WHITEPAPER

Overcome Wi-Fi connectivity challenges for medical devices in hospitals and medical institutions

www.infineon.com

Solve common Wi-Fi integration and field deployment issues while achieving high security levels, reducing latency and maintaining facility coverage

Overview

Wi-Fi plays a crucial role in modern healthcare, enabling efficient communication, patient monitoring, and data management. In non-stop, chaotic and unpredictable environments, such as hospitals and other medical institutions, Wi-Fi networks must provide robust, secure, and reliable connectivity around the clock for medical devices to meet the critical demands of healthcare operations.

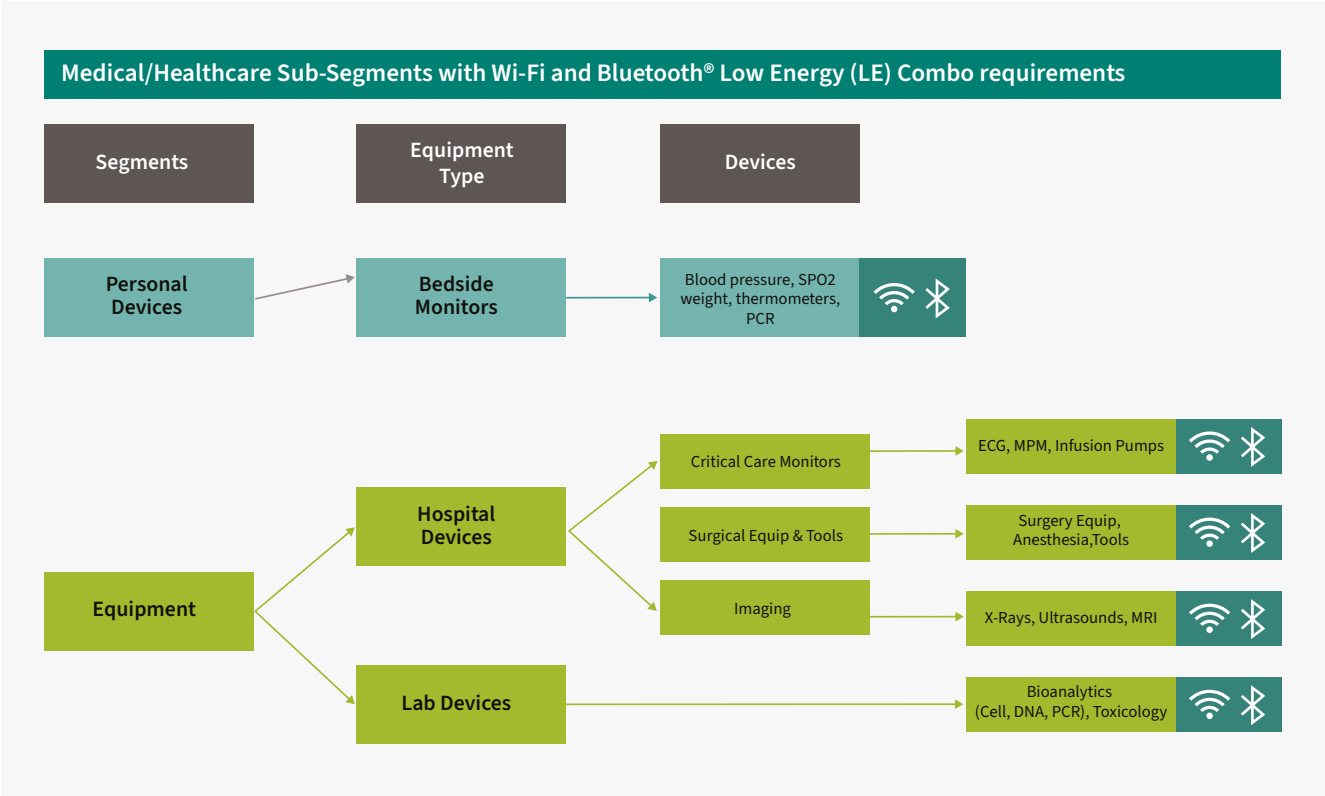
These healthcare facilities deploy enterprise-grade Wi-Fi solutions consisting of multiple access points throughout the facility to achieve secure, seamless coverage for handling many simultaneous device connections and for prioritizing network traffic to ensure that critical applications and devices receive the necessary bandwidth to function without interruption.

As a result, medical device manufacturers who serve hospitals and other medical institutions must figure out how to support a wide variety of Wi-Fi network infrastructures, security types and network configurations. Having the right Wi-Fi connectivity solution helps.

This whitepaper walks you through the environment, considerations, and key challenges medical device makers face when developing and implementing medical equipment for hospitals and other medical institutions, how to solve these challenges, and how to pick the right Wi-Fi solution to ensure optimal patient care and staff satisfaction in these environments.

Medical Devices Use Case Important Consideration

To ensure that a medical device operates effectively on many Wi-Fi networks in healthcare facilities, the Wi-Fi use case of the medical device must be considered. For instance, wearable medical devices and bedside monitors use Wi-Fi to continuously stream patient data to centralized monitoring systems, allowing for timely interventions. Medical imaging devices, like MRI or CT scanners, use Wi-Fi to transfer large data files to electronic health record (EHR) systems, facilitating quick access to patient information.



