WHITE PAPER

Brian Carlson
OMAP 5 Product Line Manager
Member of Group Technical Staff (MGTS)
Wireless business unit

TEXAS INSTRUMENTS

Going "beyond a faster horse" to transform mobile devices

Introduction

We are in the early stages of a mobile device revolution that is dramatically changing our lives. Mobile devices have become a digital extension of ourselves that we increasingly depend upon throughout the day. They are redefining how we communicate and socialize with others, learn about and navigate the world around us, capture ife moments, entertain, transact business and much more. They are primary devices we depend on for our computing needs, and the first devices we often interact with when we wake up in the morning. We are witnessing the start of the next generation of computing that was dominated by personal computers over the past two decades.

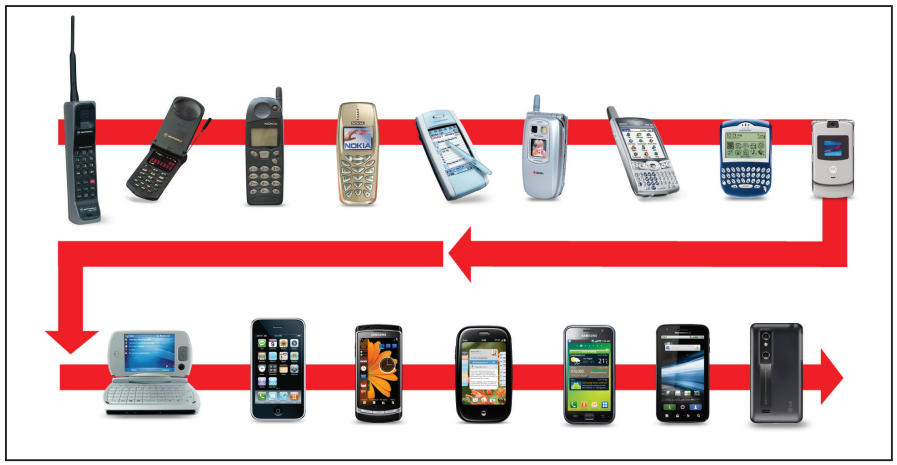
The game is changing and the technology that is enabling it is changing quickly to meet consumers' insatiable appetite to do more with the devices they carry with them. The "always-on" mobile computing experience is in demand, along with the desire for more performance, better user experiences and more applications.

There are continual technological improvements that make these mobile devices more capable. However, the TI OMAP™ 5 platform, one of the first applications processors based on ARM® Cortex™-A15 MPCore™ processors, not only brings a new level of performance, but more importantly, extends capabilities to enable new use cases that will truly transform mobile devices.

This paper focuses on some of the key new capabilities of the Cortex-A15 processor that will help drive the transformation of mobile computing.

Mobile device evolution

Mobile devices have evolved from a wide variety of technological advancements, driven by strong consumer demand. Figure 1 below shows examples of mobile device evolution. These examples illustrate the innovations that have transformed them including digital technology, color displays, touchscreen, cameras, keyboards, innovative form factors, high-performance CPUs, multimedia accelerators, pico-projectors and stereoscopic 3D (S3D) capture and display capabilities.



▲ ***Figure 1*** *– Mobile device evolution through the years*

The Next Disruptive Technology

Major disruptions from new technologies have changed the course and applications of mobile devices dramatically over the years. The next major disruption is a processor technology that elevates performance levels and capabilities to an extent that enables new operational environments, use cases and user experiences – all within mobile power budgets. The capabilities and extensions of this new processor technology set the stage for future software innovations in mobile devices, transforming them from content-consumption devices to content-creation devices that can serve as our primary computing devices. This disruptive processor technology is the ARM Cortex-A15 MPCore processor.

The Cortex-A15 processor takes mobile computing to the "next level," as it offers a substantial performance increase due to several key design enhancements compared to the previous generation Cortex-A9 processor. The Cortex-A15 processor also provides several

key new features that support more advanced system-level support, including extended physical addressing extension, hardware virtualization, improved debug/trace, soft-fault recovery and AMBA® 4 bus that enables system coherency.

