In today’s highly competitive manufacturing environment, success requires a constant focus on cost cutting while maintaining production throughput and employee safety. For manufacturers, this includes finding new ways to lower operating expenses, a large part of which are the purchase and support of industrial systems. A significant cost stems from the inefficiencies created by the growing numbers and varieties of systems on the factory floor. For instance, system proliferation is consuming precious space and straining IT resources, especially when systems have unique support requirements for configuration, backups, spares and software patching.

Efficiency can be improved when multiple factory functions are consolidated onto a single hardware platform, thus decreasing operating expense, factory footprint, energy consumption, and integration and support effort. This can be done using advanced multi-core processors along with proven virtualization technology, which has been around since the 1960s and is most notably used in data centers where many applications are consolidated onto a single server. Still, virtualization tools and methods used in the server environment are different from what is appropriate for the embedded environment.

This white paper describes how virtualization technology running on multi-core Intel® Core™ vPro™ processors can be used in industrial automation to consolidate computing devices for motion control, programmable logic control (PLC), human machine interface (HMI), machine vision, data acquisition, functional safety and so forth. This approach can help manufacturers reduce cost and complexity on the factory floor.
Virtualization Basics
In traditional industrial automation systems, application software, the operating system (OS) and the physical hardware are tightly coupled. Virtualization breaks this link and provides the ability to run multiple OSes and their associated applications on the same physical board. This is achieved by executing software in individual partitions, called virtual machines (VMs), that are managed by a new software layer, known as the hypervisor or virtual machine monitor (VMM). The hypervisor abstracts the board’s underlying hardware resources (e.g., processor cores, memory and I/O devices), so each VM runs as if it had its own machine.

As a result, applications run on their native OSes (referred to as “guest OSes” in virtualization parlance), allowing them to easily migrate to a new system – often with only minor or no changes. To illustrate this capability, Figure 1 shows that four applications running on their own OSes and boards can be consolidated onto a single board with a multi-core processor and a hypervisor. The hypervisor manages the execution of guest OSes in much the same way an OS manages the execution of the applications it hosts.

Virtualization in Industrial Automation
Some industrial control systems are designed with multiple boards because they run applications like PLC, motion control, and HMI with different sets of requirements. PLC and motion control are time-critical applications, which are best served by a real-time operating system (RTOS) that delivers deterministic performance. In contrast, developers of HMI applications may prefer a general-purpose operating system (GPOS) supported by tools that ease the development of touch screen displays, rich graphics and multimedia.

Figure 1. General Virtualization Example
Figure 2 shows how a single board with virtualization technology can address all these requirements, as well as others discussed later. Multi-core processors with virtualization technology allow systems to simultaneously run RTOSes and GPOSes, each on dedicated processor cores. This configuration can increase the determinism of time-critical applications, because they operate unencumbered by non-real-time tasks that would otherwise compete for CPU resources.

**Benefits from Consolidation**

By consolidating devices using virtualization technology, original equipment manufacturers (OEMs) developing industrial automation solutions can provide substantial benefits to their customers, such as:

- **Lower overall solution cost:** Although a consolidated device may cost more than any of the individual subsystems, it should cost less to manufacture than the combined subsystems because it has a smaller bill of materials (BOM). In addition, virtualization makes it easier for OEMs to add new functionality to a system and expand their offerings.

- **Smaller factory footprint:** Consolidated equipment takes up less factory floor space than the individual systems it replaces.

- **Reduced overall energy consumption:** The power efficiency of Intel Core vPro processors, combined with system consolidation, can yield a solution that consumes less power than the individual systems combined.

- **Reduced integration cost:** By consolidating subsystems, OEMs effectively eliminate many integration tasks for their customers. For instance, the networking, cabling, shielding and configuration that connect multiple subsystems together are handled within the system.

- **Simpler to secure:** The consolidated approach decreases the number of computing devices that require security software and may eliminate some varieties of security solutions the factory must support. In addition, there are fewer devices for hackers to attempt to infiltrate, thus reducing the attack surface of the factory floor.

- **Easier system management:** When subsystems are consolidated, factory IT personnel have a smaller number of devices to install, provision and manage. Also, a consolidated system is likely to have more capable hardware and software than the subsystems it replaces, allowing for additional manageability options and capabilities.

- **Higher reliability:** The greater the number of systems, the larger the number of devices that can fail. Consequently, a consolidated system should have a better mean time between failures (MTBF) than the combination of subsystems it replaces. Furthermore, there are fewer spares for factories to carry, and maintenance and repair procedures are simpler – all ultimately leading to shorter downtimes.
Reduction Cost and Complexity with Industrial System Consolidation

Consolidating Systems on Multi-Core Processors
Multi-core architectures, such as Intel Core vPro processors, provide the computing power needed to consolidate industrial systems and deliver real-time, deterministic performance. Multi-core processor architecture allows OEMs to dedicate hardware-level computing resources to specific VMs, thereby enabling an RTOS to behave deterministically regardless of the applications running in the other VMs. In addition, developers can more easily reallocate system resources across cores as system needs change.

