WIND RIVER HELIX VIRTUALIZATION PLATFORM

Wind River® Helix™ Virtualization Platform is a safety certifiable, multi-core, multi-OS platform that supports mixed levels of criticality. Leveraging the proven track record of successful, safety-certified, VxWorks® RTOS technology, it consolidates multi-OS and mixed-criticality applications onto a single edge compute software platform, simplifying, securing, and future-proofing designs in the aerospace, defense, industrial, automotive, and medical markets.

Helix Platform combines a true Type 1 hypervisor with pre-integrated guest operating systems such as VxWorks and Wind River Linux. The platform is designed to support critical infrastructure development applications, including safety-certified applications found in avionics, automotive, and industrial markets. It is also designed for systems requiring the mixing of safety-certified applications with noncertified ones.

Helix Platform gives you flexibility of choice for your requirements today and adaptability for your requirements in the future. For more information, visit www.windriver.com/products/helix.

USE CASES

Application Portability and Consolidation of Multiple Systems

Because device manufacturers need to optimize the efficiency, productivity, and quality levels of their products, they frequently need to migrate existing workloads and applications to new hardware platforms. In many cases, they also decide to consolidate two or more discrete systems into one virtualized hardware platform. Consolidation of different applications from multiple systems on the same compute platform through virtualization provides cost reduction, reduced space/weight/power consumption, and reduced development effort.
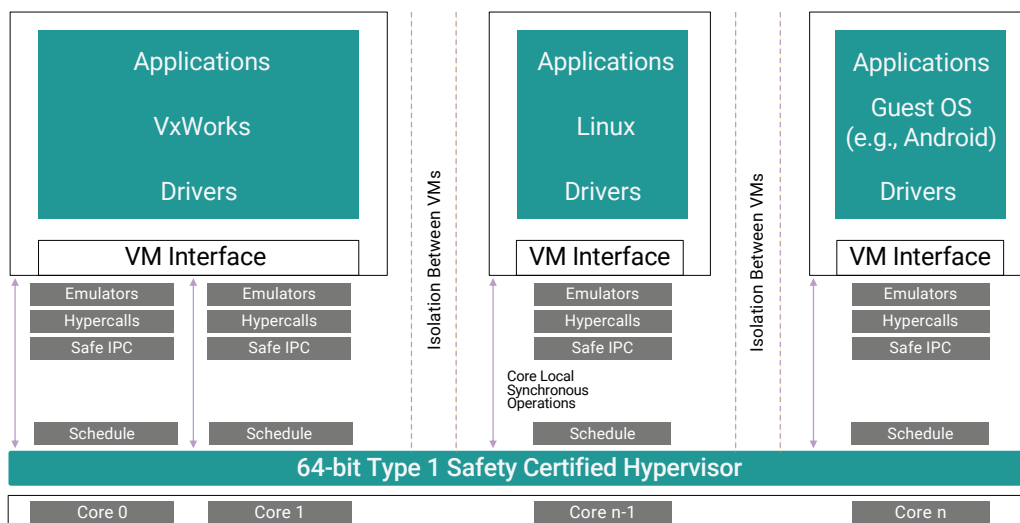

Figure 1. Isolate and protect your critical systems

Key outcomes:

- Bridge legacy, current, and future systems
- Run legacy applications at near-native performance levels
- Achieve savings in space, weight, power, and cost
- Consolidate and reuse application software
- Enable portability of applications to new hardware platforms