Table 1 provides a high-level overview of some of the key enhancements, features and benefits of the Cortex-A15 processor relative to the Cortex-A9 processor that is now coming to the market in high-end mobile devices.

Enhancements	New features	Key benefits
128-bit (vs 64) load/store path **3-inst (vs 2) instruction decode** **8-micro-ops (vs 4) issue** **64-byte (vs 32) cache line** **Simultaneous load + store** **Improved brance prediction:** • Higher capacity • Support for indirect branches **More out-of-order instructions** **Optimized level 1 caches** **Tighter integration with NEON/ VFP** **Improved memory performance:** • Tightly-coupled L2 cache reduces latency • Enhanced auto-prefetch • More requests buffering	**Virtualization support:** • Virtual interrupt controller • Second stage MMU for Hypervisor control of guest OS memory • CP15 trapping **Extended physical addressing (up to 40 bits)** **Debug/trace support:** • Integrated trace • Virtualization support **Reliability and soft-fault recovery support** **AMBA4 bus supports:** • System coherency • MMU coherency	**In the same process node:** • >1.5x single-thread performance • >1.6x floating point and media performance • Improved multiprocessing bandwidth • Improved streaming performance • Advanced system support – Hardware virtualization – Larger memory – System coherency
Cortex-A15 offers substantial enhancements and new features to dramatically increase performance and system-level support		

▲ ***Table 1*** *– Cortex-A15 processor enhancements/features/benefits*

These enhancements focus on improving the processing throughput and efficiency of the core by supporting wider paths, more parallelism, tighter integration and various optimizations. The details of all these processing enhancements are out of the scope of this paper, and can be found in ARM papers and documentation.

This paper will later focus on two new features that will significantly benefit mobile devices and extend the software they can support: hardware virtualization and larger physical address extension.

Before addressing these new features, it is important to note the significant boost in performance and improved energy efficiency that the Cortex-A15 process delivers.

Performance and energy efficiency

The Cortex-A15 processor includes an extensive list of enhancements that result in single-thread performance improvement of 1.5x and floating point and media performance of 1.6x relative to the Cortex-A9 processor in the same process technology. The Texas Instruments Incorporated (TI) Cortex-A15 implementation is in a low-power, 28nm process that provides additional frequency and power improvements over the Cortex-A9 implemented in 45nm. In general, you should expect a 2-3x peak processing improvement when going from one generation of mobile device to the next when using the Cortex-A15 processor.

It is important to note that a Cortex-A15 processor clock frequency cannot be directly compared with Cortex-A8 or Cortex-A9 processors because of architectural and instructions per cycle (IPC) differences. For

example, with its 1.5x single-thread performance improvement, a 2GHz Cortex-A15 processor could provide equivalent performance of a 3GHz Cortex-A9 processor. Memory architecture and sizing can also have a big impact on the actual performance that is achieved in end products. Performance and power comparisons should come from application benchmarks rather than using frequency and mW/MHz numbers directly.