One of the key benefits of consolidation is improved resource efficiency, which is achieved through a multi-core architecture-based platform. An industrial solution that combines multiple subsystems on one platform requires just one computing system and power supply, which results in a smaller footprint, higher density, lower power consumption and a simpler design compared to multiple subsystems with their own hardware.

Hardware-Assisted Virtualization Technologies
Although virtualization is generally viewed as a software technology, hardware features have been added to processors to improve the performance and security of virtualization. For instance, Intel has enhanced the capabilities of virtualization technology with a complementary hardware-assist technology called Intel® Virtualization Technology (Intel® VT), an ingredient of Intel® vPro™ technology. It performs various virtualization tasks in hardware, like memory address translation, which reduces the overhead and footprint of virtualization software, and improves its performance. For instance, VM to VM switching time is significantly faster when memory address translation is performed in hardware instead of by software.

In addition, Intel VT increases the robustness of virtualized environments by using hardware to prevent the software running in one VM from interfering with the software running in another VM. Along these lines, virtualization helps avoid unintended interactions between applications by preventing one from accessing another’s memory space. Some of the key benefits of virtualization in industrial automation and other embedded applications are listed in Table 1.

With respect to performance, Intel has developed three different, yet complementary, virtualization acceleration technologies that span multiple platform components, including the processor, chipset and NICs:

Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) speeds up the transfer of platform control between the guest OSes and the hypervisor. In Intel® processors, it reduces virtualization overhead by eliminating the need for the hypervisor to listen, trap and execute certain instructions on behalf of each guest OS. When hypervisor interventions are required, it provides hardware support so handoffs between the hypervisor and guest OSes are faster and more secure.

Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) accelerates data movement by enabling the hypervisor to directly and securely assign I/O devices to specific guest OSes. Each device is given a dedicated area in system memory so data can travel directly and without hypervisor involvement. I/O traffic flows more quickly, with more processor cycles available to run applications. Security and availability are also improved, since I/O data intended for a specific device or guest OS cannot be accessed by any other hardware or guest software component.

Intel® Virtualization Technology (Intel® VT) for Connectivity (Intel® VT-c) performs PCI-SIG® Single Root I/O Virtualization (SR-IOV) functions that allow the partitioning of a single Intel® Ethernet Server Adapter port into multiple virtual functions. These virtual functions may be allocated to VMs, each with their own bandwidth allocation. They offer a high-performance, low-latency path for data packets to get into the VM. Intel VT-c, integrated in Intel® Ethernet NICs, enables improved networking throughput with lower CPU utilization and reduced system latency.

Improving Virtualization Performance
It’s possible to ensure the real-time performance necessary for consolidated factory automation solutions using Intel VT and an RTOS when several main issues are addressed. Foremost, it’s necessary to minimize the interrupt latency and the overhead associated with general-purpose processors. A major source of performance loss is from VM enters and exits, which typically occur when the hypervisor must service an interrupt or handle a special event. These transitions are expensive operations because execution contexts must be saved and retrieved, and during this time the guest is stalled.

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Isolates applications in secure partitions |  • Increases system reliability and stability  
  • Eases software migration and consolidation |
| Runs RTOS on a dedicated processor core |  • Decreases loop jitter  
  • Improves determinism |
| Performs virtualization tasks in hardware |  • Decreases hypervisor load on the processor  
  • Reduces VM to VM switching time |

Table 1. Intel® Virtualization Technology Capabilities and Benefits
Figure 3. Interrupt Impact

Figure 3 depicts the VM/Host enters and exits that could result from an external interrupt. In this case, the guest OS runs until an external interrupt arrives. Subsequently, there are a total of eight exits and enters before the guest OS is allowed to restart its stalled process. This overhead can become substantial since it’s not uncommon for I/O-intensive applications to have hundreds or thousands of interrupts arriving in a second. These constant disruptions cannot be tolerated with time-critical control applications because of the resulting degradation in performance, latency and determinism.

Intel has worked together with operating system vendors to reduce the typical interrupt latency from between 300 and 700 μS to sub 20 μS, achieving near-native performance (i.e., similar to non-virtualized) in a virtualized environment. This is possible through the implementation of hardware and software mechanisms that minimize the interrupt overhead inherent in a virtualized environment, some of which are described in the following:

- **Intel® Virtualization Technology FlexPriority**: When a processor is performing a control task, it often receives interrupts from other devices or applications. To minimize the impact on performance, a special register, called the APIC Task Priority Register (TPR), in the processor monitors the priority of tasks to prevent the interruption of one task by another with lower priority. Intel Virtualization Technology FlexPriority (Figure 4) creates a virtual copy of the TPR that can be read, and in some cases changed, by guest OSes without hypervisor intervention. This eliminates most VM exits due to guests accessing task priority registers and thereby provides a major performance improvement.