Mixed Safety-Criticality Systems

Manufacturers of safety-certified systems also need to consolidate some systems. To do this, developers need a safety-certified virtualization solution that can support guest operating systems and applications with mixed criticality and safety certification levels.
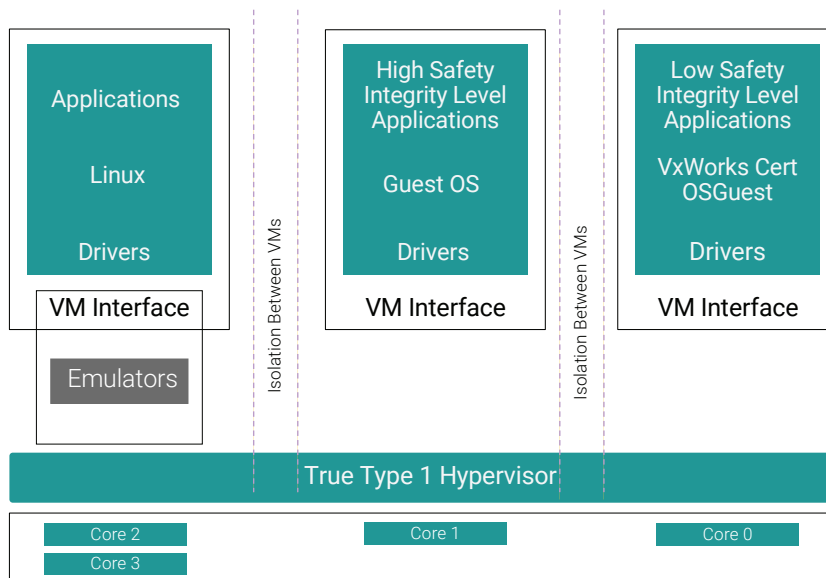

Figure 2. Safety-certified system with multiple levels of safety

Key outcomes:

- Consolidate applications of different levels of safety criticality
- Combine safety-certified and non-certified applications on one hardware platform
- Achieve savings in space, weight, power, and cost

Flexible Role-Based Development

On a large project, system configuration is the responsibility of more than one person. The platform and guest operating systems have different owners, and they are responsible for their own configurations. On a very large project, these different owners are different companies that could be competitors.

Using an XML configuration format with an independent build, link, and load (IBLL) system follows role-based development principles (such as those defined in the DO-297 standard for avionics) and allows true separation and independent development across platform provider, cert platform provider, application developers, and the system integrator. This provides maximum flexibility in distributing development roles according to their objectives and accelerates large-scale development of certified software systems.
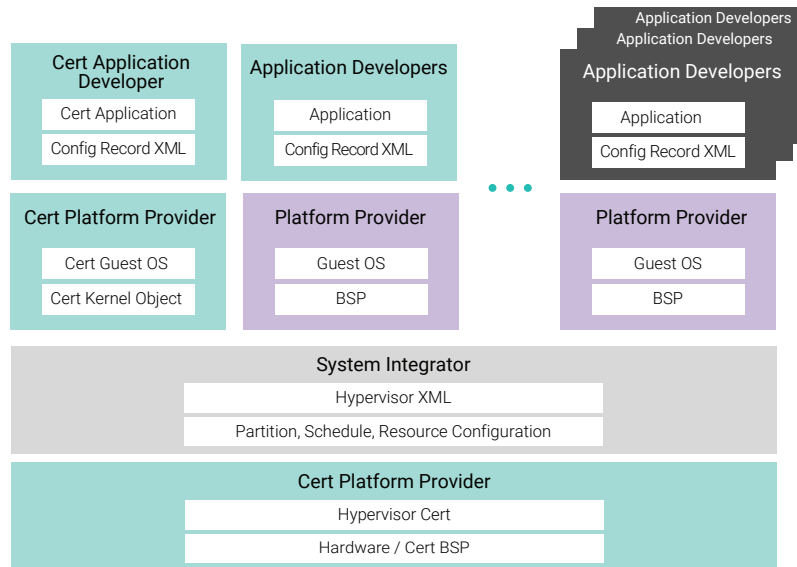
WNDRVR

Figure 3. Independent role-based development

Key outcomes:

- Allows application suppliers to asynchronously develop, test, and deliver software applications independently
- Independent supplier build process, reducing the impact of code changes across multiple development teams
- Ability to use VxWorks or Linux containers and standard cloud-native tools to further achieve application independence across complex systems

