk in the deployment of medical IT networks is the choice of appropriate wireless technology. There are many technology options available including Wi-Fi, wireless medical telemetry service (WMTS), cellular, etc. Choosing the proper technology is dependent upon the...
devices themselves and what technology choices they offer, as well as the suitability of a specific wireless infrastructure to a hospital's needs. For medical devices today, the two dominant wireless technologies in hospitals are Wi-Fi (unlicensed spectrum) and WMTS (dedicated spectrum). WMTS infrastructure is generally deployed and managed by a medical device manufacturer and is considered to be more of a plug-and-play infrastructure that is dedicated to medical devices only. Wi-Fi technology is an IEEE standards-based wireless technology that provides a significant amount of bandwidth for supporting a large number of end devices. The risk-analysis considerations with planning, deploying, and managing a WMTS medical network are usually the responsibility of the medical device manufacturer and are not covered in this paper. The risk analysis of a Wi-Fi wireless network encompasses all lifecycle stages of the medical IT network and is the focus of this paper.

**Connectivity Challenges**

The use of wireless connectivity in hospitals has clear, multifaceted benefits. However, as is typical with any advanced technology, they do not come without integration, implementation, and management challenges. In brief, some of the high-level challenges faced in implementing a wireless medical IT network are:

- The increased usage of smart phones and tablet devices
- Minimal radio frequency (RF) design experience in the hospital IT/clinical engineering (CE) staff
- Use of crowded unlicensed spectrum (e.g. 2.4 GHz)
- Proprietary functions built on top of standards (e.g. 802.11)
- Securing data over the wireless link
- Formal organizational engagement between CE and IT

To properly design and deploy a wireless network requires expertise in not only networking protocols, but a host of other highly technical disciplines. A detailed discussion of these areas is beyond the scope of this paper, but they include radio-wave propagation, link-budget analysis, electromagnetic compatibility and interference, spectrum management, and the operational characteristics of radio communications protocol(s). Some types of equipment may also require knowledge of licensing regulations from the Federal Communications Commission (FCC) and radiation safety regulations from both the Occupational Safety and Health Administration (OSHA) and the FCC.

**Network Design and Planning**

It should go without saying that it is important to ensure the wireless networks will support those devices and applications necessary for the functioning of the hospital systems. Doing so requires cross-functional understanding within the hospital organization from senior management to the clinical and network engineering staff, in agreeing that the process of designing wireless medical IT networks is an exercise in compromise and risk management. Contrary to some beliefs, not all devices and systems are compatible with one another even though they are tested to a common standard. There are no real-world, one-size-fits-all solutions. Current technologies intended to automatically configure and manage networks, especially Wi-Fi networks, have been found to work fine in some environments, yet be quite problematic in others. Because the radio spectrum is a medium shared by all co-located users, there is a thin line between a successful wireless network and a shining example of “the tragedy of the commons.”

An early step in planning a wireless network design is to determine which devices and applications the network will need to support both today and in the future. For example, in small clinics and business offices, it may be acceptable to utilize the Wi-Fi network for all connectivity needs where the majority of devices are laptops running both clinical and general purpose applications. In a busy hospital clinical setting, such as an intensive care unit (ICU), the number and variation of networked devices in terms of networking performance capabilities and requirements may be too numerous to allow all connections to be...
wireless. In these cases, those devices requiring mobility should be wireless and the hospital should provision stationary devices with a wired connection (e.g., a device bolted to the wall). This is a good example of weighing the needs of a device's networking capability with that of acceptable risk.

In some instances, a wired connection to a stationary bedside patient monitor where there is remote physiological monitoring of a patient might be an appropriate risk-control measure. In other instances, such as an infusion pump that performs periodic library updates over the network, the use of wireless connectivity is acceptable if only to eliminate wires near the bedside because the needs of the wireless connectivity are not life critical. It is important to understand that these types of decisions around risk management are the responsibility of the healthcare delivery organization. When the data transport must be as reliable as possible, use a wired connection.

