Leveraging Virtualization in Aerospace & Defense Applications

Overview
For C4ISR Aerospace & Defense applications,1 the popularity of ATCA is growing rapidly because it addresses the key requirements of next-generation systems while creating opportunities to reduce SWaP;2 increase functionality and accelerate time to market. These benefits can be expanded further through the implementation of virtualization—a complementary technology that provides better performance on multi-technology, enables multiple applications to safely work on a single blade, eases legacy software migration and facilitates software failover, among other usage models.

Virtualization has been around for many years, most notably used in data centers where various applications are consolidated onto a single server, thereby reducing the total number of servers and overall power consumption. Although the adoption of virtualization in Aerospace & Defense is still in its infancy, system developers are beginning to take a closer look at the wide range of problems this technology helps to solve.

From the perspective of Aerospace & Defense, this paper reviews some of the more interesting virtualization usage models and implementation insights arising from real-world projects involving Radisys engineers.
Virtualization Basics

Virtualization provides the ability to run multiple operating systems (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 separated from the underlying hardware resources. 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.

At the heart of virtualization is the virtual machine monitor (VMM, aka “hypervisor”), which is a software layer that abstracts the hardware and manages guest OSES in much the same way that a standard OS manages the execution of its applications. For example, the VMM in a Mobile Command Center may create VMs for battlefield communication and sensor processing running on Linux, and another VM for email and other office applications running on Microsoft Windows Server 2008, as illustrated in Figure 1. With virtualization, software applications share computing resources, therefore fewer servers are needed, reducing the size, weight and power consumption (SWaP) of mobile command centers. In addition to software consolidation, virtualization supports other usage models, some of which are described in the following section.

Usage Model 1: Consolidating Applications

Situation: A Mobile Command Center, with a similar role as a traditional data center for enterprise applications, moves on a regular basis. Therefore, the system should be relatively compact and lightweight, and rugged enough to handle packing and shipment over rough terrain.

Solution: Decrease the number of required server boards by consolidating several applications onto fewer servers. This creates an opportunity to use a smaller ATCA chassis, and decrease weight and power consumption, thereby reducing SWaP.

![Figure 1. Consolidating Applications on a Mobile Command Center](image-url)
Virtualization Usage Models in Aerospace & Defense

Virtualization is a versatile technology that gives software developers greater control over operating systems and applications with respect to their mix, porting and security. The following describes four virtualization usage models suitable for server-based Aerospace & Defense systems.

Simplify Legacy Software Migration

When it comes to legacy code in many military applications, a common perspective is, “If it ain’t broke, don’t fix it.” Unfortunately, it’s not always that simple.

When adopting new processing blades, many times it is necessary to migrate to a new operating system. This will require the legacy applications to be ported, which often necessitates rewriting and retesting the code. This rework may even be required when using the same OS vendor whose new OS isn’t 100% backward compatible with earlier versions. Further complicating migration, legacy code written in assembly language is likely to be single threaded and therefore unable to take advantage of the performance improvements of multi-core processors.

Overcoming these challenges, virtualization allows systems to execute legacy software with little or no modification. Legacy code runs on its native OS in an isolated VM, as shown in Figure 2, which also protects it from unintended interactions with other applications. Furthermore, multi-core processors can be fully utilized since the VMM uses all the available processor cores to support the VMs.

Usage Model 2: Migrating Applications without OS Porting

**Situation:** A legacy intelligence, surveillance and reconnaissance (ISR) application, running on a near real-time operating system (RTOS), acquires and processes radar images. The software is part of a new platform that is Linux-based.

**Solution:** Use Virtualization to enable the legacy ISR application to run unmodified on its own in a VM.

---

**Figure 2. Running an ISR Application Unmodified on a New Platform**

![Diagram](attachment:fig2.png)
Implement Fast Software Failover

When the operating system or application crashes, the standard remedy is a hardware reboot, which takes the system offline for a period of time. With virtualization, a failing operating system or application doesn’t have to be catastrophic since it is isolated in a VM. One option is to restart the software in the failing VM without impacting the other VMs; however, this approach does not address a corrupted software image. Therefore, a more robust solution is to maintain a backup VM (e.g., identical software) in standby mode that is ready to take over in a matter of seconds, as illustrated in Figure 3.

Using Virtualization for High Availability

Working behind the scenes, middleware provides high availability and management functions that are critical when building highly reliable systems. One of its key functions is to detect faults and manage failover to ensure continuity of service. Historically, most middleware has been closely coupled to a specific hardware platform and application, thus changing the hardware or adding new applications makes it necessary to modify the middleware.

Many of the commercial virtualization offerings provide middleware-like features that focus on the application, but not the hardware. The virtualization software monitors the application, and if it detects deteriorating performance, it can take action such as provisioning a new virtual machine for the application to run on a separate server. Some offerings support a fault tolerant model where a secondary VM runs in lockstep with the primary VM. If the performance of the primary VM degrades, the virtualization software can failover to the secondary VM. While the failover is not typically measured in milliseconds, in many cases it is fast enough.