CORE CAPABILTIES AND BENEFITS

- 64-bit Type 1 Safety Certified Hypervisor
  — No service OS or special privileged VMs required
  — Real-time response times for deterministic guest OSes
  — Low overhead and near-native performance, even with large numbers of cores and virtual machines (VMs)
  — True operating independence between cores
  — Device emulators local to the VM
  — Lockless communication between VMs
  — Separate schedulers, local timers, local emulators
  — Deterministic configuration with assignment and management of devices, communication channels, and memory
  — Direct interrupt support
  — Small footprint
  — Robust partitioning (support for multiple levels of safety across VMs)

- Tickless kernel:
  — Timer interrupts do not occur at regular intervals but are only delivered as required
  — Real-time, deterministic performance and latency
  — Low overhead for the hypervisor
  — No ticks unless queued, meaning the range of lengths of time windows isn't limited by a system tick
  — No tick at all if there is only one VM
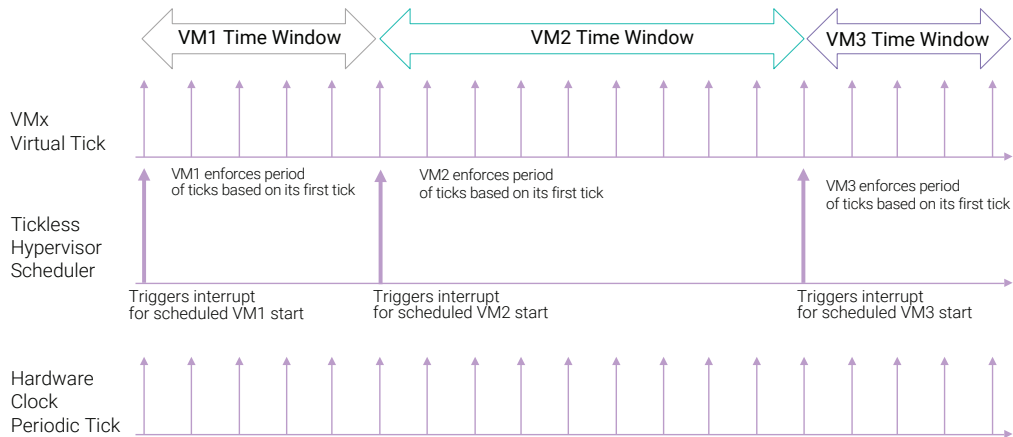 — Close to native performance

WNDRVR

Figure 4. Tickless unlimited time windows with interrupts delivered as required

- Time partition scheduler:
  - Schedules partitions or VMs according to a strict schedule
  - Allows configurable schedules with support for multiple VMs per core
  - Allows VMs to run only within a given window of time on a given core
  - Guarantees specific quanta of CPU time to each guest in a deterministic way
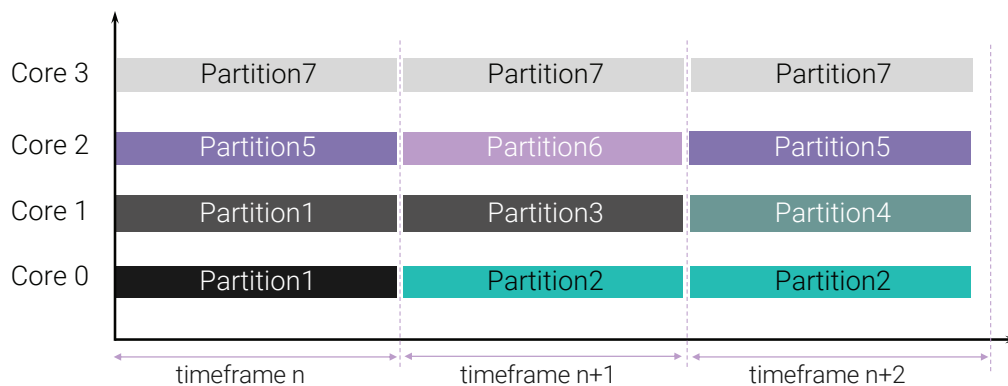 - Allows multiple schedules to be defined for a system and switched dynamically at runtime