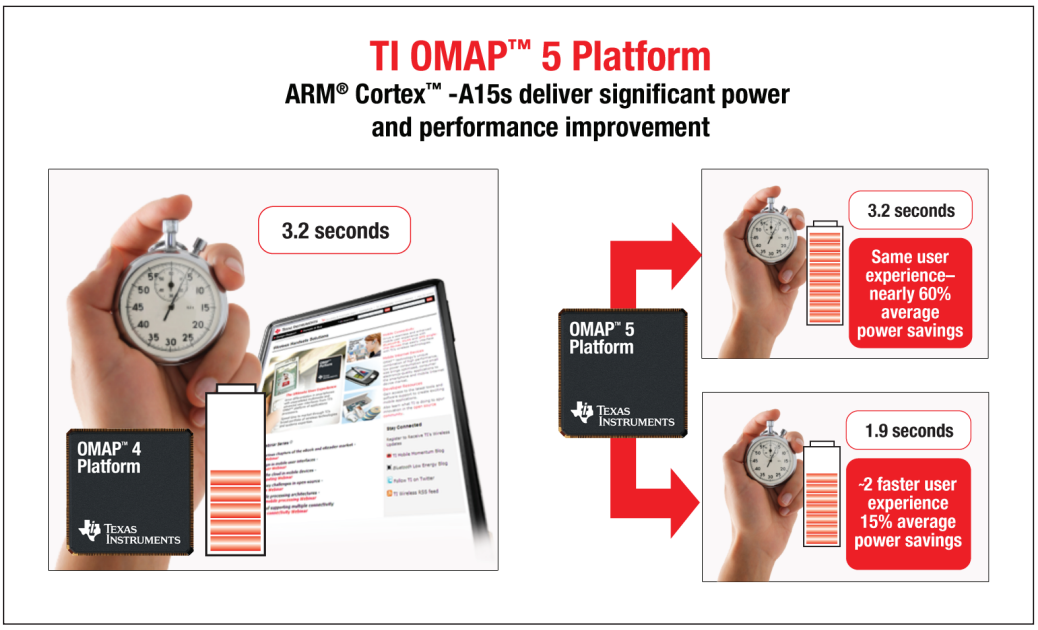
The TI OMAP™ architecture team has done extensive analysis to compare various multi-core configurations of Cortex-A9 and Cortex-A15 processors to see how they differ in performance. This is a very complex process since there are many variables and system interactions involved. For example, you have to consider the shared L2 cache size sensitivity with different types and number of cores, processor efficiencies, cache miss/hit rates and more. You also have to consider the level of available software parallelism and how this can mapped to different numbers of cores. In the end, TI has found that a dual-core Cortex-A15 configuration outperforms a quad-core Cortex-A9 configuration. When you also consider the system enhancements and what you can do with a device based on Cortex-A15 that you can't do with Cortex-A9, the Cortex-A15 is very attractive. TI recently announced the OMAP 5 applications processors, which are based on the Cortex-A15 MPCore technology to power best-in-class mobile devices in 2012.

Performance cannot be a sole metric when evaluating a processor for a mobile device such as a smartphone that must run on a battery in the typical range of 1000-1500 mAh. The mobile device world is very different than the PC world that was driven by performance without the extreme constraint of milliwatts power ranges that is required for all-day usage and multi-day standby. In mobile devices, you have to provide the maximum performance possible, while respecting the limitations of the physical/thermal and battery capacity of mobile devices. Typically there is a maximum system power limitation of 2.5-3W for mobile devices since they are small, contained (no fans) and the temperature of the device cannot rise to a point of discomfort for consumers. This power budget not only includes the processor, but other cores in the applications processor like graphics and video, as well as the other system components like the display/backlight, modem, RF and other components which can be significant contributors.

The processor in a mobile device works in a very dynamic way with extended periods of time in standby mode (still on and able to come up immediately), but also with use cases like web browsing that are processing-intensive bursts, as well as processing-intensive, sustained use cases like gaming. With such a complex operational profile, you have to look at use cases and all-day profiles of the device to properly evaluate the energy efficiency.

The Cortex-A15 processor exhibits a unique ability to not only provide a 2-3x boost in performance over previous generation processors, but also to harness this processing efficiency to lower energy consumption and extend battery life.

TI has determined that you can provide the same user experience, but do it with nearly 60% less average power by taking advantage of the Cortex-A15 processing efficiency relative to the Cortex-A9. This allows the TI OMAP 5 platform to offer a range of significant power and performance improvements as shown below.



Hardware virtualization

A significant new feature provided by the Cortex-A15 processor is hardware virtualization support, opening up a significant opportunity for power and performance-efficient, multiple guest operating system (OS) support. The ability for a mobile device to host multiple, guest operating systems or services is a game-changer because it can enable many new operational scenarios and flexibility that benefits the entire ecosystem.