Usage Model 3: Failing Over to a Backup Virtual Machine

**Situation:** The operating system hangs, requiring the system to undergo a full reboot.

**Solution:** Use Virtualization to create a backup VM that is called into action in the event of software failure, thus greatly speeding up system recovery.

![Figure 3. Primary and Backup VMs Provide Robust Failover](image-url)
Improving Security with Application Isolation

Securing applications and data is essential for many Aerospace & Defense systems, whether to prevent attacks from malicious software or to enable multiple independent levels of security (MILS). Applications requiring a higher level of security can be isolated in a VM, whose memory space is protected by hardware in Intel® processors, which is detailed in the next section. This means software running in a VM only has access to its own code and data regions (Figure 4), unable to page outside the memory boundaries specified by the VMM. Similarly, virtualization can provide greater protection against rogue software attempting to infiltrate a system’s data and programs.

Virtualization in a Ground Control System

A military equipment manufacturer migrated its ground station controller design from rackmount servers to ATCA architecture in order to make it easier to scale features and performance by adding blades that support new applications or more computing power. The manufacturer also virtualized the system, which further added software flexibility by allowing more applications to be consolidated on a blade. As a result, consolidation through virtualization enabled the system to run on fewer servers, going from ten to eight boards. Consequently, system power consumption and weight decreased by 15 and 12 percent respectively, thus reducing two facets of SWaP.

Hardware-Assisted Virtualization

Although virtualization is generally viewed as a software technology, some CPU makers have added hardware features to their 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). 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 protect 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. Hardware-assisted virtualization is going beyond the processor, with enhancements made to other platform components, including the chipset and network interface controllers (NICs). This is why Intel developed three different, yet complementary, virtualization technologies that are described in the following.

Usage Model 4: Securing the Execution Environment

Situation: A Mobile Data Center maintains various applications requiring different security clearances. However, the operating system may be vulnerable to malware that runs at the same privilege level.

Solution: A VMM can be written to run a standalone at a higher privilege level than the guest OSes and application, giving it exclusive access to page tables in the processor.
**The Processor: Intel® VT-x**

Intel VT-x helps to improve the fundamental flexibility and robustness of software-based virtualization solutions. It reduces VMM interventions by eliminating the need for the VMM to listen, trap and execute certain instructions on behalf of the guest OS as is required in software-only virtualization. By providing hardware support for transferring platform control between the VMM and guest OSes, Intel VT-x enables the VMM to switch guest OSes faster, more reliably and more securely.

**The Chipset: Intel® VT-d**

Intel VT-d speeds data movement and eliminates much of the performance overhead associated with managing I/O traffic in a virtualized environment. It accomplishes this by enabling the VMM to securely assign specific I/O devices to specific guest OSes. Each device is given a dedicated area in system memory that can be accessed only by the device and its assigned guest OS.

**Network Interface Controllers: Intel® VT-c**

Intel VT-c is a collection of technologies integrated in Intel® Ethernet Network Controllers that sort and queue traffic in hardware, resulting in fewer VMM interrupts. The end result is packet delivery to VMs is sped up and the load on the VMM is reduced. Intel VT-c can more than double I/O throughput and achieve near-native throughput for virtualized applications, so more applications can be consolidated per device with fewer I/O bottlenecks.

**Virtualization Software: What to Look For**

Developers can choose from a wide range of software solutions that provide virtualization. The two basic options are deploying a commercial offering and building your own solution based on open source software. While commercial solutions have licensing fees, they will significant reduce development cost for most applications.
The stand-alone VMM, also referred to as a bare metal hypervisor, must contain device drivers and is solely responsible for controlling the hardware after boot. This is more of the “Do it Yourself” option, which will require more effort, but also offers more control, achieves higher performance and is lower cost.

At the risk of greatly oversimplifying a rather complex set of virtualization solutions, Table 1 lists considerations and generalizations about some of the options available to developers.

**Virtualization: Implementation Learnings**

Although the benefits derived from virtualization are similar for enterprise and aerospace/defense (A/D) data centers, some of the requirements differ dramatically. For example, mobile A/D systems may be completely shut down and then turned back on several times a day, whereas most typical data center servers are only powered off for planned maintenance. A/D systems must consistently power down without issues or corruption of data, as well as meet hard requirements for startup and shutdown times.

Another difference is A/D requirements for ease of serviceability are often more rigorous than enterprise data centers—given that soldiers in the field may have less experience and fewer available resources than in-house IT departments. While soldiers operating virtualized systems are highly trained, they typically have the same skill level as a network planner with 10 years of experience. Therefore, A/D systems should have relatively simple user interfaces for start up and shut down.