Figure 5. Different partitions run simultaneously on different cores

- Direct interrupts and direct access to devices:
  - Direct interrupts offer near-native responsiveness because they go directly from the physical device to the guest operating system
  - Hypervisor is not involved in the data path to or from the device
  - When a guest is running in direct interrupt mode, there is no VM exit required, which improves interrupt latency
  - Memory, PCI attributes, and interrupts can be directly mapped into the guest operating system
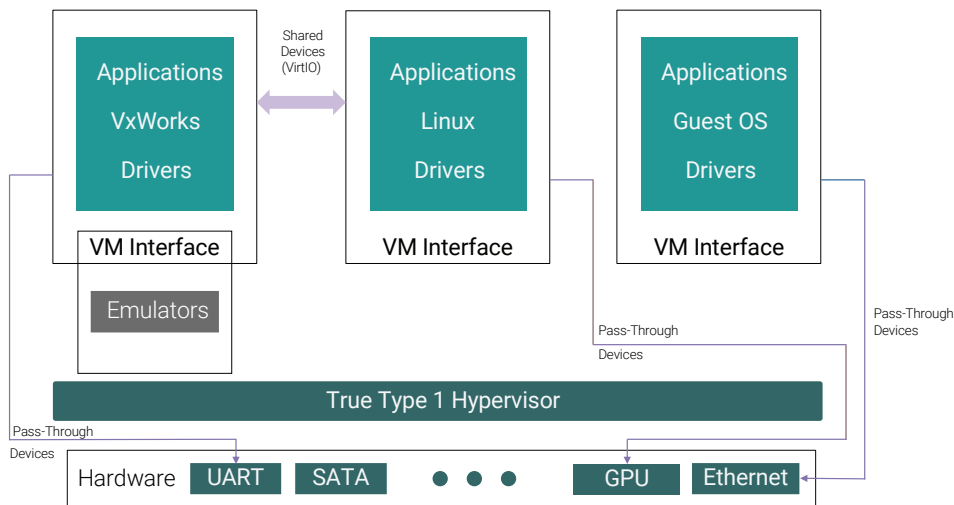
Figure 6. Direct interrupts and direct access to devices

- Scalability:
  — No limit on number of cores and guests
  — Performance is not compromised as the core count increases
  — Support for mixed criticality of guest operating systems
  — Unmodified guest support
  — Support for multi-core partitions/VMs
  — Out-of-the-box guest OS support for VxWorks, VxWorks Cert Edition, and Wind River Linux
  — Safe multi-OS communication (Safe IPC)

- Quality and performance-driven tools:
  — Platform debugger that supports system mode debugging of multiple VMs using the VxWorks RTOS, allowing a synchronized view across all VMs
  — Wind River System Viewer enables view of OS events across all VMs using VxWorks and the hypervisor, allowing developers to visualize and troubleshoot complex target activities
  — Boot profiler that provides a coherent view of the time spent in the hypervisor and the VM guest OS during initialization to allow focused boot optimization
  — Configurable health monitoring (ARINC 653 compatible), a framework that enables injection of events and provides customizable and configurable handlers and logging of those events
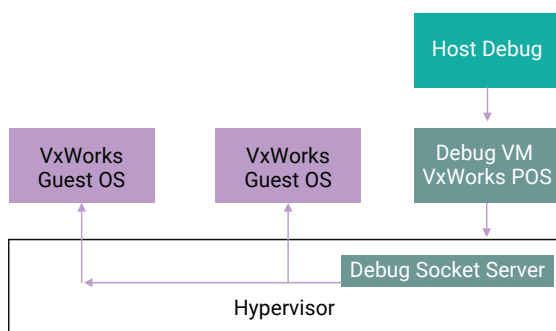

