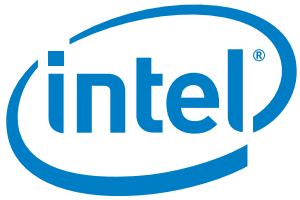


White Paper

Wind River™ Hypervisor and Operating Systems Intel® Processors for Embedded Computing

Applying Multi-core and Virtualization to Industrial and Safety-Related Applications

Multi-core and virtualization provide the opportunity to improve device performance, reduce costs through hardware consolidation and upgrade applications more cost effectively throughout the product lifecycle

Disruptive technologies and trends are affecting the embedded market and providing device manufacturers in the industrial sector with a significant opportunity to improve both their devices and their businesses. Taking advantage of the following technical and industry trends represents a significant opportunity for competitive advantage:

- **Multi-core processors**
- **Virtualization**
- **Increased complexity of safety-related devices**

The availability of **multi-core processors** causes both the most significant disruption the embedded market has seen in many years and one of the greatest opportunities. The latest Intel® multi-core processors provide increased overall performance and improved performance per watt over single-core processors. Multi-core processor-based systems can also improve application scalability and protect software investment by allowing processors with more cores to be substituted to meet future demand. The trend towards multi-core is well underway, as evidenced by Intel® dual-core and quad-core processor shipments exceeding single-core processors.

The second technology trend is virtualization, which provides the ability to run multiple virtual machines on the same physical board by abstracting the underlying processing cores, memory and devices. Virtualization provides the ability to run multiple operating environments, such as one real-time operating system like Wind River* VxWorks* or VxWorks CERT, and a general purpose operating system like Wind River Linux*, on the same device, as shown in Figure 1. Performance gains from multi-core processors and virtualization technology enable the consolidation of what were originally independent devices running separate applications onto one device. Consolidation reduces the amount of hardware and increases energy efficiency, which can lower the overall bill of materials and operating costs of the device.

Virtualization is enabled by a hypervisor, which has supervisory functions that protect the operating environments from each other and provide a measure of separation that can be leveraged to improve the reliability, security and safety of a system. This allows each application to be evolved independently, reducing the life-cycle costs of the device.

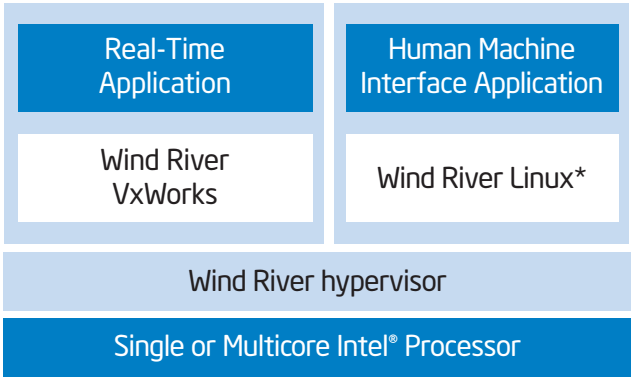


Figure 1. Virtualized System

Safety-related architectures are becoming more complex as demand for new features and regulatory compliance requirements increases. One trend driving complexity is the need for industrial devices to interface to more networks and systems like the Internet, top-floor and shop-floor. As a result, devices must support a larger variety of application software (e.g., security, protocol stacks) with different levels of criticality. And as system complexity increases, regulatory bodies are enforcing more formal certification methods and processes to help safeguard systems aThe combination of multi-core and virtualization technologies can help device manufacturers in industrial control, process automation, energy and transportation protect their development investments. These technologies enable systems to run more applications simultaneously and safely, so it's possible to upgrade an existing multi-core platform incrementally with respect to performance, security, scalability, certifiability and usability. The enhanced performance of Intel multi-core processors can also be used to consolidate control and acquisition applications, visualization and network security onto a single board with minimal software changes. Furthermore, a virtualization layer can protect software investments by reducing direct hardware dependencies. This enables developers to more easily port and upgrade to new device architectures while managing the migration to COTS (commercial off-the-shelf)

technologies more effectively. This white paper describes how Intel and Wind River multi-core and virtualization technologies are changing the way developers approach industrial and safety-related applications.gainst unintended software interactions and outside breaches. Also growing is regulatory influence by means of safety-related application standards (e.g., for IEC 61508, CENELEC 50128, ISO 26262 and IEC60880/62138) and additional industrial sub-segment standards in energy, transportation, process automation and control.

