BREAKTHROUGH INNOVATIONS IN THE MEDICAL DEVICE MARKET

Suddenly the Opportunities Exceed the Challenges

By Santhosh Nair, Director, Medical, Wind River
EXECUTIVE SUMMARY

New advances in technology, combined with new approaches to connectivity, security, and compliance, have breathed new life into the medical device market. Manufacturers are accelerating the development of a new generation of medical devices capable of delivering breakthroughs in the quality of health care and delivering business results. This paper examines the market trends that have sparked this new era of invention and describes how Wind River is helping manufacturers capitalize on the opportunities.

RESHAPING THE ECONOMICS OF INNOVATION

Conditions have not been favorable for medical device manufacturers over the past couple of years. The general economic downturn, growing concerns about device security and safety, increasing regulatory scrutiny and compliance requirements, and high development costs dampened development enthusiasm:

• The cost of acquiring and operating high-end medical devices—from blood analyzers to medical imaging systems to intensive-care ventilators—has put pressure on hospital administrators to get more from existing devices rather than purchase next-generation systems. Device manufacturers have responded by focusing more on lowering average diagnostic times and increasing performance and scalability in existing devices.

• Connectivity is an increasingly vital capability for medical devices. Diagnostics, therapy, and imaging are now connected in the hospital information system. However, while connectivity helps drive down operating expense, it increases risk by exposing devices to multiple security threats.

• In the face of ever increasing safety, security, and other regulatory mandates, fewer devices are qualifying for regulatory approval—and too many devices fail after market.

To transform these challenges into opportunities for medical device manufacturers, Wind River has been focusing on three overarching objectives.

1. Consolidation to Accelerate Development and Reduce Costs

Software has become the key differentiator for medical device manufacturers. But with the rise of embedded software comes a dramatic rise in complexity—which in turn slows down the development process.

One of the key contributors to development complexity is the piecemeal fashion in which tools and solutions are often built using ad-hoc products and technologies. Therefore, step one for device manufacturers is to consolidate tools, standards, and processes wherever possible.
Two developments in the embedded market provide a real solution for those who wish to reap the rewards of consolidation: multi-core processors and virtualization (hypervisor) technology.

The latest multi-core processors significantly boost overall performance and increase performance per watt over single-core processors. They also improve application scalability and protect software investments by allowing processors with more cores to be substituted to meet future demand. Using the latest multi-core architectures and hypervisor concepts, medical device manufacturers are now able to combine multiple operating systems on a single safety-compliant aggregation platform, providing a stable foundation that delivers lower costs and increased functionality.

The second concept, virtualization, provides the ability to run multiple operating environments separately from each other on the same physical device—for example, it is possible to run a real-time operating system such as Wind River’s VxWorks and a general-purpose operating system such as Linux on the same device. This separation, or partitioning, makes resource allocation far more flexible. For example, processing power can be allocated exclusively to one virtual board or shared across multiple virtual boards; memory can be partitioned so that each board has its own unique and enforced memory space; and enforced memory space cannot affect any other virtual board. Virtualization also makes it possible to separate safety-related functionalities.

Together, multi-core processors and virtualization are a compelling combination that greatly improves the time-to-market as well as the performance and reliability of medical devices. The net result is that manufacturers can consolidate more functionality onto fewer physical systems, cut costs and complexity, and focus on meeting the requirements that are challenging safety and regulatory certification processes.

Another key aspect of consolidation is standardizing on a smaller number of open platforms and toolsets, making software development processes more adaptable and future ready. Consolidation also allows manufacturers to build on a framework that can support comprehensive requirements and keep pace with fast-changing safety and regulatory certification processes.

As frameworks become more open and standardized, medical device manufacturers have enormous opportunities to aggregate and smoothly integrate a variety of subsystems to cut costs and complexity. Standardization also has the potential to help manufacturers shorten development cycles. Typically, the design cycle for medical devices is two to three years, with a shipping cycle of up to eight years—and a need for more than 10 years of support. The life cycle, which is more than 20 years in some cases, is under pressure to be extended even further through more frequent upgrades, in turn demanding greater support from suppliers.

Medical device vendors can overcome these challenges by taking a more modular standards-based approach to software. Standardization of technologies and toolsets not only aids time-to-market issues but eliminates the problem of repeatedly qualifying elements such as a UDP stack. Through the modular approach, standard software components can be delivered as part of a validated service pack release, thus eliminating the need for revalidation and requalification.

