Executive Summary

The world of medical electronics is shifting fundamentally. Equipment designs have traditionally lasted 20 years, with years of heritage and testing behind each design. Now more innovation is demanded, with new features and new versions being developed much faster, based on digital systems. More focus is being put on cost-effective implementation so more units can be deployed across more hospitals and surgeries.

To develop this next generation of safety-critical medical and industrial device, designers and system architects must consolidate hardware, reduce cost, and reduce time-to-market while never compromising their platform’s stability, safety, and security.

This paper addresses what medical system designers require to meet today’s challenges: a combination of multicore hardware, operating systems specialized for device certification, hypervisor software, and a consolidated but open development toolchain.

Today’s Safety-Critical Design Challenges

Increasingly, more medical system innovation is moving to software, which is creating a significant challenge in designs where safety is critical. Some elements of the software have to remain fixed, providing verified safety-critical functions, while other parts can add new functions and innovations while keeping the hardware fixed, to comply with various standards on interference and risk assessment.

Addressing the safety concerns and making the most of that heritage is vital, but these areas have been isolated and fragmented, making them expensive and slow to take advantage of the phenomenal changes in the performance and cost of electronics systems as well as making them slow to react to changing market conditions and costly to maintain over many years.

New approaches such as multicore processors and hypervisor software technology that has been optimized for the embedded market are key enablers for making this happen, driving consolidation of hardware and software that spurs innovation while providing a mechanism for enhancing safety requirements. This is not only important for medical equipment but spreads across other areas such as industrial control and transportation.

Historically these sectors were driven by functionality, but in each of these areas, safety, security, quality, maintainability, and cost-efficiency are now of paramount importance. The overarching safety requirements in the basic functional safety standard IEC 61508 and its derivatives, applicable to all kinds of industries, are driving new challenges to comply with the standard and still meet functional requirements.

Multicore for Complex Medical Applications

In medical applications there is an increase in the use of complex equipment for diagnostics, covering X-rays, CT scanners, and dialysis machines that have to add features such as automated report generation and networking while reducing costs.

Traditionally these areas have provided innovation and upgrading with separate hardware systems, particularly to conform to medical standards such as IEC 60601 for electromagnetic compatibility—vital to prevent equipment interference—and ISO14971 on risk assessment. This architecture has used one board for the safety-critical elements, often hardwired without software or with simple software that is well-established and proven over many years.

A second board is used to add the additional noncritical functions such as administration and networking.
Multicore Is Key to Innovation in Medical Applications

While this has been adequate in the past, adding new standards and new features as well as the consolidation of systems for cost and space reasons means that the two-board approach is no longer viable. Now, features added to software must be proven and compliant with safety-critical standards as directed by the U.S. Food and Drug Administration (FDA) or the European counterpart, where standards such as IEC 62304 define software life cycle processes.

Multicore devices are a key way to tackle these demands. These devices are now becoming available for the embedded market with the performance and support for the five to 10 years demanded by these industrial markets. However, they still take advantage of the availability of commercial operating systems and application software along with the cost reduction and integration that is driven by the PC and enterprise markets.

Using multiple processor cores can provide a way of consolidating the existing board architecture onto a single board, making use of one core for the safety-critical software and other cores for other noncritical functions.

### Hypervisor for System Consolidation

While this is all very well in principle, designing a system with this “bare metal” approach can require considerable time and cost as well as a large, experienced design team. This approach also requires the certification evidence to be developed with many thousands of lines of test and verification code that can take time to develop and run through the certification process.

With the faster introduction of new features, certification of safety software is changing from a “proven-in-use” model to a more formal tools-oriented model. This is perhaps the biggest shift in this market, leaving developers unsure of how to approach these changes and how to know that their investment in software and associated tools will ensure certification while extending to third-party software components. The criteria and requirements for premarket approval applications as defined by the FDA require valid scientific evidence to support a reasonable assurance of safety and effectiveness of the device. Providing evidence to off-the-shelf software can be expensive and causes unpredictability in the life cycle process.

