WIND™

Expanding the Role of Virtual Machines and Containers from IT to OT

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Operational technology (OT) and embedded systems are at an inflection point as they evolve past specialized, single-purpose hardware to obtain the business and technology advantages of hosting multiple workloads/applications on general-purpose servers. Mainstream companies are beginning to build on the approaches to transformation that have proven themselves in the information technology (IT) realm, bringing those same architectures to OT systems.

Virtualizing workloads is the technological leap that enables this transition. The key concept behind virtualization is to break down the tight coupling between hardware and software. This allows multiple independent workloads/applications to coexist efficiently and securely on both general purpose and solution specific servers, regardless of their individual requirements. In many cases, existing compute infrastructure can be repurposed for workload/application consolidation, which reduces costs and facilitates the move from legacy to modern architectures.

These changes are taking place in industries that include automotive, energy, industrial, healthcare, and transportation. The shift promises to reduce costs, increase flexibility and agility, and streamline the upgrade path from outdated hardware.

TABLE OF CONTENTS

WIND

DECOUPLING SOFTWARE FROM THE SYSTEM BOARD

As facilities mature, the components such as controller boards that are entrusted with running the software for vital capital equipment often stay in service beyond their design lifespan. Cost is a significant hurdle to keeping controller equipment up to date, both in terms of the replacement expense itself and the potential interruption to operations that swapping out physical compute components can create.

Gradual migration from dispersed computing equipment to centralized, general-purpose servers is emerging as the solution of choice for this challenge. As needed, workloads/applications can also be virtualized directly on the system board within the industrial equipment itself. Multiple types of virtualization play a role, including hypervisor-based virtualization and containers.

Hypervisor-Based Virtual Machines

In hypervisor-based virtualization, each application or workload operates in its own virtual machine (VM) that the hypervisor configures with a specific share of virtual hardware resources such as virtual processors and virtual memory, as shown in Figure 1. Each VM runs its own operating system (OS), matched to the application(s) it supports. On an as-needed basis, the hypervisor can create and eliminate additional VMs to scale capacity up and down.

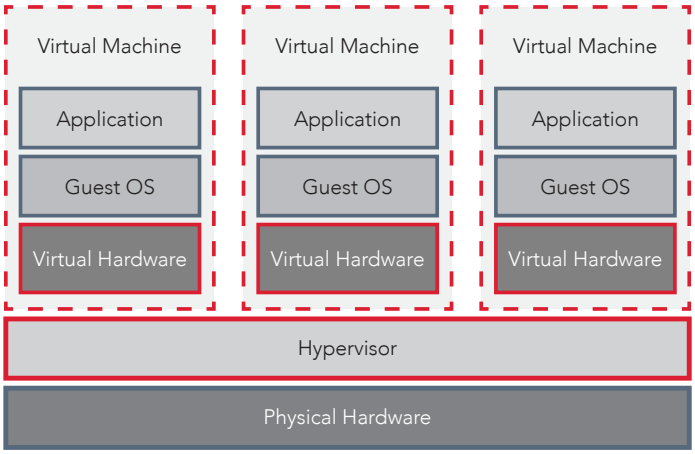

Figure 1. Virtualization using hypervisor-based virtual machines

Hypervisor-based virtualization provides a high degree of isolation between virtual machines, governed by the hypervisor and enforced at the hardware level. That isolation protects individual workloads, including those that are critical, regulated, or otherwise sensitive:

- **Data protection:** The data within that resides in a particular VM is protected against access by applications or workloads in other virtual machines.
- **Fault isolation:** Because each VM can power up or down on its own just like a physical system, a fault or failure in one VM will not impact other VMs operating on the same server or system board.

Because each VM runs a full operating system (OS), VMs based on different OSes can coexist and run on the same server or system board at the same time. This capability lets otherwise incompatible workloads share hardware. For example, applications that require different flavors of Linux, a real-time OS (RTOS), or even Microsoft® Windows® can run in separate VMs on the same server or system board, without conflict.

On the other hand, there may be dozens of VMs on a single physical host, and the presence of a full OS in each one introduces computing overhead and inefficiency. In fact, a single host may run many versions of the same OS, consuming large amounts of resources. For that reason, hypervisor-only virtualization can introduce challenges in terms of the cost and scalability of the overall solution.

Container-Based Virtualization

Packaging applications in containers provides a lightweight alternative to hypervisor-based VMs, with multiple containers being able to share a single OS instance, as illustrated in Figure 2. In most cases, the single OS instance has been Linux, but recent advancements have allowed containers to run on other OSes. Container infrastructure is responsible for orchestrating resources and for spinning containers up and down as needed. Tools and libraries required for the specific application(s) are packaged up in the container, improving interoperability on different systems.

