WIND RIVER

CHOOSING LINUX FOR MEDICAL DEVICES

Advantages, Issues, and Recommendations for Device Manufacturers

By Ken Herold, Engineering Specialist, Medical and Security Solutions

EXECUTIVE SUMMARY

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 regulatory guidelines to ensure that it will perform as promised for its intended use. Cobbling together solutions from pure Linux without commercial support puts the burdens of testing, validation, documentation, maintenance, and compliance on 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). Service, support, and documentation levels, however, vary widely. Some chip vendors also provide a version of Linux, mainly to drive processor sales, but with many vendors the relationship ends with the sale.

This paper explores the issues that software developers and manufacturers need to consider when choosing Linux for medical devices. It outlines the regulatory compliance and support requirements for software in medical devices, and explains what to look for in a commercial Linux vendor to ensure they will be met. 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 that are safe, reliable, and fully compliant.

TABLE OF CONTENTS

THE ADVANTAGES—AND CHALLENGES—OF OPEN SOURCE

Linux appears in a wide variety of medical devices, for a number of good reasons. As a general purpose operating system, it has all of the advantages that open source presents, along with additional benefits such as the following:

- Free distributions are available, and they can be modified and redistributed under the GNU General Public License (GPL) and other licenses.
- Linux has been widely adopted by many thousands of developers, making it easier to find developers who use it frequently and know it intimately.
- All major hardware manufacturers support Linux, and it runs on virtually any processor.
- Linux has a large ecosystem of board and software providers who use proven toolchains and application programming interfaces (APIs).
- Linux is feature-rich in many areas, including tools, management, security, and graphics—important for device screens that require clarity and readability.
- The innovation and maturity of Linux has made it a practical choice in medical device development.

In addition, there is growing momentum behind making embedded Linux development easier and faster. The Yocto Project, a collaborative open source project initiated by the Linux Foundation, is aimed at accelerating embedded Linux development by providing developers with greater consistency in the software and tools they're using across multiple architectures.

Wind River has embraced the Yocto Project and is using Yocto Project tools to build Wind River Linux. Wind River is also adding value by hardening the kernel, the toolchain, and the user space packages, and by providing additional quality assurance (QA). For medical device developers, Wind River support of the Yocto Project means they have the best of both worlds: an industry-standard platform that provides core functionality while remaining open to new innovations, plus the added value of a commercial vendor with deep expertise not only in Linux but also in high-reliability, life-critical embedded systems. While the Yocto Project only integrates bug fixes for versions 6 months old, Wind River offers a much longer support timeline.

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). Medical device manufacturers must follow several FDA Guidance documents, and the medical device software standard IEC 62304 is now recognized or required in most jurisdictions. The Wind River Linux operating system may be treated as software of unknown provenance (SOUP) under IEC 62304, or as off-the-shelf (OTS) software under the other FDA guidelines. The FDA also makes it clear that the burden of ensuring safe and reliable performance does not end with the product launch. When evaluating operating systems, planning for bug fixes and security updates for the entire lifecycle of the product is recommended.

REGULATORY PERSPECTIVE FOR PREMARKET SUBMISSIONS

Medical devices and their components must undergo a hazard analysis, typically performed by the manufacturer. The core objective is not simply to predict the likelihood of failure, but rather 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 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 satisfy these requirements is essential. The vendor must be able to supply the right level of documentation. As the FDA recommends, the device maker should not hesitate to conduct an audit if there is any concern about the vendor's development methodology. The purpose of the audit is to establish that the vendor can in fact meet all three of the FDA's key criteria. Wind River has been subjected to a number of such audits and completed them all successfully.

Wind River also strives to remove the burden from engineering organizations to demonstrate to purchasing and QA departments that Wind River 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 overall qualifications as a company. This by no means reduces the company's responsibility to ensure the safety and reliability of an individual software component throughout the device lifecycle, nor is it intended to mitigate the need for an audit should one be indicated by the hazard analysis. What it can do, however, is streamline the regulatory and purchasing approval process and allow engineers to focus on building their product.

CYBERSECURITY: ASSURING THE SAFETY OF NETWORKED DEVICES

The advent of the Internet of Things, an era of unprecedented connectivity and communication among devices, machines, and intelligent systems, has introduced new challenges for security. This is particularly true in the medical arena, where human lives can depend on the safety, security, and reliability of 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 nurse's 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 cybersecurity applies. Simply stated, networks remain 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 cybersecurity patches, we recommend that you develop a single cybersecurity 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 healthcare organizations will lack detailed design information and technical resources to assume primary maintenance responsibility for medical device software" ("Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," U.S. Food and Drug Administration).