Before getting into the details of virtualization, let's step back first to introduce the concept itself. Virtualization can be implemented in software, hardware or a hybrid model to manage the operational behaviors of multiple software domains. Virtualization increases the platform robustness and improves the resource sharing between these software domains. One example could be to have a device that is running a high-level OS like Android or Linux, while also running a real-time OS on the same processor or cluster. Virtualization enables these to work together on the same platform.

There are two main approaches to implement virtualization called para-virtualization in which software is used to simulate underlying hardware and hardware virtualization that uses built-in hardware in the processor. Para-virtualization requires guest OS kernel modification and also has more software layers. Hardware virtualization has an advantage of being able to host guest OS kernels without modification. This is important; as it minimizes the development work involved for faster time-to-market and can allow consumers to add new OSes and services to their devices – giving a lot of flexibility.

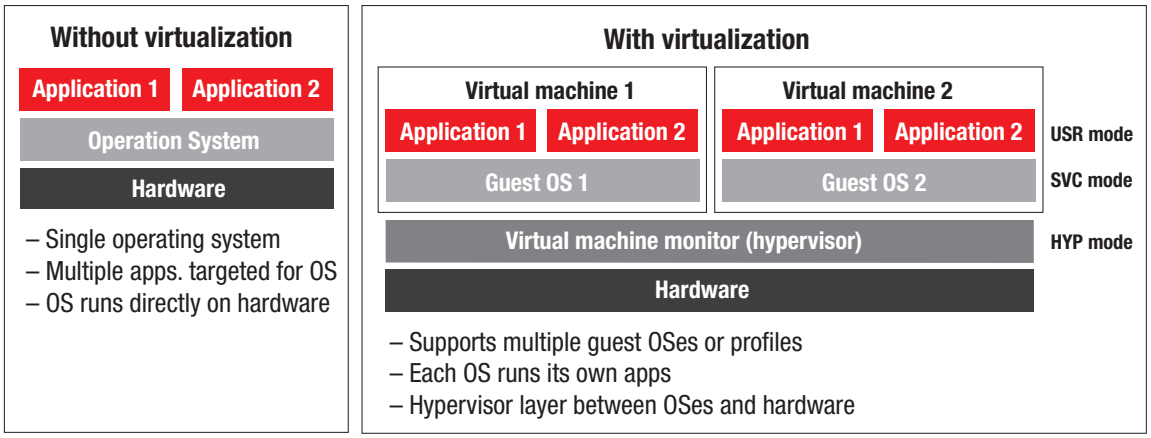
Three key requirements of virtualization were defined in a 1974 ICM paper called "Formal Requirements for Virtualizable Third Generation Architectures" by Popek and Goldberg[1]. They include:

Equivalence/Fidelity – Program runs essentially identical to that when running on equivalent machine directly

Resource Control/Safety – Hypervisor has complete control of the virtualized resources

Efficiency/Performance – Dominant fraction of machine instructions must be executed without intervention

An example of virtualization is shown in Figure 2 below.



▲ ***Figure 2*** *– Comparison of "without virtualization" and "with virtualization"*

It can be seen that without virtualization, a single operating environment running applications designed for that operating system runs on a hardware platform. With virtualization, you can have multiple guest OSes (supervisor mode), each able to run applications (user mode) designed for them with the addition of the Virtual Machine Monitor or Hypervisor that runs in a third hypervisor mode. The benefits of supporting multiple OSes will be discussed later, but they are significant and directly impact mobile device uses and capabilities.

Virtualization provides benefits to the entire ecosystem, including the developer, original equipment manufacturer (OEM), operator, business and consumer. This is a very important point, as it highlights the real value that spans all parties. Table 2 summarizes the benefits provided to each party by virtualization.