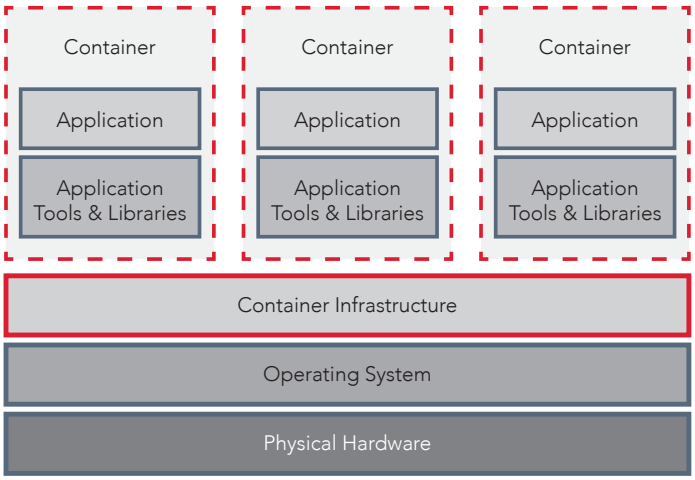

Figure 2. Virtualization based on containers

The reduced overhead can dramatically increase the number of applications that can operate on a given host, compared with VMs. It also enables containers to start up and shut down at an order of magnitude faster than VMs. Even as this approach eliminates the overhead associated with redundant instances of the OS, it also introduces limitations based on the necessity of sharing that OS.

For instance, containers that require different OSes cannot coexist directly on the same host, and containers provide a lower degree of isolation from each other, compared to hypervisor-based VMs. The isolation is provided by the OS itself and based only in software. The architecture provides less robust assurance of the separation of data among containers, and the shared OS means that application failure in one container can potentially impact applications in others.

Combined Hypervisor-Based VMs and Containers

As described above, hypervisor-based VMs and containers have complementary sets of strengths and weaknesses. Organizations can secure the advantages of both VMs and containers while mitigating their shortcomings by combining both on the same hardware, as illustrated in Figure 3. This approach envelops the entire container stack inside a virtual machine, allowing multiple application workloads to share a single OS instance, while retaining the isolation of that container stack from others that share the same physical hardware.

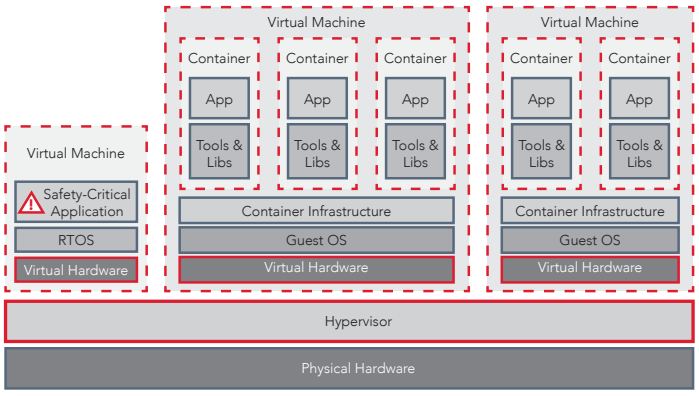

Figure 3. Example of virtualization that combines hypervisor-based VMs with containers

For example, this architecture allows a safety-critical application to run on an RTOS in its own virtual machine, in isolation from other workloads with a dedicated, guaranteed level of resources to protect its operation. On the same server or system board, additional VMs provide isolated environments where low-overhead sets of containers operate for other workloads.

MODERNIZING SOLUTIONS WITH VMS AND CONTAINERS

By packaging software using these technologies, deployed on general-purpose servers or an equipment system board, multiple functions can be consolidated on a central piece of hardware. Because the software is not tied to specific hardware, this approach dramatically improves flexibility.

The value of solutions increasingly comes from software, and when its functionality is consolidated onto a centralized server infrastructure, future upgrades can be performed in software—even over the wire—without swapping out hardware. This capability allows controller software and firmware, including all important security updates, to be delivered and activated more easily and at lower cost than replacing the entire board, with minimal impact on operations.

Mindful of the nested architecture described above, solution providers can use VMs and containers as complementary technologies. Instead of making individual boards for multiple discrete sets of functionality, providers deliver server hardware or an equipment system board, which they configure and support as needed to ensure smooth operation. Using VMs and/or containers enables endless flexibility in deployment models:

- **Containers provide OS-level virtualization.** Because they include all the software dependencies for the applications deployed in them, they can move nimbly among physical, virtual, and cloud platforms.
- **VMs provide platform-level virtualization.** The ability to run any OS inside the VM allows legacy software to be run on current systems, without requiring dedicated hardware.

Using VMs and containers to package software as part of their solutions enables providers to be more agile and innovative. For example, the relative simplicity of software upgrades enables faster iterations of version upgrades, and the resulting improved functionality and security can help deliver a competitive advantage. In addition to being able to perform upgrades in the field, providers are spared the expense of reengineering their board hardware for each generation of their products.