This is driving the move to new software approaches such as the hypervisor. This allows different operating systems to run on different cores on a single platform, allowing the designer to make use of a wider range of third-party software alongside the existing legacy safety-critical software. Often this safety-critical software can be running on one dedicated processor while others are running a real-time operating system such as Wind River’s VxWorks or a non-real-time operating system such as Linux. Different levels of criticality on the same system platform or processor also drive the need to combine off-the-shelf software with a real-time operating system specialized for device certification such as VxWorks.

Consolidated platforms will drive the need for a variety of OS platforms. Real-time operating systems, such as VxWorks, have a greater advantage when considering determinism and decreased complexity compared to a non-real-time OS such as Linux, which makes them the ideal candidate for certification. Linux has advantages when implementing rapidly evolving consumer communication standards or graphical user interfaces. It would therefore make sense to use both on the same system to get the best of both worlds. Using a consolidation technology such as a hypervisor, this becomes a real possibility.

### Importance of Supported, Validated Commercial Linux

With many machine manufacturers now looking at using Linux, the issue of support arises. Here too there is some consolidation of technology, with better development tools, but there still exists a great deal of fragmentation in the market for Linux-based solutions.

Too often, manufacturers attempt to cobble together free Linux distributions instead of choosing a supported and validated commercial distribution. The complexity of Linux and the business challenges are totally underestimated. Training on Linux, stability of the distribution, open standard compliance, indemnification, documentation, and scalability are just some of the benefits of choosing a professionally managed distribution and should therefore be considered during the decision process.

An important part of using Linux is the ability to partition safety and non-safety-critical elements of the same application on a single hardware platform. Linux provides high potential for features and innovative middleware, which often adds a layer of complexity if safety is required.

Hypervisor technology makes it possible to consolidate Linux and real-time operating systems at the software layer, allowing safety and non-safety applications to run on the same hardware platform. Multicore processor technology, together with hypervisors, enables multiple operating systems to run concurrently on the same hardware platform but in partitioned, protected spaces.

At the same time, safety-critical tasks can operate within a certified application in a real-time operating system such as VxWorks, with communication protocols running under VxWorks or Linux and perhaps another operating system, providing supervisory functions on the same machine. Hypervisor technology also enables simpler porting of legacy applications because the partitioned architecture allows
different versions of the same operating system to run simultaneously so that existing code can run unchanged but new code can make use of the added features in new versions. Integration services can further help customers take the risk out of safety and consolidation projects by guaranteeing a smooth and predictable route to market, with significant time-to-revenue advantages.

But using multiple operating systems on a system creates significant difficulties if there are separate toolchains that have to be used. This can slow down development and lead to the risk of more bugs, which is a major issue for a safety-critical medical system. This then requires more software verification and validation as driven by the FDA’s Center for Devices and Radiological Health, asking manufacturers to perform those tests, which is expensive and time consuming. Instead, a consolidated toolchain such as Wind River Workbench, based on the Eclipse open framework, supports the trend toward multiple operating systems, allowing applications targeting different operating systems to be developed at the same time in the same environment. The openness of the concept allows unitary testing or static analysis tools to be used, providing a huge benefit to development teams. The openness of the Eclipse framework, allowing other tools to be integrated with it, is now becoming key to machine developers.

**Similar Demands in Industrial Market**

The industrial market can be looked at as six independent areas with very similar requirements. Medical applications, transport infrastructure, industrial control, test and measurement, power distribution, and automotive all share very similar properties, from the importance of safety-critical systems to a range of well-established standards that have to be implemented.

All these sectors are seeing similar demands. For example in process automation, where there is a lot more distributed control and a growing complexity, there are new challenges in the flexibility needed to build and maintain new factories or plants quicker and faster, while not compromising quality and safety. Similarly in industrial control, for example, robotics is adding differentiation while ensuring safe operations with increased uptime by using near field communication between the robot head and the control unit. Machine tools now need to integrate common PC software such as report files and Internet access while at the same time adding secure connections to other equipment.

**Conclusion**

The combination of multicore hardware, operating systems specialized for device certification, hypervisor software, and a consolidated but open development toolchain are key to providing the support medical system designers need. This combination helps designers and system architects make use of the consolidation in hardware, reducing cost and reducing time-to-market while providing a secure, stable platform for adding new features and innovation in software and maintaining a certified environment while reusing as much legacy code as possible, all of which is vital for developing the next generation of safety-critical medical and industrial systems.