Party	Benefits
Developer/OEM	• Leverage legacy software investment • Faster development in virtual environment • Rapid deployment of new device variants
Operator	• Eases device management regardless of OS • Freedom for more differentiation • Maintain legacy services with new OS(es)
Business	• Improved security/isolation (corporate data) • Reduced cost of device management
Consumer	• Freedom of phone selection • Choice of OS or multiple OSes • Converged device – personal and work

▲ ***Table 2*** *– Virtualization benefits to the entire ecosystem*

Hypervisor support enables multiple software environments on a platform that provide real benefits as shown above. These software environments can be diverse, including running multiple operating systems, but also low-level real-time operating systems (RTOSes) for baseband processing or other system chores and also lightweight environments for specialized processing like shared device drivers, security code…).[2]

Below are a few examples of new mobile device use cases that can be enabled. There are many more that can transform the use of mobile devices.

Personal and work profiles on your device – Allows users to have one device for both purposes, while separating personal and confidential data in each profile from each other. This is important for businesses that have enterprise security concerns. It also can enable workers a choice of phone, not just one(s) mandated by the employer.

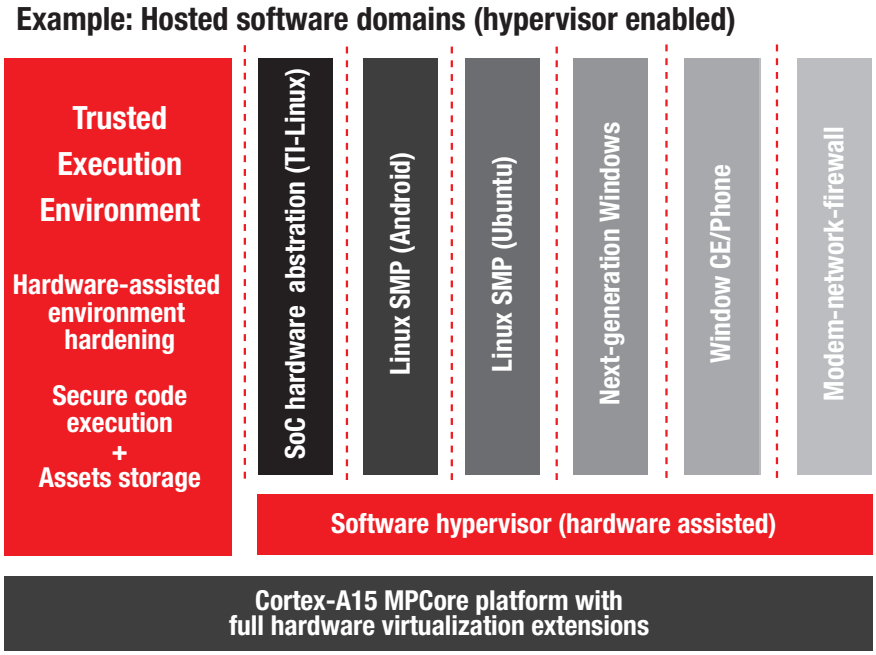
Legacy software/services support – OEMs or operators can leverage a previous legacy investment and continue to offer services based on one environment. They can also offer devices with a new operating system and efficiently support both. This can be made transparent to the user and gives the best of both worlds. Operators can leverage this to have separate branded services that are outside the main or open source operating system environment.

Phone customization – A consumer can select the operating systems that are desired on the phone rather than having to settle for what typically comes with one operating system. This gives consumers a choice. It also allows the user to run applications that are only available for a certain operating system, and it is possible to make this all seamless – for example be in one OS and run another application in another OS from the same menu display.

As mentioned, the Cortex-A15 processor includes hardware virtualization support which provides fast, power-efficient support for these use case scenarios. Without this hardware virtualization, you can support them only with para-virtualization that has several disadvantages including high operational overhead to process the high number of traps and exceptions from guest OS kernels running in user mode. This gets compounded when additional guest OSes are added. It also complicates software development because it requires changes to the guest OS and in critical areas. This can be problematic for OSes that are not open source where you don't have access to the source code to re-host them. The presentation material that goes with this paper shows the operation of a para-virtualization that has these disadvantages compared to hardware virtualization.

The Cortex-A15 provides world-class hardware virtualization that reduces the operational overhead for higher performance, enables guest OSes to run at native CPU privilege, lowers development cost and improves security and isolation. A key benefit is the ability to run native ARM OSes without the need for kernel source code which provides a lot of flexibility for developers and users.

