

SierraVisor

Embedded Virtualization

Changing the Development Landscape

Designers are increasingly turning to virtualization to satisfy reliability, security, and time-to-market requirements.

Running multiple operating systems concurrently allows manufacturers to rapidly migrate applications to new hardware; the hypervisor can hide device driver and system changes from the legacy software. Using multiple guest operating systems can also increase system functionality and improve high availability.

Virtualization offers a wide range of features and applications; SierraVisor from Sierraware allows designers to take advantage of these features by providing a powerful, dependable and high-performance hypervisor.

SierraVisor Hypervisor

Sierraware has developed a hypervisor that supports not one, not two, but three distinct modes of operation:

- Paravirtualization for ARM[®] TrustZone[®]-enabled devices
- Paravirtualization for ARM11 and Cortex-A9 devices
- Hardware Virtualization for Cortex-A15

SierraVisor allows equipment manufacturers to choose the right type of hypervisor for their processor architecture and virtualization requirements. With SierraVisor, multiple high-level operating systems, including Linux, BSD, Android, and legacy real-time operating systems, can run on a single host at the same time.

Supporting both paravirtualization and full hardware virtualization, SierraVisor can operate on any ARM11, Cortex-A9, or Cortex-A15 platform.

SierraVisor provides virtualized device and peripheral support, managed IPC communications, and a streamlined, secure architecture; application developers can use Eclipse and GNU tools for development.

SierraVisor Benefits

- Extends the life of applications by simulating the previous generation of hardware.
- Allows legacy real time operating systems to run simultaneously with Linux, BSD and Android.
- Streamlines development by supporting SMP and AMP process management.
- Reduces hardware costs by enabling a single device to perform multiple functions.
- Secures sensitive data with a Trusted Execution Environment available for every guest operating system.
- Offers flexible open source GPL and commercial license options.
- Supports I/O virtualization for graphics applications

Paravirtualization for ARM TrustZone

The SierraVisor Hypervisor leverages hardware security extensions included in ARM TrustZone-enabled devices to run multiple, high-level operating systems concurrently. The guest operating systems are aware of the fact that they are running on top of a hypervisor, so minor modifications must be made to the guest operating systems.

Because of enhancements built for TrustZone technology, SierraVisor can operate efficiently with minimal impact on performance. In addition, each high-level operating system instance can still access a secure operating system (or TEE) for sensitive applications and data.

Paravirtualization for ARM11 and Cortex-A9 without ARM TrustZone

SierraVisor extends virtualization capabilities to any ARM11 or Cortex-A9 platform. SierraVisor's paravirtualization technology minimizes modifications required for existing applications. A small number of non-intrusive hypercalls are inserted into the guest operating systems, reducing overhead. SierraVisor also offers robust multicore management, offering both symmetric and asymmetric multiprocessing for managing system utilization.

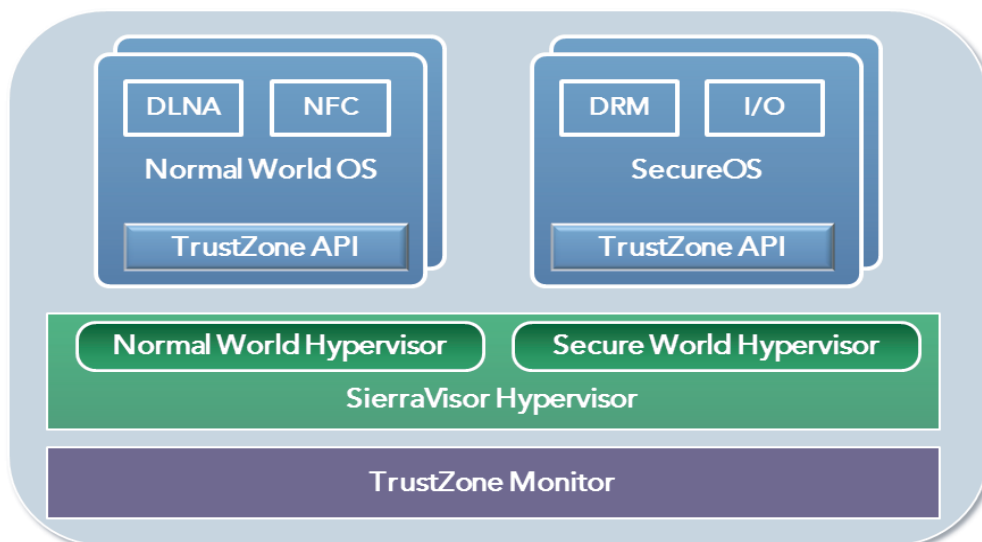
This mode of operation supports virtually all ARM-based systems currently in production today. However, it cannot match the high performance and low system impact of hardware virtualization.

Hardware Virtualization

With Cortex-A15, ARM introduced hardware virtualization support. The SierraVisor Hypervisor takes advantage of this new capability to provide true hardware virtualization. It requires no changes to the guest operating system and offers the higher performance and lower system impact than paravirtualization. The SierraVisor Hypervisor is ideally suited for equipment vendors that are developing next generation systems with Cortex-A15 processors.

Integration with SierraTEE Trusted Execution Environment

With both paravirtualization and hardware virtualization, guest systems can still access the secure world provided by ARM TrustZone technology, so each guest system can protect sensitive data like DRM applications, encryption keys, and NFC payment applications.



SierraVisor Hypervisor Architecture Diagram