Wi-Fi has the ability to operate in two unlicensed bands of spectrum; 2.4 GHz (802.11b/g/n) & 5 GHz (802.11a/n). The 2.4 GHz (comprised of 83 MHz) spectrum is the home to many wireless devices, from Bluetooth headsets to cordless telephones (potential interferers). There is considerably more spectrum, or capacity, in the 5 GHz band (comprised of up to 555 MHz). Unfortunately, many Wi-Fi devices solely operate in the 2.4 GHz band with only three non-overlapping channels. For these reasons, it is a strong risk control measure to utilize the 5 GHz band for medical devices. Additionally, many hospitals are taking advantage of the increase in bandwidth with the use of 802.11n. One of the reasons why the bandwidth is increased is the ability to use 40 MHz channels instead of 20 MHz channel widths. However, this is not practically implemented in 2.4 GHz and requires the use of the higher number of available channels in the 5 GHz band.

**Network Deployment and Configuration**

It is expected that you will identify risk control measures during the process of evaluating the options and making a choice or wireless technology for medical devices and/or applications. For example, the medical device may have high bandwidth requirements so a technology such as Wi-Fi was chosen due to its high capacity. This is a simple yet accurate example of applying risk-control measures—a wireless technology was chosen that would provide extensive wireless capacity headroom. These risk-control measures can be carried into the risk analysis performed as part of the deployment and implementation phase.

Another important step in the deployment and implementation stage is to evaluate the desired RF coverage area for interference and access point (AP) placement planning. An up-to-date floor plan should be used to map out the area of coverage required for the medical devices. Take into consideration the RF needs of the wireless devices in that area (i.e., signal level and aggregate capacity), and perform a site survey in both bands (2.4 and 5 GHz).

WiFi uses a listen-before-talk mechanism to manage device access to the network. This means that all devices must follow specific rules when trying to access the shared wireless medium—one that grants fair and equal access rights to add devices.

This type of nondeterministic approach works fine when all devices adhere to the policy and there is an overabundance of capacity available, but it breaks down in cases of congestion when there are too many devices accessing the same AP. With no means of prioritization during periods of congestion, some or all of the devices trying to send traffic over the wireless link may experience periods where they lose network access due to RF collisions (i.e., the devices step on each other). For voice-over WLAN users, this is an inconvenience where voice quality will be reduced, but for medical devices relying on remote surveillance, this can lead to patient safety issues.

The proper implementation and configuration of QoS, or Wi-Fi multimedia (WMM), allows for certain medical devices and IP telephony to be given a higher probability of gaining access to the wireless medium before other, less critical devices. An analogy to better explain the operation of WMM is to consider an ambulance (the medical device) on a highway with sirens blaring where other vehicles (less critical devices) operate only in the slower lanes, leaving the fast lane for the ambulance.

A typical best practice associated with the deployment of a WLAN that is a good example of a risk-control measure is to deploy the WLAN such that devices can operate at the

**With no means of prioritization during periods of congestion, some or all of the devices trying to send traffic over the wireless link may experience periods where they lose network access.**
Managing Network Security Changes

**Project:** The IT department implements both an Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS) as part of a plan to improve network security, but does not include clinical devices in the listing of known, approved devices.

**Problem:** Over time, clinical devices show difficulty roaming. Eventually, these devices will connect to only two APs on the entire floor.

**Cause:** The medical device manufacturer (MDM) is contacted to resolve the issue and discovers that the two APs to which the devices connect are the only APs that respond to authentication requests. The MDM eventually discovers IPS/IDS was implemented just prior to the roaming failures. Solution was to add the clinical devices to the approved list.

**Recommended Practice:** Following the guidance of 80001, the hospital should have a listing of all intentional RF radiators, which would have also included the clinical devices. Additionally, the clinical engineering department would have been apprised of the change.

