Three Steps to Medical Device Safety Through Software

By Jens Wiegand
General Manager for Industrial and Medical Solutions, Wind River
**Executive Summary**

How can developers of medical devices add innovative new capabilities while remaining compliant with all relevant safety requirements? How can they harness the power of new software technologies such as multi-core processors and embedded virtualization without jeopardizing certifications—or risking product liability lawsuits? How can they tame the increasing complexities of development, testing, and compliance while meeting cost and time-to-market goals?

The right software platform and the right development tools, used the right way, can deliver a solid foundation to meet the most stringent safety certification standards—on time and on budget. This paper examines three key steps device manufacturers can take to build this foundation.

**Regulatory Challenges**

Human lives depend on the safety of medical devices. That is why the primacy of safety in medical device development will not diminish and why developers (and regulators alike) will always go the extra mile for safety. But more and more safety-related functionality now depends on software. And as software technologies and processes grow increasingly complex, safety compliance becomes more and more difficult, time-consuming, and expensive.

Today’s embedded software technologies are capable of reversing the upward spiral of cost and complexity in safety compliance.

Software is a key source of differentiation for medical device manufacturers. Embedded software is now a crucial element in everything from CT scanners and X-ray devices to dialysis machines, medical imaging systems, blood analyzers, intensive-care ventilators, confocal microscopy systems, and clean machines.

The growing importance of software—and the impact on safety and security—is not lost on regulators. Manufacturers that have not yet adopted robust software development processes will likely face greater pressure to do so as new legislation is introduced in the years ahead. Consequently, device manufacturers who are already struggling to meet existing or emerging regulatory requirements, such as IEC 62304 for medical process standards, IEC 61508 for functionality safety, IEC 60601-1-9 for electromagnetic compatibility, and standards such as ISO 14971 on medical device risk management, could find themselves facing a whole new set of challenges.

The U.S. Food and Drug Administration’s approach has been to impose pre-market and post-market requirements, which has led to confusion. For pre-market approval, the FDA requires valid scientific evidence to support a reasonable assurance of safety and effectiveness of the device. Products that demonstrate such evidence can be placed on the market, but if they fail in service they can then be removed pending investigation against requirements not imposed before the product was placed on the market. Thus, certification can get your product to market but won’t necessarily keep it there. For device manufacturers, this represents a significant risk in terms of product liability. Conversely, new specifications that are in development to assist in the life cycle of software for medical devices, such as IEC 62304, may not go far enough. Many manufacturers of medical devices feel they could and should be doing more to limit their liability in lieu of more robust regulatory requirements.

**Design Challenges**

Further complicating the issue is that both medical systems and software development processes are growing increasingly complex:

- Software content in intelligent devices is doubling every two years, according to analysts.
- In the embedded world, many products now use 32-bit and 64-bit multiprocessor architectures and run multiple operating systems within a single device.
- Iterative or “agile” development has replaced one long development cycle with a lot of shorter ones, making testing a nonstop exercise aimed at a moving target.

**Regulatory Standards**

- **IEC 61508**: The international standard for electrical, electronic, and programmable electronic safety related systems that sets out the requirements for ensuring that systems are designed, implemented, operated, and maintained to provide the required safety integrity level (SIL)
- **ISO 14971**: The standard that specifies a process for a manufacturer to identify the hazards associated with medical devices
- **IEC 60601-1-9**: The new international standard for environmentally conscious design of medical electrical equipment
- **IEC 62304**: The standard that defines the life cycle requirements for medical device software
As more and more functionality is delivered via software, developers are struggling to integrate piecemeal legacy tools and development processes with new tools and technologies without jeopardizing safety certifications. For example, in many designs, some elements of the software have to remain fixed, providing verified safety-critical functions, while other parts can add new features, functions, and innovations while keeping the hardware fixed to maintain safety compliance.

Technology convergence is the traditional solution route to cutting cost and complexity, but for medical device manufacturers there are complications:

- For products that need to demonstrate compliance with IEC 61508, technology consolidation can raise certification issues. This can subsequently increase the cost and time of placing a revised product in the market.
- The demand for more connectivity, both wired (Ethernet) and wireless (Bluetooth, WLAN), creates additional interoperability challenges in terms of the communication stacks required.
- Many suppliers have a huge installed base of legacy applications (which require maintenance) and need to find new ways to innovate without sacrificing these investments.

Against this backdrop of multidimensional challenges, let’s take a look at solutions. Here are three specific steps medical device manufacturers can take to leverage the power of new embedded software solutions to reduce cost and complexity, remain compliant with safety requirements, and derive new sources of competitive advantage.

