WIND™

Using Linux in Medical Devices: What Developers and Manufacturers Need to Know

By Ken Herold, Engineering Specialist, Wind River

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE OVERVIEW

Linux is the operating system of choice for a wide range of medical devices, from vital-sign monitors to hospital bedside "infotainment" systems to complex imaging equipment. Yet not all Linux implementations are alike. Because patients' lives may be in the balance, software used in medical devices must meet stringent regulatory guidelines to ensure that it will perform as promised. Trying to cobble together solutions from pure Linux without commercial support puts the burdens of testing, validation, documentation, and compliance on the device manufacturers and their developers, an onerous, time-consuming, and complex process that can turn "free" Linux into a very costly proposition.

There are, of course, commercial vendors of Linux who provide value-added, stabilized versions of the open source software, along with board support packages (BSPs). But service, support, and documentation levels vary widely among them. For example, some chip vendors provide software solely to drive processor sales; and with many vendors, the relationship ends with the sale.

This paper explores the issues that software developers and medical device manufacturers need to take into account in choosing Linux for medical devices. It outlines some regulatory compliance and support requirements for software in medical devices and what to look for in a commercial Linux vendor. It highlights how Wind River addresses these issues by providing a comprehensive solution, including the necessary documentation, services, and support to help build high-performance devices.

TABLE OF CONTENTS

WIND

THE ADVANTAGES—AND CHALLENGES—OF OPEN SOURCE

Linux appears in a wide variety of medical devices—for a variety of good reasons. As a general purpose operating system, it has all of the advantages that open source presents. Free distributions are available and they can be modified and redistributed under the GNU General Public License (GPL). It has been widely adopted, scrutinized, and embraced by thousands of developers. As a result, it's easy to find developers who use it frequently and know it intimately. Linux also enjoys the support of all major hardware manufacturers and runs on virtually any processor. On top of that, it has a large ecosystem of board and software providers that use proven toolchains and APIs. And it is known for exceptional graphics support, including popular frameworks such as Qt and Android—important for device screens that require clarity and readability. This, along with the innovation and maturity of Linux, has made it a mainstay in medical device development.

For all its advantages, however, using Linux in a medical device also poses a number of challenges. Medical devices marketed in the United States are regulated by the Center for Device and Radiological Health (CDRH), a branch of the Food and Drug Administration (FDA). Whether or not device makers are claiming compliance to the medical device software standard IEC 62304, they must follow several FDA guidance documents. Accordingly, an operating system may be treated as software of unknown provenance (SOUP) or off-the-shelf (OTS) software. The FDA also makes it clear that the burden of ensuring safe and reliable performance does not end with product launch. When evaluating operating systems, planning for bug fixes and security updates for the entire life cycle of the product is recommended.

REGULATORY PERSPECTIVE FOR PREMARKET SUBMISSIONS

Medical devices and their components must undergo a hazard analysis, typically performed by the device manufacturer. The purpose is not to try and predict a likelihood of failure but to analyze the effect on the patient in the event of failure. The content for documentation of OTS software depends on the results of the hazard analysis performed. There are two levels of documentation: "basic" and "special." The more stringent "special" level, in the FDA's own words, requires the device manufacturer to do the following (from "Guidance for Industry, FDA Reviewers, and Compliance on Off-the-Shelf Software Use in Medical Devices," U.S. Food and Drug Administration):

1. "Provide assurance to FDA that the product development methodologies used by the OTS Software developer are appropriate and sufficient for the intended use of the OTS Software within the specific medical device."
2. "Demonstrate that the procedures and results of the verification and validation activities performed for the OTS Software are appropriate and sufficient for the safety and effectiveness requirements of the medical device. Verification and validation activities include not only those performed by the OTS Software developer, but also include those performed by the medical device manufacturer when qualifying the OTS Software for its use in the specific medical device."
3. "Demonstrate the existence of appropriate mechanisms for assuring the continued maintenance and support of the OTS Software should the original OTS Software developer terminate their support."

Choosing a commercial Linux vendor that can help a device maker satisfy these requirements is essential. Wind River strives to remove the burden from engineering organizations to demonstrate to their purchasing and quality assurance departments that it is qualified to be a supplier of medical software. Based on years of experience in responding to manufacturer questionnaires, Wind River has compiled the necessary information about its product development process and controls, its support organization, and its overall qualifications. This by no means reduces the company's responsibility to assure the safety and reliability of an individual software component throughout the device life cycle, nor is it intended to mitigate the need for an audit should one be indicated by the hazard analysis. What it can do is streamline the purchasing approval process and allow engineers to focus on building their products.