![Without Intel® Virtualization Technology FlexPriority](image1)

![With Intel Virtualization Technology FlexPriority](image2)

Figure 4. Depiction of Intel® Virtualization Technology FlexPriority
- **Virtual Processor IDs (VPID):** Previously, every time the hypervisor performed content switching between VMs, the active VM and its data structure had to be flushed out of the transition look-aside buffers (TLB) associated with the CPU caches. As a result, there was performance loss on all VM exits because the hypervisor did not know which cache line was associated with any particular VM.

With Virtual Processor IDs (VPID), the virtual machine control structure (VMCS) contains a VM ID tag that associates cache lines with each actively running VM on the CPU. This permits the CPU to flush only the cache lines associated with a particular VM when it is flushed from the CPU, avoiding the need to reload cache lines for a VM that was not migrated and resulting in lower overhead.

- **Guest Preemption Timer:** Programmable by hypervisor, this timer provides a mechanism to enable a hypervisor to preempt (i.e., halt) the execution of a guest OS by causing a VM exit when the timer expires. This feature makes it easier to switch tasks, fulfill real-time control requirements or allocate a certain amount of CPU cycles to a task.

- **Descriptor Table Exiting:** This feature enables a hypervisor to protect a guest OS from internal attack by preventing the relocation of key system data structures. This mechanism helps to better protect safety-critical applications.

- **Pause-Loop Exiting:** Spin-locking code typically uses PAUSE instructions in a loop. This feature detects when the duration of a loop is longer than “normal” (a sign of lock-holder preemption) and forces an exit into the hypervisor. After the hypervisor takes control, it can schedule another VM. Spin locks are often used in control applications for inter-process synchronization.

- **Virtual Advanced Programmable Interrupt Controller (vAPIC):** The hypervisor previously had to maintain a virtual APIC model in software for handling interrupts. This functionality is now implemented with microcode, called the vAPCI, which the guest can access without triggering a VM exit, as shown in Figure 5.

![Diagram of vAPIC implementation](image_url)

**Figure 5.** The vAPIC Implemented in Hardware
Single-Root I/O Virtualization (SR-IOV): The PCI Special Interest Group (PCI-SIG) specification, SR-IOV allows one NIC to service multiple VMs, as shown in Figure 6. The specification provides a standard mechanism for devices to advertise their ability to be simultaneously shared among multiple virtual machines. It also allows for the partitioning of a PCI function into many virtual interfaces for the purpose of sharing the resources of a PCI Express* device in a virtual environment.

Each virtual function can support a unique and separate data path for I/O-related functions within the PCI Express hierarchy. Use of SR-IOV in factory automation, for example, allows the bandwidth of a NIC to be partitioned into smaller slices that may be allocated to specific virtual machines, or guests, via a standard interface. This resource sharing can increase the total utilization of any given resource presented on an SR-IOV-capable PCI Express device, potentially reducing the cost of a virtual system.


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

<table>
<thead>
<tr>
<th>Platform Components</th>
<th>Required Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® Core™ vPro™ Processor</td>
<td>Intel® Virtualization Technology (Intel® VT)-enabled</td>
</tr>
<tr>
<td>Intel® Chipset</td>
<td>Intel VT-enabled</td>
</tr>
<tr>
<td>Virtual Machine Monitor Software</td>
<td>Available from software vendors, such as Green Hills*, LynuxWorks*, TenAsys*, Real-Time Systems* and Wind River*</td>
</tr>
<tr>
<td>BIOS</td>
<td>Intel VT-enabled, available from AMI*, Phoenix* and Insyde*</td>
</tr>
</tbody>
</table>

Table 2. Required Intel® Virtualization Technology Components

Figure 6. Technologies for Improving Virtualized I/O
The Path to Industrial System Consolidation

For product manufacturers, factory floor equipment plays a critical role in creating a competitive advantage with respect to manufacturing precision, throughput and cost. On the cost side, industrial system consolidation can have a large impact in reducing overall equipment cost, factory footprint, energy consumption, integration effort, security complexity and system support. This is achievable with virtualization technology, a powerful capability in Intel Core vPro processor-based platforms that allows OEMs to combine multiple devices found in today’s manufacturing environment into a single system. The path to lower cost and complexity is being blazed by Intel’s continual innovations in multi-core computing and virtualization technologies that help OEMs deliver higher performing and more robust industrial systems.

For more information about Intel solutions for industrial automation, visit www.intel.com/industrial

---

2. Intel® Virtualization Technology (Intel® VT) 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.
3. Performance estimates are based on internal Intel analysis and are provided for informational purposes only.
4. 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 http://www.intel.com/performance/resources/limits.htm.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core and Intel vPro are trademarks of Intel Corporation in the United States and/or other countries.
*Other names and brands may be claimed as the property of others.