---Steven Baker and Ken Fuchs

---

Case Study: Managing Network Security Changes

**Project:** The IT department implements both an Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS) as part of a plan to improve network security, but does not include clinical devices in the listing of known, approved devices.

**Problem:** Over time, clinical devices show difficulty roaming. Eventually, these devices will connect to only two APs on the entire floor.

**Cause:** The medical device manufacturer (MDM) is contacted to resolve the issue and discovers that the two APs to which the devices connect are the only APs that respond to authentication requests. The MDM eventually discovers IPS/IDS was implemented just prior to the roaming failures. Solution was to add the clinical devices to the approved list.

**Recommended Practice:** Following the guidance of 80001, the hospital should have a listing of all intentional RF radiators, which would have also included the clinical devices. Additionally, the clinical engineering department would have been apprised of the change.

---Steven Baker and Ken Fuchs

---

**Hazards**

Identify hazards such as loss of wireless connectivity

**Causes**

List causes (e.g., RF interference, device failure)

**Risk Control Measures**

Identify risk control measures (e.g., spectrum tools, RF redundancy)

**Implementation**

Deployment of risk-control measures

**Verification**

Verify operational performance of risk-control measures (e.g., pre go-live testing)

---

Wireless Networking

The main hazards when using wireless devices connect to only two APs on the entire floor.

**Problem:** Over time, clinical devices show difficulty roaming. Eventually, these devices will connect to only two APs on the entire floor.

**Cause:** The medical device manufacturer (MDM) is contacted to resolve the issue and discovers that the two APs to which the devices connect are the only APs that respond to authentication requests. The MDM eventually discovers IPS/IDS was implemented just prior to the roaming failures. Solution was to add the clinical devices to the approved list.

**Recommended Practice:** Following the guidance of 80001, the hospital should have a listing of all intentional RF radiators, which would have also included the clinical devices. Additionally, the clinical engineering department would have been apprised of the change.

---Steven Baker and Ken Fuchs

---

**Hazards**

Identify hazards such as loss of wireless connectivity

**Causes**

List causes (e.g., RF interference, device failure)

**Risk Control Measures**

Identify risk control measures (e.g., spectrum tools, RF redundancy)

**Implementation**

Deployment of risk-control measures

**Verification**

Verify operational performance of risk-control measures (e.g., pre go-live testing)

---

**Risk Management**

Figure 1 provides a flowchart outlining the application of risk management in medical IT networks as defined in the draft IEC technical report on wireless guidance. Note that not all steps in the risk-analysis process are outlined here as the technical report and this paper are only concerned with the steps focused on the wireless aspects of the medical IT network. For more information, please see IEC 80001-2-1 Step by step risk management of medical IT-networks; Practical applications and examples.

**Hazards in Wireless Connectivity**

The main hazards when using wireless
technology to connect medical devices to networks are the loss of and/or the impairment of connectivity. When the clinical functionality of a device is dependent on the connectivity aspects of a network and the connectivity is lost or impaired, the patient safety and clinical efficacy may be exposed to higher-than-acceptable levels of harm and degradation, respectively. The risk analysis as outlined in this paper focuses on the causes that can lead to the loss or impairment of the wireless link, and the applicable risk-control measures that can be implemented to reduce the probability of hazard occurrence.

There are many “causes” that can create a hazard, some of which were reviewed in the opening sections on design and deploying a WLAN. Each hospital will create its own unique list of causes as part of their risk-management process.

**Risk-Control Measures**

Risk-control measures as applied to wireless networks can be technical (wireless design concepts) or process related (e.g., change control, clinician step-by-step actions during network outages).

The following are a few examples of wireless network risk analysis identifying potential causes and associated risk-control measures. It is not an exhaustive list and does not cover every potential cause and risk-control measure. They may not be applicable in each case or every hospital.