**Step 1: Consolidate Using Multi-core and Embedded Virtualization**

Two developments in the embedded market provide a real solution for those who wish to reap the rewards of consolidation without jeopardizing compliance with safety and security standards: multi-core processors and embedded 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. The trend toward multi-core is well underway, and multi-core-optimized operating systems, middleware, and tools are now available. Using the latest multi-core architectures, suppliers are now able to combine multiple operating systems on a single safety-compliant aggregation platform.

The second concept, embedded 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 OS such as Linux on the same device. This separation or partitioning makes resource allocation far more flexible. Processing cores 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. Embedded virtualization also makes it possible to separate safety-related functionality (e.g., soft PLC) from other functionality.

Together, multi-core processors and embedded virtualization allow medical device manufacturers to consolidate more functionality onto fewer physical systems, cut cost and complexity, and keep the focus on meeting the requirements that are challenging safety certification processes.

**Step 2: Standardize on Open Platforms**

With the increased focus on differentiating via embedded software, the ability to standardize hardware platforms has become a key consideration for medical device manufacturers.

For example, the use of real-time kernels in programmable logic controllers is now commonplace. However, convergence and consolidation are occurring further up the value chain. Device manufacturers are now counting on software to provide an overall environment for safety, security, and connectivity. They are in a position to consolidate functionality, but they also need a lot of support at the software layer.

At the same time, the issues of safety and security are also moving up through the value chain, creating the need for more strategic partnerships with suppliers of embedded software development tools, operating systems, and middleware. As frameworks become more open and standardized, manufacturers have enormous opportunities to aggregate and smoothly integrate a variety of subsystems.

These trends also have the potential to help manufacturers resolve life cycle issues. Typically, the design cycle is two to three years, with a shipping cycle of up to eight years—and a need for more than 10 years’ support. The life cycle, which is already more than 20 years in some cases, is under pressure to be extended even further through more frequent upgrade programs, demanding greater support from suppliers.
Device software vendors can help customers overcome these and other challenges, such as protecting market share, intellectual property, and time-to-market, while reducing the total cost of ownership. A modular software approach, for instance, helps with time-to-market issues but raises the problem of paying to repeatedly certify elements, such as a UDP stack. Through modular certification, standard software components can be delivered as part of a certification package, thus becoming a trusted component. Customers can then rely on this evidence package for certification against IEC 61508, allowing not only a faster approvals process but greater flexibility at the design phase and more predictability in the business.

With many device manufacturers now looking at using Linux, the issue of support arises. The complexity of Linux and the business challenges are totally underestimated. Too often manufacturers attempt to cobble together free Linux distributions instead of choosing a supported and validated commercial distribution. 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.

Through modular certification, standard software components can be delivered as part of a certification package. Customers can then rely on this evidence package for certification against IEC 61508.

Open technology, combined with embedded virtualization and multi-core concepts, creates powerful new capabilities. For example, 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. As an open operating system, 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. Multi-core processor technology, together with hypervisors, enables multiple operating systems to run concurrently on the same hardware platform but in partitioned, protected spaces.

**Step 3: Build on a Foundation That Can Support Change**

One of the key reasons software processes are often perceived as part of the problem rather than part of the solution is that they are built in a piecemeal fashion from ad hoc tools and technologies, resulting in enormous complexity.

Standardizing on open platforms will help to make software development processes more adaptable and future-ready, but it is also important to build on a framework that can support comprehensive requirements and keep pace with fast-changing safety certification mandates.

Specifically, look for a combination of operating system agnosticism, safety and security solutions, and a rich set of middleware that offers a robust commercial off-the-shelf (COTS) foundation.

A flexible, agile software platform will make it possible to take advantage of new technologies as they emerge without sacrificing previous investments. For example, it will allow you to use hypervisor technology to consolidate Linux and real-time operating systems at the software layer, letting safety and non-safety applications run on the same hardware platform; it will allow you to combine embedded virtualization and multi-core technologies so that multiple operating systems can run concurrently on the same hardware platform (in partitioned, protected spaces); and it will allow safety-critical tasks to operate within a certified application in a real-time OS such as VxWorks, with communication protocols running under VxWorks or Linux, providing supervisory functions on the same machine.

**Conclusion**

The primacy of safety is the only constant in the development of medical devices. Design requirements, tools, hardware architectures, development processes, and safety regulations will all remain in a state of flux for the foreseeable future. To remain competitive, manufacturers must find a way to deliver safe devices on time and on budget, using a mix of legacy and next-generation tools and processes.

It can be done.

Today’s embedded software technologies are fully capable of cutting the cost and complexity of safe medical devices. This approach implements more agile software platforms and processes, but the real starting point involves something far less technical: your attitude. If you can focus on the opportunities, not just the challenges, you’re already a step ahead.