Scaling Processors for Industrial Solutions

VxWorks, Wind River Linux, and the Wind River hypervisor run on a wide range of Intel® processors and are supported by an open standard tool chain that brings efficiency to the multi-core and multi-OS development processes. These capabilities can be extended to different types of industrial control equipment represented by the different layers of the "Automation Pyramid", as shown in Figure 2. The enterprise layer or top-floor infrastructure supports servers and workstations running a mix of applications, including collaborative production management (CPM), financials and asset management databases. Intel® Xeon® processors supply the computing horsepower needed to keep the business running smoothly and efficiently. They run a large number of enterprise applications simultaneously by supporting configurations with eight or more processor cores and by speeding up parallel processing with large on-chip caches that reduce context switching.

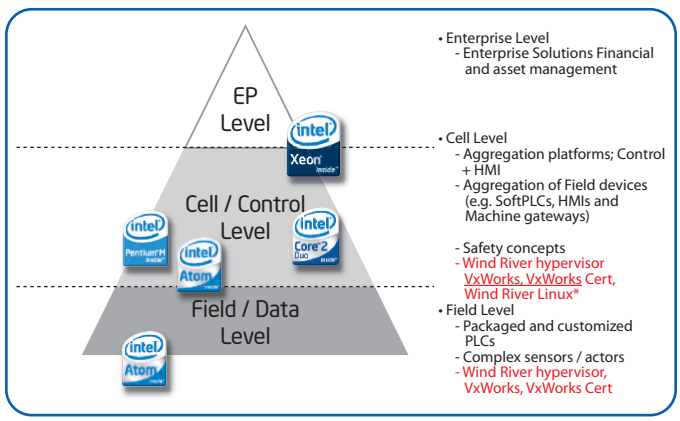


Figure 2. Automation Pyramid

The cell and control layer contains equipment performing a combination of real-time control and HMI functions that have different levels of criticality. This equipment is an ideal candidate for the Wind River hypervisor and Intel multi-core processors that can deliver the computing performance and software separation and reliability required by safety-related applications. The Intel® Core™2 Duo processor, with two processor cores, can run time-critical control functions on a dedicated core and run other functions, like HMI and operator panels, on the second core. This multi-core processor has revolutionary performance per watt, allowing it to be deployed in space constrained systems.

The lower field and data layer controls the factory floor, linking sensors and actuators to controllers and ultimately to manufacturing equipment. Typically, this level requires equipment with very low power consumption, which is why the Intel® Atom™ processor Z5xx series (Figure 3) for embedded computing is a good fit. This processor has a thermal design power, as low as 2.0 watts, and delivers the benefits of Intel® architecture for small form factor, embedded control devices.

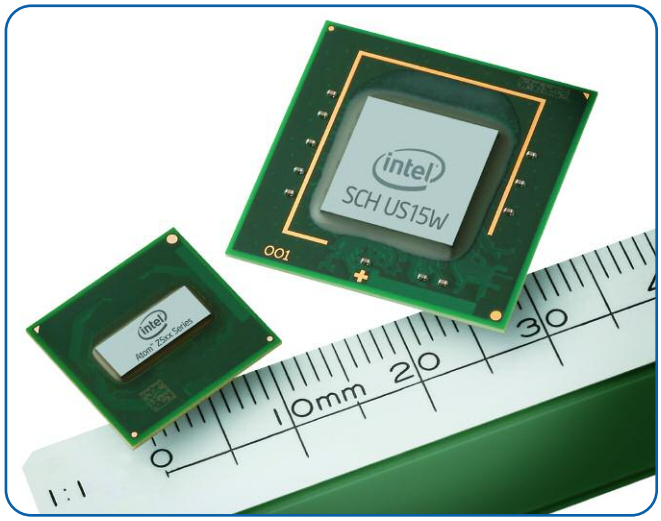


Figure 3. Intel® Atom™ Processor and the Intel® System Controller Hub US15W

From top-floor to shop-floor, developers can build different platforms with varying performance levels and the same code base using embedded Intel processors with long life cycle support. In addition to these advantages, equipment makers typically find maintaining software code for general purpose processors, like Intel® Architecture Processors, is easier than for application specific hardware. This is because Intel processors are supported by a broad ecosystem offering a wide range of mature development tools. For example, as a member of the Intel® Embedded and Communications Alliance, Wind River works closely with Intel to ensure their solutions take advantage of the latest processor features as soon as they come to market.

Virtualization with the Wind River Hypervisor

The Wind River hypervisor provides the ability to partition a physical board's resources into virtual boards, as shown in Figure 4. Each virtual board can host either an operating system, known as a guest, or a minimal executive. Configuration tools are provided in order to partition the processing cores, memory and devices on the physical board. Processing cores can be allocated exclusively to one virtual board or can be shared by multiple virtual boards using the appropriate scheduling algorithm. Memory is partitioned such that each virtual board has its own unique and enforced memory space and cannot affect any other virtual board. Shared memory buffers can be allocated for high speed communication between virtual boards. Devices such as a serial line or Ethernet can be either dedicated to one virtual board or shared between multiple boards.