CYBER-SECURITY: ASSURING THE SAFETY OF NETWORKED DEVICES

The networking of what were once standalone medical devices is becoming increasingly common, for example, monitors in patients' rooms that feed data directly into a centralized monitor in a nurses' station. If Linux is being used in a medical device designed to be connected to a network, whether wired or wireless, the FDA's guidance on cyber-security applies. Simply stated, networks are vulnerable to hacking, and the manufacturer must have a maintenance plan in place to deal with any networking vulnerabilities.

More specifically, the FDA says, "You should maintain formal business relationships with your OTS software vendors to ensure timely receipt of information concerning quality problems and recommended corrective and preventive actions. Because of the frequency of cyber security patches, we recommend that you develop a single cyber security maintenance plan to address compliance with the QS regulation and the issues discussed in this guidance document.

"While it is customary for the medical device manufacturer to perform these software maintenance activities, there may be situations in which it is appropriate for the user facility, OTS vendor, or a third party to be involved. Your software maintenance plan should provide a mechanism for you to exercise overall responsibility while delegating specific tasks to other parties. The vast majority of health-care organizations will lack detailed design information and technical resources to assume primary maintenance responsibility for medical device software" (from "Guidance for Industry—Cyber-security for Networked Medical Devices Containing Off-the-Shelf Software," U.S. Food and Drug Administration).

If a commercial Linux vendor does not enter into formal support relationships with its customers or does not have an ongoing cyber-security plan in place, the burden falls solely on the device manufacturer to monitor the Linux community, identify vulnerabilities, and take the necessary actions—a full-time job that requires a dedicated and highly specialized team.

The Wind River Linux security response team identifies, monitors, responds to, and resolves security vulnerabilities. The security team monitors and participates in various email lists and security forums, issues patches and alerts, and releases a bimonthly security bulletin. The bulletin notifies customers of the status of Wind River Linux relative to each and every publicly announced vulnerability. In addition, the team follows the Wind River security response policy, which establishes target response times based on the priority of the vulnerability. With Wind River Linux, manufacturers get not only a steady stream of security updates but same-day closure of some of the most severe vulnerabilities.

Wind River's response to the DNS cache poisoning vulnerability of July 2008 vividly illustrates its security capabilities. The Wind River team became aware of this vulnerability, affecting virtually all Linux implementations, before it became public knowledge, allowing for same-day closure, keeping customers ahead of potential hackers.

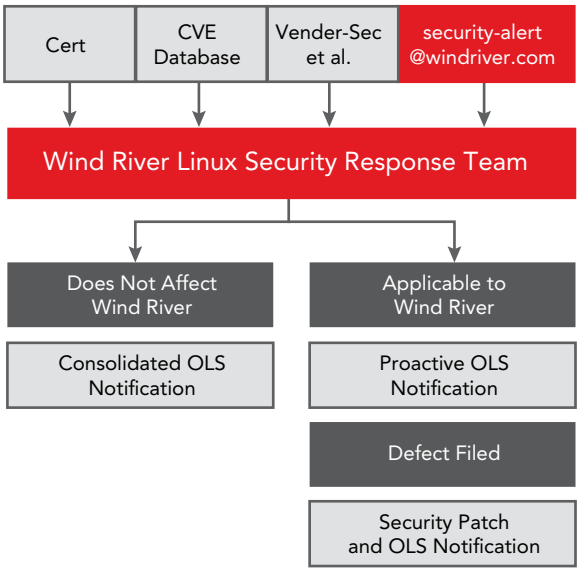
In 2010, a typical year, the team analyzed some 4,000 issues against all releases of Wind River Linux. These reviews identified more than 250 vulnerabilities affecting Wind River Linux and resulted in the creation, testing, and distribution of patches to address them. In addition to such efforts, the security response team proactively executes various security scanning and attack simulator tools against Wind River Linux and issues patches and updates as appropriate. All patches are rolled into future service packs and major releases of Wind River Linux, ensuring that every subsequent release contains no known security vulnerabilities.

If security functionality is not a core competency of the device manufacturer, it is critical to have an operating system vendor who will assist with the configuration of the security components of the network stack. In the face of growing malware attacks such as the Stuxnet worm, medical device manufacturers and their software partners need to be especially vigilant. Using a kernel configurator to remove the USB components from the final kernel is one way to help protect against a USB borne infection, but at the cost of some functionality.

