Safety: Make Software Part of the Solution

Three Steps That Control and Process Automation Developers Can Take to Achieve Safety Compliance While Cutting Costs and Complexity

JENS WIEGAND
General Manager for Industrial and Medical Solutions
Wind River
Executive Summary

The cost and complexity of safety compliance continue to spiral upward. The list of safety regulations, standards, and government mandates is growing, and the result is more pressure on already tight schedules and budgets, constant training and retraining of engineers, and less time to add new functionality to equipment and devices.

The primacy of safety in control and process automation will never diminish, for obvious reasons. Beyond the moral and ethical imperatives are stark legal, monetary, and business considerations. Lack of compliance means potential liability issues, financial penalties, and missed market windows. In some well-publicized cases, noncompliance has led to intervention by regulatory agencies and safety recalls that dealt a major blow to the company’s image and profitability.

As more and more safety-related functionality is built into control and process automation systems via embedded software, it is all too easy to see the software development process as part of the problem—another complex challenge to deal with. That view is shortsighted. Today, the right software platform and the right development tools and technologies, used the right way, can deliver a solid foundation to meet the most demanding safety certification standards—on time and on budget.

Today’s embedded software technologies can reverse the cycle of increasing cost and complexity for safety compliance.

This paper describes three steps manufacturers of control and process automation systems can take to leverage the power of new embedded software solutions to reduce costs, remain compliant with safety requirements, and gain a new source of competitive advantage.

“There is a real window of opportunity for suppliers in the control and process automation markets to harness new technologies that consolidate all the functionality delivering safety and security capabilities.”

TOMAS EVENSEN, CHIEF TECHNOLOGY OFFICER, WIND RIVER
Step 1: Consolidate Using Multi-core and Virtualization

Consolidation is the traditional route to cost savings. However, for suppliers in the control and process automation market, there are complications:

- For products that need to demonstrate compliance with IEC 61508, technology convergence 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.

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 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 and hypervisor concepts, suppliers are now able to combine multiple operating systems on a single, safety-compliant aggregation platform, providing a stable foundation that returns a reduced bill of materials 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 VxWorks and a general-purpose OS such as Linux on the same device. This separation or partitioning makes resource allocation far more flexible. For example, 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. Virtualization also makes it possible to separate safety-related functionality (e.g., soft PLC) from other functionality. Consider also that consolidated platforms will drive the need for a variety of OS platforms. Operating systems will be used more and more in a best-practice method. Real-time operating systems have a greater advantage when considering determinism, and less complexity compared to a non-real-time OS such as Linux, which makes them the ideal candidate for certification. Linux on the other hand has advantages when implementing rapidly evolving communication standards or graphical user interfaces. It would therefore make sense to use both on the same system to leverage each one’s success, to get the best of both worlds. Using a consolidation technology such as a hypervisor, this becomes a real possibility.

Together, multi-core processors and virtualization are a compelling combination that greatly improves the performance and reliability
of industrial systems. The net result is that control and process automation manufacturers can consolidate more functionality onto fewer physical systems, cut costs and complexity, and keep the focus on meeting the requirements that are challenging safety certification processes.

The question for many development teams is not whether to move to multi-core and virtualization but how to do so without increasing risk or jeopardizing existing safety certifications.

Many organizations rush into multi-core and hypervisor adoption, excited about what they can provide to their particular devices, without thoroughly assessing the complexities and pitfalls. More importantly, they fail to consider whether their software platform has what it takes to deliver on the promise of multi-core and virtualization.

For a discussion of the key considerations in adopting multi-core and virtualization, read the following Wind River white papers at www.windriver.com/whitepapers/:

- “Applying Multi-core and Virtualization to Industrial and Safety-Related Applications”
- “Checklist for Success with Multi-core”

### Step 2: Standardize on Open Platforms

The role of embedded software has shifted as a result of the increased focus on differentiation at the software layer. The ability to add safety and security features through software on standardized hardware platforms has become a key consideration.

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. Machine 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, machine manufacturers have enormous opportunities to aggregate and smoothly integrate a variety of subsystems to cut costs and complexity.

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,

---

“With a platform that is optimized for multi-core, it becomes easier for developers to enable next-generation applications that really deliver on both real-time and services-oriented connected requirements.”

TOM STEENMAN, VICE PRESIDENT, DIGITAL ENTERPRISE GROUP, INTEL
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 elements, such as a UDP stack, must be certified repeatedly. 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 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.

**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 the virtualization and multi-core concepts described previously, creates powerful new capabilities. For example, an important part of using Linux for control and process automation customers 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.

Wind River is the only embedded software provider today that offers a complete solution. Based on open standards, our end-to-end development and run-time platforms make it possible to consolidate, integrate, and manage complexity while mitigating risk. Wind River solutions allow control and process automation customers to meet stringent real-time determinism requirements while taking advantage of the flexibility and cost benefits of open standards. Our combination of operating system agnosticism, safety and security solutions, and industry-specific platforms with a rich set of middleware offers a robust commercial off-the-shelf (COTS) foundation, and our independent software vendor (ISV) partner ecosystem enables you to speed up, build out, and customize your solutions.

For example, Wind River VxWorks 61508 Platform enables developers to deliver applications that must be certified to IEC 61508 requirements and other related standards, IEC 62304 for medical, and CENELEC 50126 for transportation. With VxWorks 61508 Platform, developers can take full advantage of multi-core with the assurance that they will have a strong operating system foundation for meeting the most stringent safety certification requirements. Through the addition of hypervisor technology, safety-critical tasks can operate under Wind River’s VxWorks, with communication protocols running under Linux (and perhaps another operating system), providing supervisory functions on the same machine. The concept of hypervisor technology also simplifies the porting of legacy applications. Integration services 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. And a consolidated, Eclipse-based toolchain further supports the trend toward multiple operating systems, allowing applications targeting different operating systems to be developed at the same time in the same environment. This is a huge benefit to development teams. The openness of the Eclipse framework, which allows other tools to be integrated with it, is becoming critical to machine developers.
Conclusion

The environment for process control and machine manufacturers is undergoing a revolution. Where functionality once drove innovation, cost-efficiency, and time-to-market, safety and security are now the overriding requirements. Convergence and consolidation will see more functionality being ported to cost-effective hardware platforms, demanding even more from the software.

For more information about Wind River’s solutions and support capabilities for control and process automation customers, visit www.windriver.com/solutions/industrial/.

“Wind River is the only company with all the different technologies to solve these very tricky problems around multi-core and virtualization. We’ve got the operating systems, Wind River Linux and VxWorks, that can configure in different ways depending on your needs. We have the middleware, such as very high performance network stacks. We’ve got professional services around it that will tie all these things together. And we’ve got world-class tools that will help you solve the problems with multi-core and virtualization.”

—TOMAS EVENSEN, CHIEF TECHNOLOGY OFFICER, WIND RIVER