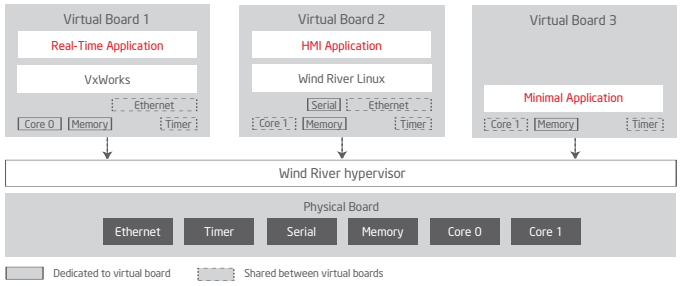


Figure 4. Partitioning a System Into Virtual Boards

The virtual board mechanism enables the porting and paravirtualization of an existing proprietary operating system onto the hypervisor, which can be run alongside a commercial operating system. This provides a gradual **migration** path to COTS technologies as well as the ability to move more easily to new hardware, including advanced Intel® multi-core platforms. This allows the reuse of existing legacy applications that may be very robust and do not require changes while providing the ability to create new and innovative functionality on a more fully featured operating system such as Wind River Linux.

In many industrial applications, two or more separate computing platforms were required to provide the complete system. The reason for separate hardware could have been due to the different nature of the applications; perhaps a hard real-time application for control was required while an advanced human machine

interface was needed for interaction with the operator. In other cases performance limitations may have necessitated separate hardware. The improved processing power of multi-core processors coupled with the separation and protection provided by the virtual board mechanism are a compelling combination that allows for the **consolidation** of industrial systems.

The isolation and protection between virtual boards prevent a fault in one virtual board from affecting another. If a problem occurs in the less critical human machine interface application, it will not affect another virtual board supporting critical system tasks. In addition, the supervisory functions of the Wind River hypervisor will allow for a critical fault to be detected in a virtual board and for that virtual board to be rebooted while other virtual boards continue to run. These capabilities can greatly improve the **reliability** of industrial applications.

The Wind River hypervisor is part of Wind River's multicore software solution, which includes many technologies required for industrial device makers to take advantage of multi-core processors. The multicore software solution is comprised of:

- Support for multi-core software configurations and virtualization
- Industry Leading Operating Systems
  - VxWorks, the industry leading RTOS
  - VxWorks Cert (RTOS that is DO-178B and IEC61508-Part3 certifiable for safety-related applications)
  - Wind River Linux
- Wind River Workbench for developing, debugging and optimizing multicore and virtualized systems

The Wind River hypervisor used on either Intel single-core or multi-core processors provides a high performance solution for consolidating hardware while keeping applications separate.

Taking Virtualization to a New Level with Intel® Virtualization Technology (Intel® VT)

Intel has enhanced the capabilities of virtualization technology with a complementary hardware-assist technology called Intel® Virtualization Technology (Intel® VT). Intel VT performs various virtualization tasks in hardware, like memory address translation, which reduces the software footprint of the hypervisor and improves its performance.

The Wind River hypervisor takes advantage of Intel VT to provide optimal virtualization performance and increased reliability. Without this new technology, the hypervisor would be responsible for handing off more of the platform control to the operating system, which requires complex, compute-intensive calculations. With Intel VT, the hardware takes over this crucial operation, which reduces the computational burden on hypervisor software, thereby increasing its performance. In addition, without hardware assistance, the hypervisor is the sole protector of key processor and operating state information stored in unprotected memory space. Intel VT adds a powerful enforcement layer that prevents any software component, other than the hypervisor, from accessing key system information.

Intel offers three classes of virtualization technology:

- Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x): provides the basic framework that virtual machine monitors (VMMs) need to operate efficiently.
- Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d): facilitates the virtualization I/O devices, such as remapping DMA accesses into segment memory locations, filtering and remapping interrupts.
- Intel® Virtualization Technology (Intel® VT) for Connectivity (Intel® VT-c): runs in conjunction with Intel® Ethernet controllers that support filtering and mapping network traffic to specific queues 'owned' by a particular virtual machine (VM).

Devices using a hypervisor that leverages Intel VT can benefit from an increase in the performance and security of its virtualized environment.