Going a little deeper technically, Radisys engineers have highlighted some key learnings from deploying virtualization on ATCA-based systems for aerospace/defense applications:

<table>
<thead>
<tr>
<th>Considerations</th>
<th>OS Hosted</th>
<th>Stand-alone VMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of OS support out of the box</td>
<td>More options</td>
<td>Fewer options</td>
</tr>
<tr>
<td>License fees</td>
<td>Higher</td>
<td>Lower or free (Open Source)</td>
</tr>
<tr>
<td>Latency (e.g., VM to VM switching)</td>
<td>Higher</td>
<td>Lower (better)</td>
</tr>
<tr>
<td>Integration effort (i.e., drivers)</td>
<td>Lower</td>
<td>Higher</td>
</tr>
<tr>
<td>Software privileges</td>
<td>VMM privilege same as Host OS</td>
<td>VMM privilege higher than all other software</td>
</tr>
<tr>
<td>Middleware availability</td>
<td>More choice</td>
<td>Less choice</td>
</tr>
</tbody>
</table>

Table 1. General Considerations for Virtualization Software

**Managing the System**—In order to achieve interoperability between system components for traditional data centers and ATCA solutions, it may be necessary to map features from their respective platform management specifications. ATCA platform management leverages the Service Availability Forum, which is an open standard defining an application programming interface (API). Similarly, data centers often manage platforms according to the Distributed Management Task Force (DMTF) specifications. Simply put, the APIs for both specifications need to be merged, and one way to accomplish this is with a mapping/translation scheme.

**Virtualizing the Entire System**—Virtualizing single board computers today is straightforward since most have standard virtualization packages that already support the on-board silicon components. However, other parts of the system, such as switching, storage and some of the unique I/O used by A/D applications, are typically not supported by the virtualization software. This needs to be considered in the overall system design.

**Powering Systems On/Off Gracefully**—Compared to a data center, a chassis for an aerospace/defense application needs to power on/off gracefully and rather quickly. This may require careful scripting of the platform management software to ensure the different hardware and software components are shut down and brought up in the correct order.
Virtualization-Ready ATCA Blades

Getting the most out of a virtualized system requires a high performance compute blade capable of running many applications simultaneously. Ideal for mobile, server-centric installations, the Radisys XE80 compute blade is a single slot AdvancedTCA computer module based on a dual socket Intel® Xeon® processor L5638 or Intel® Xeon® processor E6545. The XE80, pictured in Figure 6, supports 10-Gigabit fabric connectivity and eight DDR3 DIMM sockets.

The XE80 compute blade provides the highest performance possible in a single slot. The blade can execute up to 24 concurrent software threads since Intel® Hyper-Threading Technology allows each of the 12 cores to process up to two threads simultaneously. Support for eight DIMMs of DDR3 allows memory density of up to 64GB, while providing a cost effective solution for applications that have lower density memory requirements.

The XE80 is available as a fully validated component in the Radisys family of platforms, which include 2, 14 and 16 slot platforms. It is fully interoperable with Radisys DSP, packet processing and switch products, and has been validated with various storage components.

Built Tough

Lowering risk for equipment manufacturers, Radisys offers prevalidated ATCA systems that demonstrate compliance to airborne, ground mobile and seaborne application requirements. These systems also meet 810 requirements for ground transportation and airborne uses. In some cases, ATCA boards and chassis were further ruggedized (e.g., conformal coating) to satisfy MIL-STD specifications.

Radisys has extensive experience with virtualization, including integrating VMware vSphere software into ATCA systems for Aerospace & Defense customers. These projects transitioned systems from a traditional ATCA environment to an environment where all the boards are virtualized.

Radisys’ portfolio of ATCA products includes single board computers (SBCs) based on the latest Intel processors, 40G switching, packet processing and DSP products. Using Radisys Trillium Software, in conjunction with ATCA products, allows customers to reduce their development cost and time-to-market when developing battlefield communications systems, such as femtocells and collapsed Evolved Packet Core (EPC) networks for mobile 3G/4G/LTE.

Deploying Virtualization on ATCA

ATCA is enabling aerospace/defense equipment manufacturers to build highly ruggedized and reliable systems within a multi-vendor compatible environment. Intent on lowering cost, improving SWaP and increasing software flexibility, system developers are turning to virtualization technology. Save time and get the most out of virtualization by taking advantage of Radisys’ extensive ATCA experience, aerospace/defense application understanding and close engineering relationship with Intel.

References

1 C4ISR: command, control, communications, computers, intelligence, surveillance and reconnaissance

2 SWaP: size, weight and power

Corporate Headquarters
5435 NE Dawson Creek Drive
Hillsboro, OR 97124 USA
503-615-1100 | Fax 503-615-1121
Toll-Free: 800-950-0044
www.radisys.com | info@radisys.com

©2011 Radisys Corporation.
Radisys and Trillium are registered trademarks of Radisys Corporation.
*All other trademarks are the properties of their respective owners.