- **RF Interference**
  - **Cause:** As outlined in “Wireless Medical Systems: Risks, Challenges and Opportunities”—another paper in this issue of Horizons—there are many potential sources of electromagnetic interference, which make the identification and implementation of risk-control measures a significant challenge. Microwave ovens, cordless telephones, and Bluetooth radios all operate in the 2.4 GHz band and can impair the performance of devices in proximity. Many motors have spark-gaps and emit broad-band RF interference.
  - **Risk-Control Measure(s):** Locate and identify sources of RF interference that can be removed or eliminated through the initial, periodic, and real-time use of spectrum management tools to gain visibility into the RF space in a hospital. As mentioned earlier, the use of 5 GHz (802.11a/n) for medical devices is a strong risk control measure.

- **Network Capacity Overload**
  - **Cause:** Overutilization of the AP can be blamed on multiple factors, including too many devices sending traffic at the same time, a single device usurping all available capacity, abuse of certain protocols such as broadcast messaging, and reduction in expected capacity due to poor channel planning or adjacent networks.
  - **Risk-Control Measure(s):** Due to the many causes of capacity overloading, the risk-control measures are at least as numerous.

---

**Case Study**

**Massager Breaks Telemetry System**

**Project:** New foot massager is purchased

**Problem:** VHF telemetry system fails intermittently for patients near the nurse station.

**Cause:** Analysis found the failures correlated with use of the foot massager that was located at the nurse station and that the massager was not working properly. It was emitting considerable electro-magnetic interference in the WMTS (FCC allocated band for medical telemetry) band that the telemetry system was using. Solution was to replace the foot massager.

**Recommended Practice:** While it would be difficult to prevent this situation from occurring, the hospital should maintain a list of emitters and their baseline spectrums. If one of these devices fails in such a way that its emissions increase, the biomed department can more easily find the potential culprits.

—Steven Baker and Ken Fuchs

**Case Study**

**Managing Wireless Infrastructure Firmware Upgrades**

**Project:** IT receives a security advisory from the infrastructure manufacturer and immediately schedules an upgrade for the controller and AP firmware.

**Problem:** Nurses report that their devices are neither communicating with central stations nor IT applications.

**Cause:** During the upgrade time of 30 minutes, the Wi-Fi network and all wireless communication are unavailable. The nursing staff was not apprised of the change.

**Recommended Practice:** Systems supporting clinical systems are never taken offline without notice. The security risk of not upgrading would be compared against the clinical risk of a down network. Prior to the upgrade, confirmation of verification testing for compatibility with all critical systems should be made, or at least assess the risk of not having that testing. Part of the infrastructure purchase review would have included the risks associated with firmware upgrade. A 30-minute upgrade solution would likely require a staged upgrade and perhaps a different solution with faster upgrade would have been selected.

—Steven Baker and Ken Fuchs

© Copyright AAMI 2011. Single user license only. Copying, networking, and distribution prohibited.
Case Study
Managing Infrastructure Firmware Updates

**Project:** IT department upgrades the firmware level on their wireless controllers and APs based on the recommendation of their wireless infrastructure manufacturer.

**Problem:** Clinicians notice periodic loss of data.

**Cause:** Investigation reveals the updated firmware has the APs changing channels as fast as every 10 seconds, forcing clients to roam unexpectedly. The wireless infrastructure manufacturer indicates that channel switch announcement should be enabled, but that makes things even worse. Further investigation shows the APs send a de-auth packet when clients re-associate after the channel change. Solution was to increase the minimum channel dwell time.

**Recommended Practice:** Applying 80001, the risk manager would have included the clinical team in the risk analysis and preferably indicated the risk of upgrading was high and should only be done after clinical validation testing is complete. The AP vendor would have been asked and disclosed the changes in function and these would be presented to the medical device manufacturers for review.

—Steven Baker and Ken Fuchs

Case Study
Managing Wireless Infrastructure Features

**Project:** Wireless infrastructure vendor convinces IT to start using the automated radio manager feature to manage the power levels and channel selection of their APs.