Wind River is addressing the requirements of consolidation, standardization, and modularization with end-to-end development and run-time platforms. Wind River’s offerings make it possible to consolidate, integrate, and manage complexity while mitigating risk. Wind River solutions allow medical device manufacturers to meet stringent real-time deterministic requirements while taking advantage of the flexibility and cost benefits of open standards.
Wind River’s combination of operating system flexibility, multi-hardware-architecture coexistence, safety and security solutions, and medical-industry-specific platforms with a rich set of middleware creates a robust, commercial off-the-shelf (COTS) foundation, and its independent software vendor (ISV) partner ecosystem enables medical device manufacturers to speed up, build out, and customize their next-generation products.

For medical device manufacturers trying to get products to market quickly, Wind River can lower the barrier for innovation by providing a standardized platform on which to build high-quality applications.

2. Strengthening Security for Connected Devices

Three years ago, an article in the New England Journal of Medicine reported that computer hackers could gain wireless access to implanted pacemakers and shut them off or reprogram defibrillators to deliver fatal jolts of electricity. This generated an avalanche of press worldwide about the hidden risks of medical devices, followed by requisite hand wringing from politicians and promises of stiffer regulations.

As a result, makers of medical devices have been steadily increasing their focus on security. The threat is far broader than a hacked pacemaker; embedded software plays a role in a broad swath of devices from imaging systems such as CT scanners to intensive-care ventilators. And the rapid growth in the number, the intelligence, and the volume of data generated by medical devices has created an upward spiral in security threats. The following are just a few examples:

- Diagnostics, therapy, and imaging devices are connected in the Hospital Imaging System (HIS), and a vulnerability in any one device puts the entire HIS at higher risk.
- In the United States, hackers have been able to glean personal patient data by eavesdropping on signals from wireless radios embedded in implants.
- Security experts worry that hackers might go after medical devices that are designed to deliver medicine. In 2010, Dr. Tadayoshi Kohno and Dr. William Maisel of the Cardiovascular Institute of Beth Israel Deaconess Medical Center in Boston called for the U.S. Food and Drug Administration (FDA) to regulate and work with medical device manufacturers to stop potential security breaches in a wide range of wireless devices.
- In New South Wales, Australia, a virus infected the computer dispatch system of an ambulance service, forcing staff to shut it down. As a result, health officials had to revert to coordinating the state’s paramedics and ambulances via a manual paper-based system—putting lives at risk.

Equally alarming, a new breed of hackers is exploiting security flaws. It’s not just smart kids trying to breach a firewall for sport anymore. Professional, well-funded groups—including organized crime, government agencies, and terrorist cells—are attempting to crack into secure networks, access sensitive information, and alter the behavior of critical systems, causing physical harm to equipment and potentially putting lives at risk.

For the developers of medical devices, two things have become crystal clear. First, tackling the emerging security challenges is an urgent imperative; and second, solving security issues can create significant competitive advantages.

Medical device developers now realize that a more holistic approach to device security is necessary. Development teams are considering security issues at every layer of the development stack: the hardware platform, the virtualization technology, the operating system, the network stack or other communications middleware, the packets of data being sent across the network, and the applications.

Security is becoming an integral part of system design, with regard to specific technology selections, application development processes, and even application management tasks such as patching and upgrades geared toward security and patient privacy. Security threats that are inherent in configuration or customization are being analyzed and addressed. Software updating and provisioning processes are designed with security in mind. The assessment includes security threats that can be introduced by the end user, such as malware, viruses, worms, and Trojan horses, all of which can affect reliability and performance.

In addition, the use of security-certified components has emerged as an effective way to build in security rather than bolt it on. Certified operating systems, network stacks, and middleware are independently validated by a trusted expert to prove they meet specified standards and are conformant with specified requirements. Certification also provides a benchmark that can serve as a basis for comparison. Dozens of device manufacturers have
started to require certified assurances, given the increase in government regulations that are now being required in many markets and associated devices.

By taking a platform perspective to security and harnessing the efficiencies of cyber-security-certified components, medical device developers can cut development costs and time frames while decreasing overall security risks. More than a paradigm shift for embedded developers, this approach is driving a true transformation in device development, resulting in more secure medical devices and stronger financial results for development firms and the health-care industry.

Historically, security protections in the embedded space and the application arena have been handled separately. However, given the increasingly connected nature of today’s embedded devices, it has become a strategic imperative to deal with security threats in a more comprehensive way. Since embedded devices have technology requirements that differ from traditional IT equipment—namely limited power, memory, and performance constraints—traditional security solutions are insufficient.

The teeming of McAfee, Intel, and Wind River now allows embedded developers to implement security measures at all layers of the software stack, including the application layer. Equally important, McAfee and Wind River combine the concepts of “whitelisting” and “reputation-based intelligence” to deliver stronger security to embedded devices. For example, the whitelisting approach focuses on allowing access from only the known good. By integrating these concepts with “graylisting,” where security threat assessment is reputation based, Wind River, Intel, and McAfee can deliver a new security paradigm that addresses the full range of issues, threats, and exploits.

