



## Design Update Capabilities for Medical Devices

### Build in Safety and Security to Meet Regulatory Requirements

The top objective of the U.S. Food and Drug Administration (FDA) and other regulatory agencies is to provide healthcare patients with access to safe medical devices that meet their healthcare needs. With the major priority to achieve better results in patient healthcare and lifesaving techniques, regulatory agencies such as the FDA continue to establish new rules and regulations to make medical devices safer and more secure for patients. In a 2018 announcement, the FDA released an article, “[Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health](#),” that describes new FDA actions to improve medical device safety. A major component of this plan is the call for mandatory built-in capabilities providing safety and security updates to medical devices.

### THE CHALLENGE

Medical device manufacturers must meet the FDA challenge of building secure, reliable, and cost-effective safety and security update capabilities into their medical technology. No longer is the development phase the only and most significant cost driver in the medical product lifecycle. The built-in capability to update the system is required to meet new and evolving FDA and other regulatory requirements for medical devices. This use case outlines solutions for designing such update capabilities into a medical device.

### THE SOLUTION

This new update requirement has become a golden opportunity for medical device manufacturers to bring innovation to medical technology, especially given the growing use of medical devices by doctors and patients in hospitals and at home. Now, new safety and security concerns merge with the medical device system operation that must maintain patient health and treatment.

#### MEDICAL DEVICE CHALLENGES

- Accelerate device time-to-market
- Reduce development, deployment, and ongoing maintenance
- Meet stringent regulatory compliance requirements
- Update or replace legacy, stand-alone devices and systems
- Utilize safe and secure over-the-air wireless communications to update systems or transmit medical data
- Improve flexibility and agility to deploy new technologies
- Connect and manage medical devices and healthcare facility systems
- Ensure system security from outside intrusion

Additionally, as new cybersecurity vulnerabilities are discovered, they need to be managed to ensure continuing patient safety.

Wind River® offers a portfolio of products and modern tools that can help medical device companies create and deploy secure, reliable software update capabilities in a cost-effective manner. These include the use of virtualization technology available with Wind River Helix™ Virtualization Platform; the VxWorks® real-time operating system; Wind River Linux; and Wind River Studio, the first cloud-native DevSecOps platform for embedded development.

### Wind River Helix Virtualization Platform

Helix Platform consolidates multi-OS and mixed-criticality applications onto a single edge compute software platform, simplifying, securing, and future-proofing critical infrastructure solutions. It provides a safe, secure, and reliable software development environment with a Type 1 hypervisor solution for medical technology systems as well as for other industries.

This virtualization platform manages and allows the creation of virtual machines (VMs) on a single compute platform with a mix of operating systems and mixed-criticality workloads to allow greater flexibility, safety, and security, as required for today's medical devices. Helix Platform's hypervisor can manage multiple VMs running VxWorks, Wind River Linux, and other guest operating systems such as Windows® and Android. It supports multiple software applications, including those for safety-critical or security systems, running together or segregated.

Thus, safety-critical applications on a medical device can be reliably run and updated via the network and wireless over-the-air (OTA) connections. To protect patients, medical device architects can use our industry-leading virtualization technology to segregate different software applications into independent VMs in separate partitioned processor cores as necessary, to more easily maintain, patch, or replace current software with new safety or security updates.

### VxWorks

VxWorks is a real-time operating system found in more than 2 billion devices in medical, industrial, transportation, and defense solutions. It is proven in mission-critical medical applications, where safety, security, and reliability are paramount. Its small footprint enables devices to meet hard real-time operating requirements in scaling from small to large medical devices. It works on all major processor architectures, including Arm® and x86.

### WIND RIVER SOLUTIONS

- **Wind River Studio:** A cloud-native toolset for developing, deploying, operating, and servicing mission-critical intelligent systems across the edge
- **VxWorks:** The first and only RTOS in the world to support application deployment through containers, helping to meet rigorous certification standards for safety, security, and performance in connected medical devices
- **Wind River Linux:** The industry-leading open source operating system with a comprehensive suite of products, tools, and lifecycle services to build and support intelligent edge solutions
- **Wind River Helix Virtualization Platform:** A real-time, embedded, Type 1 hypervisor that consolidates multi-OS and mixed-criticality applications onto a single edge compute software platform, simplifying, securing, and future-proofing critical infrastructure solutions such as medical equipment

The latest release of VxWorks includes support for OCI containers. Now you can use modern IT-like technologies to develop and deploy intelligent edge software better and faster for medical technology. Best-in-class, pre-integrated security functionality in VxWorks includes foundational security capabilities for devices, communication, and management for security and privacy. VxWorks provides documentation for medical device manufacturers for inclusion in compliance-related vendor qualification, as well as for use in premarket submission to the FDA.

## Wind River Linux

Wind River Linux is the industry's most advanced embedded Linux platform, with a comprehensive suite of products, tools, and lifecycle services to build and support intelligent edge solutions such as medical devices. Wind River Linux delivers vital components for the productization and commercialization of any medical device or intelligent edge device.

The KVM hypervisor is a component of Wind River Linux. To provide the capability to easily update FDA-approved and security functions in a medical device, Wind River Linux, with its KVM hypervisor capability, can run applications in various VMs running Wind River Linux, VxWorks, or another guest OS. An FDA-approved security application or function would run in its own separated VM, safe from interference or conflicts from applications in other VMs. Each medical application and security VM can be easily updated via the network or an OTA wireless connection, or a mirrored VM can quickly be updated and then swapped with the updated functions.

Wind River Professional Services can support a medical device company in developing a Wind River Linux solution that can easily update VMs and be secure, protecting the operations and data on the medical device. Additionally, Wind River Studio Linux Services can aid in scanning, remediation, and ongoing monitoring of vulnerabilities, helping to fulfill the requirements of a plan for ongoing vulnerability management.

## WIND RIVER STUDIO

Wind River Studio is the first cloud-native platform for the development, deployment, operations, and servicing of mission-critical intelligent edge systems. Use it to develop medical device solutions with modern software development methods and tools to create quality, leading-edge healthcare devices. Develop in the cloud using secure public, private, and hybrid clouds. Utilize continuous integration/continuous deployment (CI/CD) practices to connect all workflows through a single pane of glass for agile, secure, and cyber-protected development and deployment for mission-critical medical applications and devices on the edge. Automate processes by bringing AI and machine learning into development, security, deployment, and operations with the workflow automation and digital feedback loop capabilities in Wind River Studio for fast, high-quality, innovative medical device solutions with device update capabilities designed in from the start.

WNDRVR