**Problem:** Nurses start to notice that the waveforms from their 802.11 based wireless devices have gaps.

**Cause:** The MDM traces the gaps back to the radio manager feature as this puts the APs into an offline state to scan other channels for short periods of time, during which real-time data are not received. The MDM found this problem during verification testing and developed a solution with the AP manufacturer to hold off the scanning, but hold-off feature was not enabled.

**Recommended Practice:** The potential of features such as rogue AP detection or automatic channel and power allocation to create issues for medical devices is well known and covered in the IEC 80001 Wireless TR. A risk analysis should be performed to learn the side effects of using features before implementing those features.

—Steven Baker and Ken Fuchs

Examples include the overprovisioning of network capacity (dense AP deployment in 5 GHz), setting up alert notifications when capacity thresholds are exceeded (thresholds that are set at levels before congestion occurs), and the proper use of QoS, or WMM, to provide higher probability of medical devices accessing the network over less critical devices.

- **Access Point Failure**
  - **Cause:** Hardware failure
  - **Risk-Control Measure(s):** Create RF redundancy in 5 GHz where AP coverage is allowed to overlap, but on different channels. If an AP fails, there is RF failover since another AP can provide connectivity in that physical area, albeit on another channel.
  - **Network outage (1)**
    - **Cause:** Infrastructure software upgrade and even a planned network upgrade can lead to extended or unexpected network outages.
    - **Risk-Control Measure(s):** Implement change control procedures where clinical engineering is involved in the planning and execution of network software upgrades. Possibly add IT and nursing staff to provide real time, onsite support during the time of network outage.
  - **Network outage (2)**
    - **Cause:** During initial deployment or updating WLAN or device configurations, incompatibilities between new configurations and networking components or ancillary devices can lead to network outages.
    - **Risk-Control Measure(s):** Study vendor-specific manuals (this is not putting together a bicycle) and verify new configurations in a pre go-live network. Establish a working relationship with the networking vendors and medical device manufacturers to understand and become aware of any compatibility testing that may have been done previously, and to share the planned introduction of new devices and their required or recommended network configurations.

**Summary**

When implementing medical devices on a wireless network, the safety, efficacy, and security of the medical devices are paramount. Close coordination between the hospital, device manufacturer, and IT vendor is required to ensure the infrastructure is installed and configured to properly support the intended use of the medical device.

If conflicts are found to exist between the medical device and another application, the hospital should determine if a separate network for the medical device or conflicting application is appropriate. This separate network could entail using a different technology or partitioning the radio spectrum to obtain sufficient frequency separation to avoid interference. The medical device might be able to utilize the...
If conflicts are found to exist between the medical device and another application, the hospital should determine if a separate network for the medical device or conflicting application is appropriate.

Wi-Fi technology provides many features and capabilities that allow for a converged network. But the many challenges associated with a converged network along with the implications of patient safety and data security require the application of industry-proven tools—such as risk management as outlined in IEC 80001-1:2010 and the upcoming technical report on wireless guidance—to ensure that the network can support the many and varied networking performance requirements of medical and nonmedical devices. 

Case Study
Managing Changes in Network Configuration

Project: A hospital IT department changes network topology from a flat network to having different subnets in each building. They enable IP mobility to support roaming across subnets.

Problem: Clinicians notice data loss, particularly for ambulatory patients, and the MDM is asked to investigate.

Cause: The MDM network specialists discover a nonvalidated configuration. They and the infrastructure provider test and find that EAP-authenticated fast roaming does not work when IP mobility is enabled. Solution was to disable IP mobility until the infrastructure vendor fixes the bug and MDM validates the new build.

Recommended Practice: Under 80001-1, the network change would be documented and the clinical department apprised of the change. A risk analysis would indicate that the configuration isn’t supported by the MDD. If the hospital chooses to go forward with the change, a recovery plan would be in place, and upon detection of degraded performance, would have been used.

—Steven Baker and Ken Fuchs

Don’t just be inspired.

Be the Inspiration!

Expanding the horizons of clinical engineering practice since 1990

Learn more about our activities and membership programs at http://www.accenet.org