Key Wi-Fi Challenges

The use of Wi-Fi in hospitals and medical institutions presents several challenges, due to the high number of connected devices, interference issues, roaming issues, latency concerns, and power consumption in battery-operated and mobile equipment.

1. High Device Volume degrades network performance

Hospitals have a dense network of devices connected to Wi-Fi, including smartphones, tablets, medical carts, infusion pumps, patient monitors, and more. This high device density leads to significant radio frequency (RF) interference and congestion, especially in the 2.4 GHz band, which is used by many Wi-Fi, Bluetooth®, 802.15.4, DECT devices and microwave ovs. The congestion and interference can degrade network performance, causing delays in data transmission, dropped connections, and poor signal quality. In critical healthcare settings, such delays impede timely access to patient data or disrupts the operation of essential medical equipment, potentially affecting patient care.

To improve Wi-Fi network and device performance, many hospitals are requiring Wi-Fi devices utilize the less-congested 5 GHz band. As hospitals install the latest Wi-Fi infrastructure that supports Wi-Fi 6E, which supports the new 6 GHz band, they also will want medical devices to support this new band.

The high device volume and network congestion also results in increased latency, which in turn causes delays in data being sent or received over the network. For real-time applications, like patient monitoring, telemedicine, or remote surgery, low latency is critical. Any delay in data transmission could have serious consequences, such as delayed alerts for patient conditions or interruptions in the flow of vital information between healthcare professionals. Managing network traffic through Quality of Service (QoS) settings is one approach, but it requires careful planning and the devices on the network do the appropriate packet tagging to ensure their packets are prioritized appropriately.

2. Medical Device Battery Drain

Portable monitors, infusion pumps, and wearables are battery-operated and rely on Wi-Fi for connectivity. Constantly searching for and maintaining a Wi-Fi connection can drain device batteries, leading to shorter operating times and more frequent charging. In healthcare environments where uninterrupted operation is critical, advanced power

management strategies, such as optimizing Wi-Fi settings for low power consumption, can mitigate this issue. These strategies often reduce performance or connectivity though. It is best if medical devices integrate a Wi-Fi solution that allows for changing these settings and them exposing them for in-field device technicians to be able to change the settings.

3. Many Security Concerns

Security is a significant challenge when implementing Wi-Fi in hospitals and other medical institutions given the sensitive nature of healthcare data and the critical role that connectivity plays in patient care. There are six key security concerns: Access control, network segmentation, device vulnerabilities, legacy systems, insider threats, and regulatory compliance requirements.

Access control

Hospitals handle vast amounts of sensitive data, including patient health records, which are protected under regulations like HIPAA in the United States. Wi-Fi networks must be secured to prevent unauthorized access to this data. If a Wi-Fi network is compromised, it could lead to data breaches where patient information is stolen, exposing the hospital to legal penalties and damaging its reputation. Security standards, such as WPA3-Enterprise, are essential to protect data transmitted over Wi-Fi, but they must be implemented correctly and consistently across all devices and networks.

Network segmentation

Hospitals must ensure that only authorized devices and users can access their Wi-Fi networks. However, with a diverse range of devices, including personal smartphones, medical equipment, and IoT devices, managing access control becomes complex. Weak or poorly managed authentication methods can allow unauthorized users to access the network, potentially leading to data theft, network disruption, or even direct attacks on connected medical devices. Hospitals must implement strong authentication protocols, such as 802.1X, specified in WPA2-Enterprise and the latest WPA3-Enterprise, to enhance security.

Device Vulnerabilities by Insiders and Outsiders

Many medical devices connected to Wi-Fi are not designed with strong device security features, making them potential entry points for attackers. These devices often have outdated software, hardcoded passwords, or lack the ability to receive security updates, making them susceptible to exploitation. If compromised, a medical device could be used to launch attacks within the network, steal data, or even interfere with patient care by insiders or outsiders. Device manufacturers need to ensure that their connected devices meet stringent security standards and are regularly updated to address known vulnerabilities.

Legacy Systems

Many hospitals operate with new and legacy medical devices, some of which were not designed to connect to modern Wi-Fi networks. Customizing older devices to be Wi-Fi compatible may require additional hardware, such as wireless adapters, or software modifications, adding another layer of complexity. Custom solutions might be necessary to bridge the gap between old and new technologies.

Regulatory Compliance

Medical devices can be subject to stringent regulatory standards set by the U.S. FDA or the European Medicines Agency (EMA). These regulations (e.g. FDA's 510(k) and EU's MDR) often require that any connectivity on the device, including its Wi-Fi capabilities, must not compromise the device's safety or efficacy. Integrating a device's Wi-Fi functionality, therefore, involves rigorous testing and validation to ensure compliance with these regulations.

