Wireless Systems and Alarm Management

Jim Moon

About the Author

Jim Moon is chief technology officer with Sotera Wireless, Inc. E-mail: jim.moon@soterawireless.com

A Helpful Resource

For clarity on any of the acronyms or terms used in this article, please see the glossary on page 46.

The advent of portable wireless devices presents both opportunity and risk. The available technology permits patient-worn monitoring devices to communicate with central monitoring stations, electronic medical record (EMR) systems, and portable devices carried by the clinical team. People have become accustomed to receiving an e-mail at any time and any place through their smartphone. Why shouldn't that same remote notification be available for patient monitoring systems?

For the medical device manufacturer to create competitive products that utilize modern networking technologies, this means the addition of new engineering skills that are not traditionally associated with biomedical device design. New manufacturing test methodologies and facilities also become critical to the reliable production of wireless devices.

For the hospital biomedical engineer, wireless medical devices require a new level of technical product evaluation and understanding of both wireless network technology and their facility's network infrastructure. The demands of wireless medical devices place new requirements on the coverage and performance of the wireless network. The infrastructure that supported clinical charting and data access functions may not be suitable for real-time monitoring, especially for ambulatory patients.

Wireless networks are inherently unreliable as compared to hard-wired networks. Many factors well beyond the scope of this article contribute to errors in transmission that occur routinely on wireless networks. The mitigation of those factors to provide a successful wireless solution involves design considerations at the physical, data link, transport, session, and application layers of the system design. While this article focuses on providing a healthcare delivery organization (HDO) a list of questions to ask medical device manufacturers, there are questions an HDO should ask of itself that address the physical layer. For example, consider the case studies included with this article, where the installation process failed to adequately consider the risks to alarm distribution when making changes and additions to wireless networks.

Good design at the lower levels of the stack involves resources that go well beyond those of most medical device companies. As a result, medical device manufacturers need to work closely with the semiconductor and wireless systems suppliers that serve the much broader wireless network industry. The implementation of those technologies within the medical device, however, is still a key design element. The choice of standards such as those for quality of service (QOS) and encryption is an important consideration both from a communications reliability perspective, and also from an information security perspective. The chosen technology must "play well with others" if it is expected to integrate well with other wireless systems in a hospital environment.

There are many standards that apply to

various aspects of wireless devices to verify the device's ability to deal with conducted and radiated electromagnetic interference (EMI), and to ensure that the device is neither affected by or interferes with other equipment. The standards that apply to many of the critical wireless communications details at the data link, network and transport levels, however, are either found in the Institute of Electrical and Electronics Engineers (IEEE) 802.11x standards, or in industry standards that are still weaving their way through the formal standards committees and industry approval process.

One of the best ways to ensure compatibility in a network environment that serves more than one application is to certify a device to the Wi-Fi Alliance testing standards. This suite of tests verifies that an 802.11 device adheres to the network protocols for association/disassociation with wireless access points, roaming from access point to access point, establishing and managing QoS, encryption key exchange, and a myriad of other network protocol details to ensure that the radio in the device under test is functioning correctly, and to reduce the probability that it will impact the operation of the network or other 802.11 devices. At the present time, the Wi-Fi Alliance, an industry-sponsored standards certification organization, has the only comprehensive methods to verify the network protocol performance of a device.

Even when all of the factors mentioned above have been designed into and verified in a medical device, there are still aspects of the application layer that must be carefully designed to ensure reliable system operation and patient safety. Careful separation of primary and secondary alarm subsystems and synchronization of information across the network are critical considerations. The evaluation of an alarm system design in a wireless medical device should include the following considerations:

1. Are primary alarm algorithms always located in the device at the patient? Alarm thresholds, recognition, activation, delays, prioritization, suspension, and reactivation should reside at the patient-connected device and require no network connection for proper operation.
2. Is the network connection required for the device to recognize an alarm condition or event and initiate a local audible and/or visual alarm or alert?
3. Is the network communication protocol appropriate for the nature of the information to be communicated? High-data rate, noncritical information, such as an SpO2 plethsymograph waveform, could utilize user datagram protocol (UDP) data transport to minimize device and network overhead. Critical communication, such as an alarm notification or patient-to-device association information, should ensure messages are received, and this may be achieved through use of a protocol such as a transmission control protocol/internet protocol (TCP/IP) and have an appropriate QoS to ensure reliable, timely end-to-end packet delivery or notification of failure. Network parameters and device software performance must be well understood and verified to meet the system requirements.
4. Is the patient-located device always aware of its network connection status? Loss of a network connection should not delay the activation of an alarm or the secondary notification if the network connection is restored during an alarm event.
5. Do alarm/alert strategies that utilize the network to activate remote secondary alarms to minimize patient discomfort and distur-