Figure 3 shows an example of a Cortex-A15 platform supporting multiple software domains (OS, hardware abstraction and other services are shown). It is important to note that these run in the non-secure state, separate from the Trusted Execution Environment. A software hypervisor provides the minimal support required due to the hardware virtualization capability that helps in several ways, reducing the entry to the hypervisor by separating the virtual and physical effects more cleanly and giving more precise control over what enters the hypervisor.



▲ ***Figure 3*** *– Cortex-A15 world-class hardware virtualization*

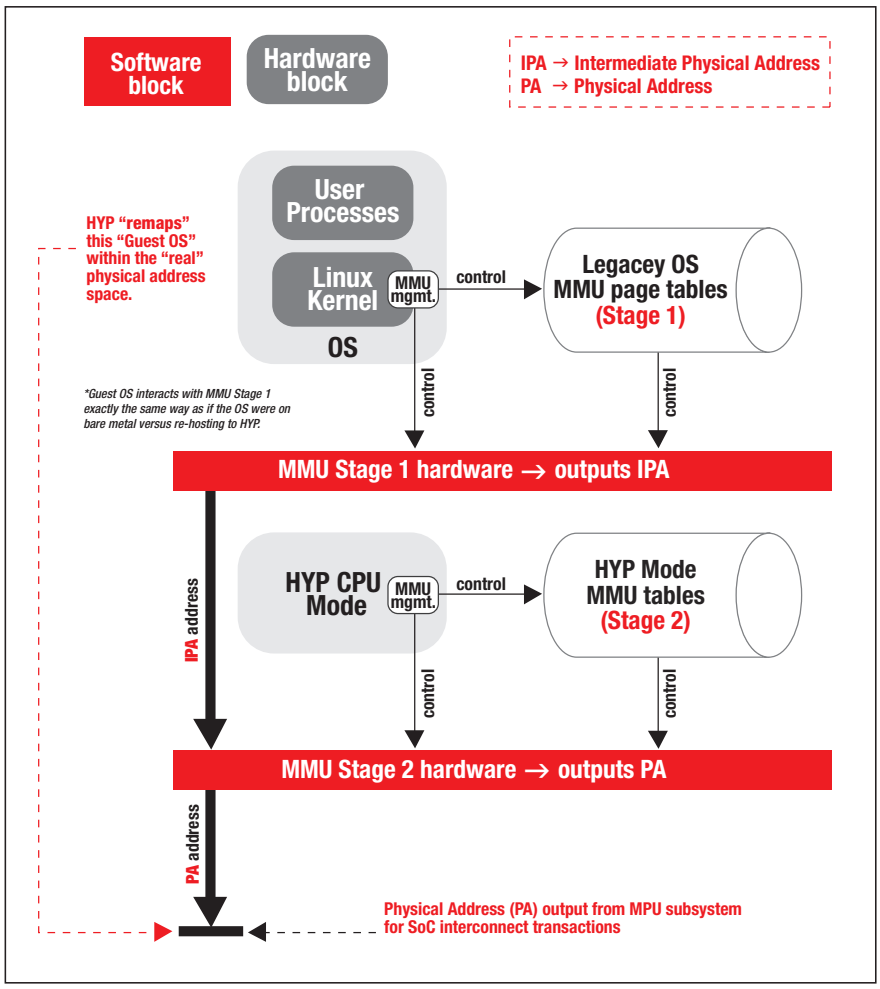
The Cortex-A15 processor does an extraordinary job with separation of virtual and physical. It is standard for microprocessors to separate virtual and physical interrupts. However, ARM has gone way beyond by separating the page table management done by the guest OS from the virtualization page tables handled by the hypervisor, a benefit that is not provided by processors. The Cortex-A15 solution for interrupts means that the guest OS doesn't need to enter the hypervisor when servicing virtual interrupts, even several queued for the guest OS.

It is important to note that with the Cortex-A15, it is possible to run a guest OS without any code changes and with good performance.