Figure 7. Platform debugger that supports system mode debugging of multiple VMs

WNDRVR

KEY FEATURES

- Guest OS support
  - VxWorks (included with Helix Platform)
  - VxWorks Cert Edition (safety-certified guest included with Helix Platform)
  - Wind River Linux (Linux binary included with Helix Platform)
  - Bare metal guests
  - Third-party guests
  - Guest operating systems that are virtualized with Helix Platform can support containers (including VxWorks and Wind River Linux)

- 100% of source code provided
  - Long product lifecycles

- Processor support
  - 64-bit processor support with 32-bit and 64-bit guest support
  - ARMv8 and Intel x86-64 processors
  - Includes support for SoCs from manufacturers including Intel, AMD, NXP, Aptiv, Texas Instruments, and Samsung

- Device emulation
  - Device tree
  - VirtIO
  - Shared memory
  - Virtual network interface (VNIC) over shared memory
  - Custom

- Safety certification
  - Supports mixed levels of criticality
  - Certification for DO-178C DAL A, IEC 61508 SIL 3, and ISO 26262 ASIL-D
  - 330 customers over 750 safety programs in more than 120 civilian and military aircraft

- Security
  - Support for DO-356A
  - Isolation and separation of guests
  - Resource access control
  - Intrusion protection through security policy configuration
  - Support for guest OS security features
  - Monitoring and remediation of MITRE CVEs

- Wind River Workbench development environment
  - Project build and configuration
  - System integration support
  - Independence for build, configuration, and packaging (IBLL)
  - Multiple projects for independent payloads, supported hypervisor projects type:
    - Workbench debugging
    - Helix Platform system debug (independent of cert)
    - Helix Platform System Viewer
    - Hypervisor (non-cert)
    - VxWorks Guest OS (non-cert)
    - VxWorks direct debug (non-cert)
    - VxWorks Direct System Viewer (non-cert)

- Build support within Wind River Studio

SAFETY CERTIFICATION

In its history of more than 40 years, Wind River has built an extensive portfolio of safety certification experience, with more than 600 programs in more than 100 civilian and military aircraft and more than 360 customers using the Wind River safety platform in automotive, aviation, and industrial safety-certified products. Wind River operating system platforms have been certified to meet ISO 26262 automotive safety, DO-178C avionics safety, and IEC 61508 industrial functional safety requirement standards.

Architecture and certification reduce total cost of ownership:

- Designed for simplified certification of safety-critical applications according to the stringent requirements of the DO-178C (DAL A) Software Considerations in Airborne Systems, IEC 61508 (SIL 3) industrial functional safety, and ISO 26262 automotive safety standards

WNDRVR

- Modular, open architecture employs robust partitioning that dramatically reduces retesting and recertification of an entire platform when a change is made to one of the partitions/VMs
- This reduces the total cost of ownership (TCO); new partitions can easily be added to any device without the typical retesting requirements of an entire system

WIND RIVER PROFESSIONAL SERVICES

The CMMI Level 3–rated Wind River Professional Services organization leverages years of system design and development expertise to work collaboratively with customer design and program teams. Professional Services interprets system requirements; architects platform options; and provides recommendations for meeting business, technical, and program goals. The Professional Services team also has a safety-critical services practice that can deliver safety certification evidence for additional software components, including certified board support packages (BSPs), middleware, and application software.

For more information, visit www.windriver.com/services.

WIND RIVER EDUCATION SERVICES

Wind River offers instructor-led, on-demand, and mentored learning, including our anytime, anywhere access to online subscription-based e-learning. For more information, visit www.windriver.com/education.

WIND RIVER CUSTOMER SUPPORT

Helix Platform is backed by the Wind River award-winning global support organization. We offer live help in multiple time zones, the online Wind River Support Network with multifaceted self-help options, and optional premium services to provide the fastest possible time-to-resolution.

For more information, visit www.windriver.com/services/customer-support.

WNDRVR