Case Study

Managing Interference

Project: A hospital CIO mandates use of a distributed antenna system (DAS) to support enterprise-wide wireless VoIP (i.e., wireless telephony) that is used to relay clinical alarms

Problem: After installation, staff complains that the wireless phone system is not working well on one floor and alarms are not being reliably transmitted. Further, there was no escalation of alarms.

Cause: The IT department discovers that the biomedical department has a 2.4 GHz Frequency Hopping Spread Spectrum (FHSS) system installed. Moreover, the DAS runs adjacent to the FHSS Access Points (APs) and the DAS efficiently conveys all the FHSS transmissions to the 802.11b/g APs. Solution was to move the DAS to a distance of 3-m from the FHSS APs.

Recommended Practice: By following 80001, the CIO would consult with the risk manager before making such a mandate. The risk manager would have a list of all intentional radiators and alert the DAS installation team to work with the telemetry system manufacturer to mitigate interference risk. The DAS would have been installed with 3-meter separation from the FHSS APs and not presented issues. The patient risk due to no alarm escalation would have been noted and mitigated if the risk level was too high.

–Steven Baker and Ken Fuchs

bance include positive acknowledgement of receipt of the information by the remote device? Users must be able to acknowledge the alarm or alert, and safe timeout mechanisms must be in place to revert to local audible/visual notification if the alarm or alert is not acknowledged by the remote user in a reasonable period of time.

6. Do the devices respond appropriately if the network connection status changes at any time during an alarming sequence, and revert to local primary alarms if needed?
7. Do remote displays of alarm thresholds always obtain a fresh copy of those thresholds over the network from the device? Will the remote display update automatically if the threshold is changed at the bedside?
8. Are changes to alarm thresholds from a remote location implemented as a "change request" that must be communicated to the device at the patient, confirmed by the patient device as properly formatted and within range, and returned to the remote location as confirmation that the new threshold is then in effect? Until such return confirmation, the remote display should not indicate to the user that the threshold has been changed.
9. Do indications to a user that an alarm has been acknowledged require round-trip confirmation over the network that the patient device has received the alarm acknowledgement? How does the secondary device respond if the confirmation fails?

Design of alarm-management systems that utilize the benefits of wireless networks must be based on the premise of an imperfect network.

The alarm-system design requires that all of the possible state combinations of both the local and remote nodes of the system be accounted for and have proper state transition criteria. The state definitions must also account for those states that result from network transit and error recovery delays. The verification and validation testing of the system must ensure that all of the state combinations have been dynamically exercised.

Network reliability issues are a fact of life. Good network design and management can create a system that serves the needs of its users with a high degree of reliability. However, it must always be recognized that networks fail, and that they fail in a wide range of ways, and often at an inopportune moment. Design of alarm-management systems that utilize the benefits of wireless networks must be based on the premise of an imperfect network. The design, verification and validation of alarm-management systems must ensure that in all cases of network error or failure, the alarm is properly annunciated and that misleading information is never displayed at remote locations. ■

Case Study

Too Much of a Good Thing

Project: Hospital installed a wireless network over multiple floors. Over time the number of access points increased and the power level on some APs was also increased to improve coverage.

Problem: After some time, users reported that the wireless network seemed "slow" and devices sometimes took a long time to connect. Investigation revealed that distribution of patient alarm conditions was unreliable.

Cause: IT investigated and found that it did not have current documentation of the wireless infrastructure. After updating the map of AP locations and configurations they found that the AP density was too high, especially given the power level settings. This resulted in a situation where the amount of beacon traffic was so high that normal communications were severely affected, despite all the APs having a Wi-Fi certification. Solution was to decrease transmit power and AP density.

Recommended Practice: According to the best practices outlined in IEC 80001, the wireless network is maintained under configuration control. Any changes are analyzed carefully and tested if possible to ensure that the integrity and performance of the network is not degraded.

–Steven Baker and Ken Fuchs