The Cortex-A15 hardware virtualization support is vast, so for the purpose of this overview, this article will focus on the key hardware MMU support and interrupt virtualization.

The Cortex-A15 includes a 2-stage MMU, which is only present on the non-secure side. The first stage is 100% compatible with OSes and is "owned' by the guest OS. This stage performs mapping from the virtual address map of each application on each guest OS to an intermediate physical address (IPA) map. The second stage is owned by the hypervisor and performs the mapping from the IPA to the real system physical address map. Each software layer (OS and hypervisor) can manipulate tables independently. This 2-stage MMU approach is fully compatible with guest OSes (they don't even know about the second stage), yet enables support for the hypervisor in an efficient manner.

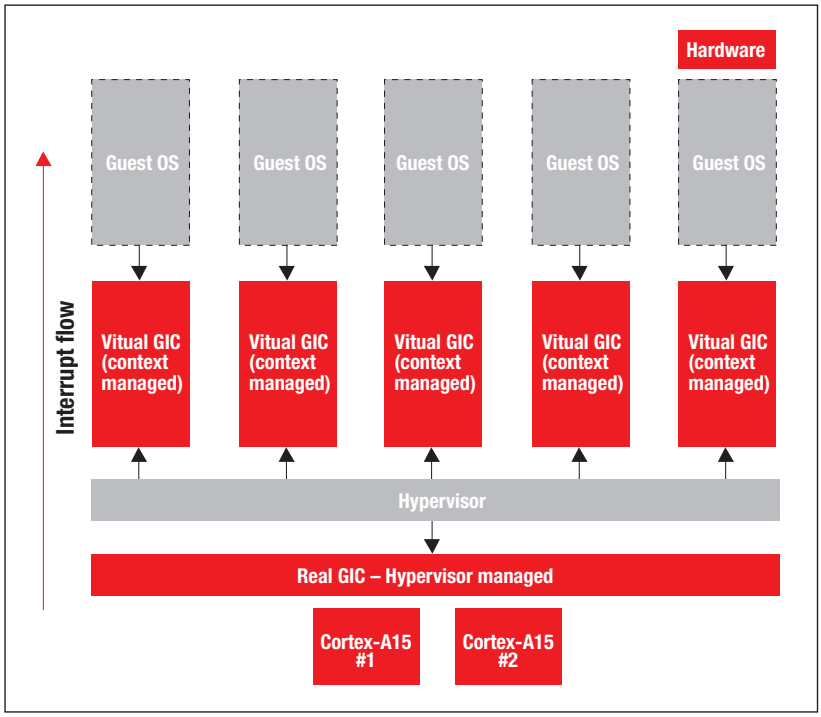
Figure 4 illustrates the implementation of the 2-stage MMU in the Cortex-A15 processor.



▲ ***Fig. 4 –*** *Cortex-A15 2-Stage MMU for hardware virtualization*

Virtual interrupts are also supported, as interrupts need to be routed to the current guest OS, another guest OS that is suspended or directly to the hypervisor. To maintain stability, guests may not directly manipulate interrupts, so virtual interrupts are maintained for each guest. Without this support in hardware, a software implementation would need to do a lot of processing and have associated overhead. In the Cortex-A15, the guest OS sees the virtual GIC (VGIC) as if it was the real GIC.

Figure 5 illustrates how virtual interrupts are supported by the Cortex-A15 for efficient processing as part of its hardware virtualization support.



▲ ***Fig. 5 –*** *Cortex-A15 virtual interrupt support*

Larger physical address extension

Another significant new feature introduced by the Cortex-A15 processor is the Larger Physical Address Extension which extends the address space from 32 bits up to 40 bits. This is very important to support the future needs of mobile devices on their current memory trajectory, as well as enabling support for new applications and usage of the mobile devices.

Today's high-end smartphones support 512MB of DRAM and tablets are extending this to 1GB. Based on TI predictions, and consistent with industry data, tablets will exceed 2GB of DRAM in 2012 and smartphones in 2013. DRAM size increase is being driven by larger OS memory needs and support for richer content and data sets.