RAISING THE SECURITY BAR

Device manufacturers have to decide what level of security is appropriate. In devices where prevention of any kind of breach is mission critical, device manufacturers may want the added assurance with respect to security. In response to this need, Wind River has developed another off-the-shelf solution, Wind River Linux Secure. This alternative meets or exceeds common industry definitions of a trusted operating system: Common Criteria certification, mandatory access control, and multilevel security. Different functions of the device, such as access to USB, can then be made accessible to specific users based on their roles, while restricting others to functionality requiring only lower security clearance. Secure cryptography capabilities help ensure the security and confidentiality of patient data. Audit trail functionality creates logs showing when the system has been entered and whether any data has been changed and by whom and isolates affected portions while sustaining uncorrupted functionality.

For a manufacturer to try and add this level of security to an open source or commercial version of Linux would entail a steep investment in time and resources, which is not the most productive use of engineering expertise. As a complete off-the-shelf solution, Wind River Linux Secure can reduce development costs and risks and speed time-to-market.



Wind River Linux security response process

SUPPORT FOR IMPLEMENTATION

Along with the regulatory, safety, and security issues, there is the practical matter of building a device that is reliable in performance and successful in meeting the needs of the marketplace. The following are among the issues to consider:

- **Integrity of testing:** Obtaining quality tools to fully test your design is crucial, and being able to show validation artifacts for those tools is also a requirement. Not only must the OTS software be designed according to good principles, but the tools used to evaluate it must themselves be validated to prove that they are reliable. Using a testing system that automatically creates the documentation of the testing performed may deliver a time-to-market advantage over manual systems while reducing the likelihood of human error and giving greater confidence in the results.
- **Open source compliance:** It is essential to comply with the requirements of the GPL and other applicable open source licenses. Wind River performs reviews of the compilation and documentation of the GPL and other licenses that control each major release of Wind River Linux. Wind River examines the source code to identify licensing compliance issues before the product is released. Customers receive thousands of pages of detailed documentation to assist in their own evaluation and review.
- **BSP development:** Board support packages are essential in implementing embedded operating systems, and Linux is no exception. Few manufacturers are equipped to develop BSPs in-house, and the effort required to create customized BSPs can be extremely costly. Wind River Linux supports four major architectures (ARM, MIPS, PowerPC, and Intel) and has BSPs available to use. In addition, Wind River has an experienced professional services organization that can create a BSP from scratch or extend one by adding middleware or drivers for any needed peripherals. The team will also provide test artifacts and long-term support tied to a specific BSP, which reduces costs.

WIND RIVER PROFESSIONAL SERVICES

Wind River can provide medical device manufacturers with a stable, enhanced embedded Linux solution on which to build applications. Many manufacturers, however, may find themselves short on resources, facing fast deadlines, or needing expertise that they don't have in-house to bring a complete solution to market. That's where Wind River Professional Services comes in. In addition to board support packages, performing specific enhancements such as radically improving boot time and reducing kernel footprint, Wind River's professional services team can design, test, and implement entire systems. Companies engage Wind River Professional Services at any or all phases of the development cycle to leverage expertise beyond their core competency to assure high quality and accelerate time-to-market.

LICENSE COMPLIANCE

Wind River reviews its major Linux releases to

- Verify open source license compliance.
- Verify licenses are compatible with one another.
- Prepare a comprehensive open source disclosure document, including license notices found in the source code.

In the development of multi-core systems, the goal of simplifying the system design while still gaining the performance advantages of multiple processors and operating systems presents a new set of challenges. Developers using advanced analysis tools in a Linux environment may encounter obstacles that are multiplied in a multi-core or multithreaded environment. Using tools from a commercial OS provider reduces that burden for developers and allows for professional-level support.

More and more developers are using embedded hypervisors to leverage virtualization and enable multiple operating systems to run on a single board. By using an embedded hypervisor to configure the multi-core environment, boot several cores, allocate hardware resources, provide access to and protection of memory (for safety and security), and monitor system health, the device maker can focus on its particular application.

CONCLUSION

With its inherent flexibility, lower costs, and widespread adoption, Linux is understandably popular among developers of embedded software for a variety of applications. Its use in medical devices, however, raises special considerations—regulatory, safety, security, design, and implementation—of which manufacturers need to be aware. To manage all these issues successfully, it's important to have a commercial OTS Linux partner with the resources, expertise, and long-term support to help device makers deliver effective end products that will not only win regulatory approval but will perform reliably for many years.

With Wind River Linux, device manufacturers get an operating system backed by a wealth of experience and resources, with maintenance and security support as well as a premium, extended support option to cover the entire life span of the product. And as Linux moves forward, so does Wind River, providing a migration path that effectively makes the product design "future-proof," mitigating against obsolescence with commercially supported software on a plethora of hardware choices.

Learn more about Wind River Linux at www.windriver.com/products/linux.html.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.