Safety Certification Challenges

A major challenge facing device manufacturers is that during the certification process, they must meet the requirements specified for safety-related software and demonstrate that it's separated or protected from other parts of the system. If the system's hardware and software is fully consolidated, the non-safety related applications running on a general purpose operating system must also be deemed safe. This is very challenging and expensive because of the size of the general purpose operating system (GPOS). In addition, it would be advantageous to have the flexibility to revise the non-safety related software frequently in order to improve the human interface or improve connectivity without having to endure the costs and schedule impacts of recertifying the entire system multiple times during a product's life-cycle.

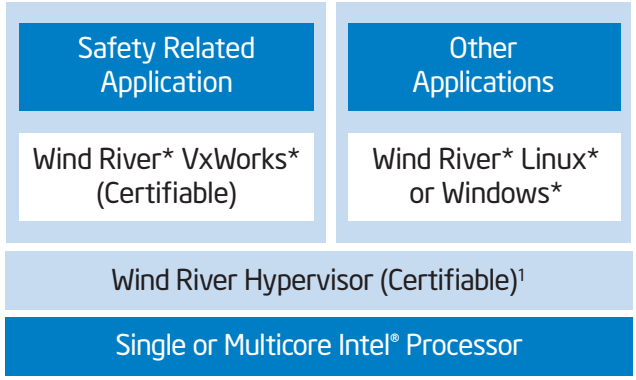
Safety-related components require temporal and spatial separation from other system components with different levels of criticality. Today's separation concepts are mostly designed to use completely independent subsystems for each function, but this approach isn't hardware efficient and increases cost. Furthermore, legacy dependencies imposed by proprietary or RYO

(roll your own) technologies often present additional challenges when OEMs migrate to commercial-off-the-shelf (COTS) hardware and software technologies. However, developers who designed systems with software migration flexibility in mind are well-positioned to benefit from new innovative technologies like multi-core processors and virtualization.

Reducing Risk

Aside from aerospace and defense, where ARINC 653 separation standards are well-defined, most industries lack a unified approach to functional safety. This leaves safety standards open for interpretation and can cause greater unpredictability and uncertainty for device manufacturers. In many cases, device manufacturers face increasing requirements to incorporate different levels of software criticality and address more stringent regulations. As in the ARINC 653 environment, a useful approach is to increase software separation so that software components can be certified as independent modules.

Wind River, a market leader in DO-178B-certified ARINC 653 separation concepts, is applying its experience to the industrial market to mitigate risk and help engineers develop safe and deterministic applications. The memory protection provided by the Wind River hypervisor can be leveraged to ensure the spatial separation of the applications in the virtual boards, as shown in Figure 5. This configuration provides applications with dedicated and secure memory contexts, which is a critical aspect of guaranteeing the safety integrity of independent software modules. Spatial separation enables applications to run as independent modules, so OEMs can certify them as smaller, simpler components. Additionally, temporal separation can be provided by dedicating virtual boards to individual cores or by leveraging the appropriate scheduling algorithm in the hypervisor when multiple virtual boards share a core.



[1]The above is intended to outline Wind River's general product direction. It is intended for informational purposes only, and may not be incorporated into any contract or relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Wind River products remains at the sole discretion of Wind River.

Figure 5. Virtualization System for Safety Related Applications

Wind River's performance optimized hypervisor solution running on Intel processors provides:

- A mechanism to implement temporal and spatial separation between applications.
- The possibility to separate safety-related functionality (e.g., soft PLC) from other functionality (e.g., graphical user interfaces).
- An open modular approach that has the potential to enable cost-efficient safety.

Addressing Future Safety and Performance Requirements

The combination of multi-core and virtualization technologies provides a path for meeting future safety and computing performance requirements of industrial and transportation applications. As such, hardware and software technologies from Intel and Wind River can help developers using a standardized approach to temporal and spatial separation. The exceptional processing performance of Intel multi-core processors with Intel Virtualization Technology enables applications to run safely in a virtualized environment. Wind River supplies a software framework including the IEC61508 and DO-178B certifiable VxWorks Cert operating system and the certifiable Wind River hypervisor.

OEMs certifying safety critical applications, according to IEC61508-Part 3 or other vertical standards derived from the IEC61508 specification, can benefit from using Wind River products with Intel Architecture Processors that enhance safety and reliability in a real-time virtualized environment.

For more information about Intel® processors for embedded computing, please visit:
www.intel.com/products/embedded

Learn more about Wind River's Multicore Software Solution and hypervisor at:
http://www.windriver.com/multicore-software.

WIND RIVER

Printed in USA 0109/SI/S2/PDF Please Recycle XXXXXX-001US