

# Applying Virtualization to Embedded Devices

Ease software migration, improve real-time performance and enhance security

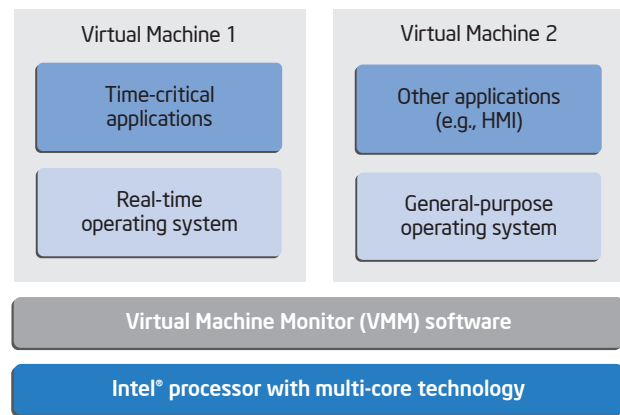
Today, most embedded systems use a single operating system (OS), typically either real-time, general-purpose or homegrown. Although one OS is sufficient for most devices, some developers are choosing to run multiple OSs in secure partitions using virtualization. This enables them to simplify the porting of legacy applications onto new platforms, increase the determinism of time-critical functions and improve the security and stability of safety-critical code.

Virtualization provides the ability to run multiple virtual machines (VMs), containing an OS and its associated applications, on the same physical board by abstracting the underlying processing cores, memory and devices. This is achieved by adding a new software layer, called a virtual machine monitor (VMM), which manages the execution of “guest OSs” in much the same way that OSs manage the execution of applications. Systems can run real-time and general-purpose OSs simultaneously, as shown in Figure 1, which provides both fast response for time-critical code and many standard features for application development. If the guest OS running the GUI crashes, the RTOS and the time-critical functions will continue to run deterministically because they are isolated and protected.

## Hardware-assisted Virtualization

Virtualization has been around for many years, most notably used in data centers where many applications are consolidated onto a single server. In recent years, Intel has developed different versions of Intel® Virtualization Technology<sup>1</sup> (Intel® VT) to improve the fundamental flexibility and robustness of software-based virtualization solutions.

**Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64<sup>2</sup> and Intel® Architecture (Intel® VT-x)** speeds up the transfer of platform control between the VMM and guest OSs by using hardware-assist to trap and execute certain instructions on behalf of guest OSs, relieving the VMM of such duties. These commonly used virtualization operations are very secure because they are performed in hardware and thus unalterable by hackers.



**Figure 1.** Embedded Virtualization Example

Capabilities	Benefits
Isolates applications in secure partitions	<ul style="list-style-type: none"> <li>Increases system reliability and stability</li> <li>Eases software migration and consolidation</li> </ul>
Runs RTOS on a dedicated processor core	<ul style="list-style-type: none"> <li>Improves real-time performance</li> <li>Decreases loop jitter, increases determinism</li> </ul>
Performs virtualization tasks in hardware	<ul style="list-style-type: none"> <li>Decreases VMM load on the processor</li> <li>Reduces VM to VM switching time</li> </ul>

**Table 1.** Intel® Virtualization Technology Capabilities and Benefits

**Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)** enables the VMM to securely assign specific I/O devices to specific guest OSs, where each device is given a dedicated area in system memory accessible only by the device and the designated guest OS. Hardware assistance speeds up data movement and lowers VMM activity, hence processor load, because the VMM is no longer involved in every I/O transaction.

**Intel® Virtualization Technology (Intel® VT) for Connectivity (Intel® VT-c)** optimizes the network for virtualization by integrating extensive hardware assists into Intel® 10 Gigabit Server Adapters used by servers, storage infrastructure and various external devices. By performing device queuing and PCI-SIG Single Root I/O Virtualization (SR-IOV) functions, Intel® VT-c speeds I/O delivery and reduces the load on the VMM.

## Addressing Software Challenges

By employing Intel VT, software developers have greater control over operating systems and applications with respect to their mix, performance and security. Virtualization addresses many design challenges, like migrating legacy software, increasing real-time performance and making applications more secure, as described in the next three sections.

### Ease Legacy Software Migration

Changing operating systems or porting legacy applications to a new OS often necessitates rewriting code and testing for software conflicts. In some cases, the legacy code may only exist in binary format or was written in assembly language, further complicating the software migration effort. Virtualization allows systems to execute legacy software, with little or no modification, in an isolated virtual machine, prevents it from interfering with other applications and protects it from unintended interactions with other applications.

### Increase Real-Time Performance

Many embedded systems, like industrial controllers and radar monitoring systems, require a combination of low-latency, deterministic response and full-featured user interfaces. Satisfying both objectives, virtualization and multi-core processors enable systems to simultaneously run real-time and general-purpose OSs (RTOS/GPOS), each on dedicated processor cores. This configuration can increase the speed and determinism of time-critical applications, because they operate unencumbered by non-real-time tasks that would otherwise compete for CPU resources.

### Improve Security with Application Isolation

Securing applications and data is essential for many embedded systems, such as railway traffic control systems protecting safety critical code, military laptops enabling multiple independent levels of security (MILS) and networked equipment preventing attacks from malicious software.

Platform Components	Required Capability
Processor	Intel® Virtualization Technology <sup>1</sup> (Intel® VT)-enabled
Chipset	Intel VT-enabled
Virtual Machine Monitor Software	Available from software vendors, such as Green Hills, LynuxWorks RTOS, TenAsys, VirtualLogix and Wind River
BIOS	Intel VT-enabled, available from AMI, Phoenix and Insyde

**Table 2.** Required Intel® Virtualization Technology Components

Applications requiring a higher level of security can be isolated in secure virtual machines (VM), whose memory space is protected by hardware features in Intel® processors and Intel VT. This means software running in a VM only has access to its own code and data regions, unable to page outside the memory boundaries specified by the VMM.

## Deploying Intel® Virtualization Technology

Intel VT is enabled by a number of hardware and software components, which are listed in Table 2, including Intel VT-enabled Intel processors and chipsets. Intel VT requires virtual machine monitor software and VT-enabled BIOS software.

For more information on Intel Virtualization Technology, visit [www.intel.com/technology/advanced\\_comm](http://www.intel.com/technology/advanced_comm).

Additional information about Intel® embedded products can be found at [www.intel.com/products/embedded/index.htm](http://www.intel.com/products/embedded/index.htm).

<sup>1</sup> Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

<sup>2</sup> 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit Intel Performance Benchmark Limitations.

Copyright © 2009 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others.