Help Is Here

The Ezurio Sona IF513 WiFi 6E + Bluetooth® 5.4 module, powered by the Infineon Technologies AIROC™ CYW55513 chipset, addresses Wi-Fi interference by utilizing advanced technology and spectrum management. By operating in the 6-GHz band, Wi-Fi 6E significantly reduces interference since this band is less crowded compared to the traditional 2.4- and 5-GHz bands.

This expansion also reduces congestion and minimizes overlap with Bluetooth®, which mainly operates in the 2.4-GHz band. The chipset employs coexistence algorithms to manage the 2.4 GHz spectrum, ensuring that Wi-Fi and Bluetooth® signals do not interfere with each other. Techniques like Adaptive Frequency Hopping (AFH) in Bluetooth® 5.4 help avoid Wi-Fi channels, dynamically reducing interference.

Wi-Fi 6E's use of Orthogonal Frequency-Division Multiple Access (OFDMA) and error-correction coding improves spectrum efficiency and data integrity, mitigating interference and enhancing communication reliability. Lastly, the module features optimized antenna placement and tuning, further reducing physical interference between Wi-Fi and Bluetooth® signals.

Rest assured that the robust Wi-Fi 6E + Bluetooth® 5.4 solution goes beyond the Wi-Fi 6/6E standard to offer extended range and reliable connectivity for medical devices no matter where they are—inside or outside the buildings—around the clock. The devices also support Bluetooth® and Bluetooth® Low Energy (LE) Audio along with LE Long Range, which are important technologies enabling the latest audio headset applications as well as for connecting sensors and trackers over a wide coverage area.

The combo device consumes very low power in both active and standby modes, which keeps battery-operated equipment and mobile units lasting longer in critical use cases. Also contributing to power savings is the high-performance transmitter and receiver with (aforementioned) interference mitigation technology. This robust radio design reduces wireless retransmissions which needlessly increase active airtime and waste battery power.

When it comes to the extended device lifetime, the module partner, in this case Ezurio, would manage the device availability beyond the lifespan of the silicon, and would extend device support to offer the 10+ years that are generally needed for the applications discussed here. It does this by understanding the needs of the device maker as well as the realities of the silicon partner and makes "last-time" buys.

Reduce Delays for Medical Devices in Healthcare Facilities

Latency and throughput are critical issues when using Wi-Fi in hospitals or medical devices due to the need for real-time, reliable data transmission in healthcare environments. For example, low latency is crucial for real-time monitoring of vital signs. Delays can lead to late responses to critical changes in a patient's condition, potentially endangering lives. High latency can disrupt the transmission of large medical images, potentially affecting diagnosis and treatment decisions.

The AIROC™ CYW55513 chipset addresses the described latency and throughput problems through a combination of advanced hardware and software features. By operating in the 6-GHz band, it offers additional channels and wider bandwidths, which reduce congestion and increase throughput. Its Multi-User MIMO (MU-MIMO) feature lets the chipset handle multiple devices simultaneously without compromising speed, crucial in environments where numerous medical devices require real-time connectivity.

On the software side, the chipset also uses OFDMA to allocate resources more efficiently by splitting channels into smaller sub-channels. This reduces latency by allowing more devices to communicate simultaneously without interference. In addition, advanced co-existence algorithms manage spectrum sharing, especially in the crowded 2.4-GHz band, minimizing interference between Wi-Fi and Bluetooth® signals. And integrated QoS mechanisms can prioritize critical data, such as patient monitoring signals, over less important traffic, ensuring low-latency communication where it matters most.

A Complete Package

The availability of technical support, support for Linux, Android, and RTOS drivers, software tools like ModusToolBox™ Software for Embedded Bluetooth® and Bluetooth LE Audio development and Premium Wi-Fi Advantage that come bundled with or leverage the CYW55513 chipset are crucial for the success of the medical facility's Wi-Fi deployment.

Ezurio's Premium Wi-Fi Advantage provides access to advanced features and optimizations that improve Wi-Fi performance, including enhanced security, better spectrum utilization, and advanced network management. In hospitals, this ensures reliable and secure connectivity, which is essential for protecting patient data and maintaining operational efficiency.

When it comes to cost reduction, the Sona IF513 Wi-Fi 6E + Bluetooth® 5.4 Module, powered by the AIROC™ CYW55513 chipset, stands out in in a few different ways. For example, by combining Wi-Fi 6E and Bluetooth® 5.4 in a single module, it eliminates the need for separate communication components, reducing hardware costs and simplifying the design and manufacturing process. The module's advanced features, such as improved coexistence algorithms and high throughput, minimize connectivity issues, leading to fewer device failures or malfunctions, reducing maintenance and support costs over time.

Picking the Right Partner Matters

Choosing the right long-term partner is one key to success. That partner should come with a trusted and experienced team of FAEs to support and solve any potential issues specifically related to hospitals and medical devices. Medical-device OEMs should reach out to the experts to realize the benefits and understand the advantages of Wi-Fi 6 and what direct benefits they will realize.

Contact Infineon Technologies or Ezurio today.

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Version: V1.0_EN
Date: 10/2024

Stay connected!

Scan QR code and explore offering
www.infineon.com

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.