If a commercial Linux vendor does not enter into formal relationships or does not have an ongoing cybersecurity plan in place, the burden falls on the manufacturer to monitor the Linux community, identify vulnerabilities, and take the necessary actions—a full-time job requiring a dedicated and highly specialized team. Wind River has assembled just such a team, whose services are included with every Wind River Linux service agreement.

The Wind River Linux Security Response Team (SRT) 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 bi-monthly security bulletin. The bulletin proactively notifies customers of the status of Wind River Linux relative to each and every publicly announced vulnerability. In addition, the team ensures adherence to 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 also same-day closure of some of the most severe vulnerabilities.

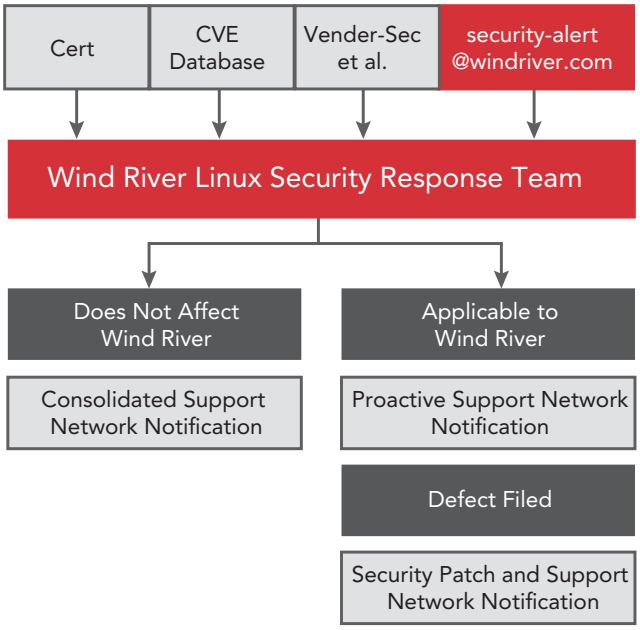

Figure 1: Wind River Linux security response process

The Wind River response to the "Kaminsky Bug" vulnerability of July 2008 (CVE-2008-1447: DNS Cache Poisoning Issue) vividly illustrates its security capabilities. The SRT became aware of this vulnerability, affecting virtually all Linux implementations, before it became public knowledge, allowing for same-day closure and keeping customers ahead of potential hackers.

In 2010, a typical year, the SRT analyzed some 4000 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 these vulnerabilities. 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 manufacturer, then it is critical to have an operating system vendor who will assist with the configuration of the security components of the network stack. Wind River networking experts are available to configure network stack components, performing tasks such as setting up the IP tables or configuring the firewall for the appropriate level of security. In the face of growing malware attacks such as the Stuxnet worm, medical device manufacturers and their software partners need to be especially vigilant.

RAISING THE SECURITY BAR

Device manufacturers used to have the luxury of stipulating that their devices will be deployed only on a network secured behind a firewall. Recent thinking has become more realistic, accepting that not every hospital network that is supposed to be secure is secure in practice. IT staff in hospitals, just as in other industries, struggle to keep their networks patched and up-to-date. Increasingly, they are asked to connect greater numbers and more diverse types of devices to that network, resulting in many exceptions to the original rules of deployment. Medical devices are also being deployed beyond the hospital walls in long term care facilities or in the home, where there is no IT department to build a secure network. The FDA is taking cybersecurity seriously, and the draft Guidance from June 2013, "Management of Cybersecurity in Medical Devices," is the first step.

It is now recommended that the premarket submission include justifications for security features to limit access to trusted users, ensure trusted content, and provide fail-safe and recovery features. Premarket submission should now include:

- Hazard analysis, mitigations, and design considerations to identify cybersecurity risks of the medical device, as well as justification for the corresponding controls, including a traceability matrix
- A systematic plan for providing validated updates and patches to operating systems
- Documentation to demonstrate that the device is free of malware, as well as recommendations for configuration of the firewall and antivirus software for the environment of use

FDA personnel are apparently aware of the blueprint offered by the Stuxnet worm; the draft Guidance explicitly calls out devices that have portable media such as USB enabled as posing a higher security risk. Using a kernel configurator to remove the USB components from the final kernel would be one way to protect against a USB-borne infection, but at the cost of some functionality.