3. Achieving Connectivity and Compliance for Mobile Health Care

For the makers of medical devices used in mobile health or home care solutions, interoperability is becoming increasingly critical. Devices are becoming more intelligent and controlling more aspects of patient care, clinical diagnostics, and hospital administration. And they are interacting not just with people—expanding our ability to communicate and share information—but with other devices, controlling systems that literally keep people alive. Machine-to-machine (M2M) interaction, delivered by ever smaller, ever smarter components, allows for new levels of “situational awareness” and analytics, revolutionizing medical practices.

Business realities are also driving the need for ever greater connectivity in medical devices. Interoperable connectivity is important for keeping costs in line and ensuring compliance with safety and security standards and requirements. For example, to reduce costs and meet consumer demands, seamless connectivity via Bluetooth and wireless local area networks (WLANs) are often required. Cost is another important consideration: The use of open connectivity standards can reduce implementation and life cycle costs. Connectivity also increases efficiency: IT integration with medical device functionality enables preventive monitoring and workflow optimization.

Equally important, connectivity impacts compliance. To meet medical industry safety standards and regulations, device manufacturers must find a way to tackle the increased security risks of the connected era. According to McAfee, more than 55,000 new malware programs, aimed at attacking connected devices of every type and size, are uncovered each day. However, cyber-security certification needs to be ensured for a complete, integrated system, including applications.
In short, the complexity of interoperability is creating huge headaches for medical device manufacturers. The problem is compounded by the rapid growth of the health-care industry itself over the past decade. Today, there are too many devices, made by too many companies, utilizing too many competing standards, deployed at too many hospitals and clinics to tie the system together in any cohesive way.

As a result, several different manufacturers make similar devices using slight variants of standards, and these devices can’t communicate with each other effectively. They can’t be connected or share data. They add cost and complexity. They end up reducing the quality of patient care rather than improving it. They could end up exacerbating the mistakes made in a high-stress environment such as the emergency room or operating room.

Clearly, consolidation of standards is necessary in the medical device industry. Wind River is attempting to address the situation by making available a health-care-standards protocol stack—a middleware stack that can be used by all device manufacturers to ensure their devices can communicate with all other devices built to the standard. Wind River is expanding the use of key industry standards within its platform with its ecosystem of partners. Manufacturers can simply take the Wind River medical solutions stack and integrate it into their products seamlessly. This will not only help medical device manufacturers enable connectivity in their products through standard off-the-shelf components but also focus on building meaningful applications built on these standards to improve the quality of health care and the workflow within the hospital information system.

Wind River has the right technologies and expertise to make connectivity part of the solution rather than part of the problem. Wind River helps medical device manufacturers provide interoperable connectivity while meeting all relevant safety requirements; standardize on open platforms to simplify, accelerate, and future-proof development; and take advantage of next-generation connectivity technologies and standards as they emerge.

**ADDING UP TO LOWER COSTS**

By keeping the focus on reducing the complexity of manufacturing medical devices—less development complexity, more holistic approach to security, fewer competing standards, and more—Wind River is helping to cut development costs significantly:

- The use of multi-core processors enables medical device manufacturers to consolidate hardware and accelerate the development process, saving both capital expenditure (CAPEX) and operating expense (OPEX).
- Virtualization technology allows manufacturers to pack more functionality onto fewer physical systems, further reducing CAPEX.
- By implementing security measures at all layers of the software stack, including the application layer, McAfee and Wind River enable manufacturers to address the full range of security issues, threats, and exploits proactively rather than try to bolt on security after the fact, cutting total development costs substantially.
- By encouraging consolidation of competing standards into a unified, certified middleware stack, Wind River is helping to simplify both the development process and vendor selection by device manufacturers, reducing total costs.

By helping reduce development costs and time frames, Wind River can allow medical device manufacturers to focus less on the development cycle and more on their core competencies: innovating and creating devices that improve the quality of patient care and extend human lives.

**CONCLUSION**

Medical device makers are on the brink of a revolution in new capabilities and business results. Where functionality once drove innovation, cost efficiency, and time-to-market, now safety, security, and connectivity are the overriding requirements. Convergence and consolidation will see more functionality being ported to cost-effective hardware platforms, thereby meeting the increasing demands on software—and creating new opportunities for true breakthroughs in medical devices.

For more information about Wind River’s solutions and support capabilities for medical device makers, visit [www.windriver.com/solutions/medical/](http://www.windriver.com/solutions/medical/).