HOW THE WIND RIVER PORTFOLIO ENABLES NEXT-GENERATION OT

Wind River® is well known for its leadership in providing safe, secure, reliable embedded software technologies for critical infrastructure. With a nearly 40-year history, Wind River solutions power more than two billion devices, from the NASA Mars rovers to the factories that built them, as well as airliners, medical devices, industrial systems, and many others. As solution providers contemplate how virtualization using VMs and containers can enable their next generation of products, Wind River provides a proven, comprehensive portfolio that sets the stage for innovation. The Wind River portfolio also helps development teams move faster and improve product quality by bringing agile and DevOps development practices to embedded development.

Real-Time OS: VxWorks

As the foundation for billions of deterministic applications, the VxWorks® RTOS powers critical infrastructure with real-time performance, security, and safety certification. It minimizes latency and jitter for hard real-time embedded applications in a flexible platform that offers developers access to the source code to customize for specific solution needs. VxWorks is based on a hardened kernel, complemented by advanced encryption, controls, and alerting to help secure applications. In addition, the RTOS conforms to a robust set of international standards and provides an extensive set of safety certifications.

Embedded Linux Distribution: Wind River Linux

The most widely distributed embedded Linux distribution, Wind River Linux is based on the upstream Yocto Project, which enables solution providers to build a Linux OS that is optimized for a specific device, without the complexity normally involved in building a custom OS. Wind River Linux is open source, and it can be downloaded for free or it can be accompanied by a commercial subscription that enables ongoing additional benefits. KVM hypervisor is available with Wind River Linux, providing virtualization capabilities and allowing for the management of virtual machines. These include training and long-term technical support, continuous threat monitoring and security updates, and compliance and documentation support for global export of solutions.

Real-Time Virtualized Foundation: Wind River Helix Virtualization Platform

Based on the VxWorks RTOS, the Wind River Helix™ Virtualization Platform is a Type 1 hypervisor, meaning that it runs directly on bare metal for performance and supports an unmodified guest OS within virtual machines. It enables solutions to run real-time, safety-critical applications in static, safe partitions alongside standard applications in dynamic, flexible partitions, tailoring the environment to the requirements of each. By consolidating multi-OS, mixed-criticality applications within virtual machines on a single platform, Helix Platform simplifies and future-proofs solution designs while promoting reuse and consolidation of existing software assets. It is also designed to facilitate certification of safety-critical applications as well as adoption of modern development practices such as agile and DevOps.

Secure, Scalable VM and Container Platform: Wind River Titanium Control

For critical applications and systems, Wind River Titanium Control provides an on-premise virtualization and on-premise cloud platform that supports both VMs and containers. It enables solution providers to migrate from proprietary hardware to standard IT-class servers and runs virtualized control functions with six nines (99.9999%) availability. To facilitate building distributed cloud for the network edge, Titanium Control is complemented by Wind River Titanium Cloud™, which also supports deployment options from very small footprints all the way to large data center environments. The Titanium Cloud ecosystem extends that flexibility and helps ensure real-world success with pre-validated virtualization solutions for COTS platforms from leading hardware providers.

Simulation of Systems in Software: Wind River Simics

By simulating complex systems of hardware, software, and connectivity, Wind River Simics® allows developers to test on a virtual representation of any target system, on demand. This approach enriches testing by eliminating the need for physical targets where it would be expensive or impossible to provide them, such as with a large, complex IoT system. Because all team members can have unlimited access to the simulation, Simics improves collaboration by giving everyone a common baseline to test against, which can be easily distributed and changed

as needed. Simics also provides the rapid feedback needed to support continuous integration and delivery, helping companies on their path to agile development and DevOps.

Optimized for Multi-Core and Multiprocessor Platforms

Wind River technologies support operation on 32-bit and 64-bit processors, with extensive optimizations for the hardware parallelism inherent in multi-core and multiprocessor systems. Platform flexibility embraces a broad spectrum of processors, extending from Arm® to Intel® architecture, including Intel Atom® processors for space- and power-constrained applications, Intel® Core™ processors for middle-tier applications, and Intel® Xeon® Scalable processors for server and cloud platforms.

CONCLUSION

The proven maturity of virtualization in IT has demonstrated the effectiveness and high ROI of workload/application consolidation. Wind River is delivering on requirements specific to the OT domain (reliability, performance, and enhanced security), and we are seeing the benefits of virtualization in the OT domain without increased risk. Decoupling software from hardware allows solution providers to consolidate the software components of their solutions on a centralized server infrastructure or system boards. Both legacy and state-of-the-art systems are defined in software, so they can coexist on standards-based COTS servers or equipment system boards. And version updates are simplified, because software can be easily deployed, even over the wire, independent of the underlying hardware.

That sets the stage for continuous delivery, which Wind River enables further by integrating modern programming methods and languages into its tools, helping development organizations along their Agile and DevOps journeys. As the industry leader in providing embedded software technologies for critical infrastructure, Wind River is helping OT solution providers break new ground in delivering the next generation of products, enabled by virtualization.

WIND

Wind River is a global leader in delivering software for the intelligent edge. Its comprehensive portfolio is supported by world-class professional services and support and a broad partner ecosystem. Wind River is accelerating digital transformation of critical infrastructure systems that demand the highest levels of safety, security, and reliability.