Wind River has a history of developing Linux-based solutions such as Wind River Linux Secure that meet or exceed common industry

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 CMMI Level 3–certified Wind River Professional Services comes in. In addition to BSP assistance and performing specific enhancements like radically improving boot time and reducing kernel footprint, the 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, assure high quality, and accelerate time-to-market.

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 only to specific users based on their roles, while other users are restricted to functionality with lower security clearance.

Manufacturers have to decide what level of security is appropriate and take into account both intentional and unintentional cyber-security risks. In devices where prevention of any kind of breach is mission critical, manufacturers may want the added assurance of security functionality built right into the operating system.

In response to this need, Wind River has developed another OTS solution, Wind River Intelligent Device Platform. This platform reduces the effort required to deploy secure platforms by providing preconfigured functionality that eliminates the need to build from scratch on top of the Yocto Project. For a manufacturer to add this level of security to an open source or commercial version of Linux would entail a steep investment in time and resources—not the most productive use of engineering expertise. In addition, as medical devices and medical workers become more mobile, it becomes increasingly important to ensure that communications between devices are secured through encryption. In the United States, compliance with the Health Insurance Portability and Accountability Act (HIPAA) requires adherence to the "Security Standards for the Protection of Electronic Protected Health Information," better known as the Security Rule, which covers protected health information that is in electronic form. Compliance with the Security Rule requires a thorough assessment of current security risks and gaps, including both data that is "in motion" and data that is "at rest." Through Transport Layer Security (TLS) or IPsec, sensitive information can be protected and the privacy and confidentiality requirements of the Security Rule can be met.

In addition to the encryption support in Linux, audit trail functionality creates logs showing when the system has been entered, whether any data has been changed, and by whom it was changed. It also isolates affected portions while sustaining uncorrupted functionality.

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. Among the issues to consider are the following:

- **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 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 an automated testing system that automatically creates the documentation of the testing performed will deliver a time-to-market advantage over manual systems, while reducing the likelihood of human error and assuring greater confidence in the results.

IP ASSURANCE

To facilitate the IP compliance process for the medical device manufacturer, all major Wind River Linux releases have an IP compliance team that performs the following:

- Verifies open source license compliance
- Verifies licenses are compatible with one another
- Prepares SPDX files for each package
- Prepares a third-party notice file highlighting special terms
- Prepares a package list noting the associated licenses

Wind River also provides a free service that creates SPDX files for software uploaded to an automated server that utilizes various algorithms and heuristics to determine licensing information for each file based solely on the information contained in the software package.

- **IP assurance:** In order to legitimately build a Linux-based device and thus redistribute open source software, the device manufacturer must pay attention to the many open source licensing terms of the software from which the device is derived. Wind River vets each package of Wind River Linux to identify the license terms, determines whether they can be complied with, and performs a check of the overall IP wellness of the package. Wind River may remove files within a package or outright exclude a package if it does not meet certain IP wellness criteria—for example, licensing that may not be clear, or a package with contradictory licensing. Keeping in mind that a package can be made of many source files, Wind River generates artifacts that become the Licensing Disclosure Document, including: an SPDX file per package, a third-party notice file (which highlights special license terms for a given package), and a package list with the associated licenses. The medical device manufacturer can use this aggregated and formatted information within their compliance program to determine how to satisfy their open source license obligations without incurring the costs of reviewing close to a thousand packages and the hundreds of thousands of files that comprise those packages.
- **BSP development:** BSPs 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.
- **Multi-core design:** 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 multi-threaded environment. Using tools from a commercial provider with professional-level support allows the developers to focus on development instead of debugging complicated tools.
- **Virtualization:** 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. A hypervisor can also provide a way to protect intellectual property by isolating it from other applications on its own virtual board and allow Linux to be safely run next to a real-time operating system, Windows or Android, on a multi-core processor.

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 Linux partner with the resources, expertise, and long term support to help deliver a safe and effective end-product that will not only win regulatory approval, but also perform reliably for many years.

With Wind River Linux, manufacturers get a proven 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 lifespan 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 the risk of obsolescence with commercially supported software on a plethora of hardware choices.

For more information on Wind River Medical Solutions, visit http://windriver.com/solutions/medical/.

WIND RIVER

Wind River is a world leader in embedded software for intelligent connected systems. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in more than 1 billion products. To learn more, visit Wind River at www.windriver.com