There is a need to extend beyond the current total 4GB of addressable space for the system I/O and memory, of which today only 2GB is supportable for the DRAM. This makes the need for Cortex-A15 critical for high-end mobile devices in the 2012-2013 timeframe.

With the Cortex-A15 extension of the physical address space, it provides the ability to support a larger DRAM size which will transform mobile devices in several ways. With larger memory these devices can support:

- increasing OS memory needs,
- multiple OS memory needs (in conjunction with hardware virtualization),
- larger, richer applications and mixture of applications,
- more simultaneous processes, and
- larger data sets and richer content.

In the end, this will improve the capabilities of mobile devices. More memory will enable more advanced software and expand their usage beyond content consumption devices to content creation/editing devices and help drive them as the next generation of computing devices.

The TI OMAP 5 platform supports up to 8GB of DRAM with its Cortex-A15 integration to enable new use cases that were not previously possible with the Cortex-A9 processor.

Transforming mobile devices

The Cortex-A15 offers a lot of performance enhancements and new features that will dramatically transform mobile devices. Mobile devices will become more capable mobile computers with higher performance, larger memory and the ability to support new opportunities. It will do all this and maintain power within the strict budget required of battery-powered mobile devices.

There will be many new use cases that mobile devices can support as part of this transformation. As mentioned, they will become more content creation devices. They will be able to support mainstream computing beyond their current focus as content consumption devices. With efficient hardware virtualization, we will see many new multiple software environments products and use cases including such things as multiple personalities/profiles on phones and the ability to run applications from any vendor on any device. Operators and OEMs will be able to preserve legacy software and services in addition to supporting the latest operating systems, allowing consumers to have a seamless expanded user experience. It is also likely that we will see adaptive mobile device operation based on your location. For example, a device could run Google Android when mobile and automatically switch to Google Chrome or the next generation of Microsoft Windows when docked.

The future looks very bright with the new ARM Cortex-A15 processor coming to a mobile device near you -- powered by TI's OMAP 5 applications processor. For more information about the OMAP 5 platform, visit **www.ti.com/omap5arm15-wp**

References

1. Requirements for Virtualization: Popek and Goldberg - 1974 - www.wikipedia.org/wiki/Popek_and_Goldberg_virtualization_requirements
2. Mobile Virtualization - Coming to a Smartphone Near You – Steve Subar – Open Kernel Labs www.visionmobile.com/blog/2010/06/mobile-virtualization-coming-to-a-smartphone-near-you/

Special thanks to Steven Goss and Steve Krueger from Texas Instruments for providing virtualization insights and supporting graphics.

About the Author

Brian Carlson
OMAP Product Line Manager
Member of Group Technical Staff (MGTS)
Wireless Business Unit
Texas Instruments Incorporated

As a product line manager for the Texas Instruments Incorporated (TI) Wireless Business Unit, Brian Carlson is responsible for defining future OMAP platforms, overseeing related worldwide concept-to-production activities and driving communications strategies. He also represents TI on the MIPI® Alliance Board of Directors and serves as the vice-chairman. Brian is a member of TI's Group Technical Staff, composed of TI's top 20percent of technical achievers company-wide. With over 25 years' experience in technology marketing, business development and engineering, Carlson has a rich background in mobile communications, DSP, and multimedia product development.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Audio	www.ti.com/audio	Communications and Telecom	www.ti.com/communications
Amplifiers	amplifier.ti.com	Computers and Peripherals	www.ti.com/computers
Data Converters	dataconverter.ti.com	Consumer Electronics	www.ti.com/consumer-apps
DLP® Products	www.dlp.com	Energy and Lighting	www.ti.com/energy
DSP	dsp.ti.com	Industrial	www.ti.com/industrial
Clocks and Timers	www.ti.com/clocks	Medical	www.ti.com/medical
Interface	interface.ti.com	Security	www.ti.com/security
Logic	logic.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Power Mgmt	power.ti.com	Transportation and Automotive	www.ti.com/automotive
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com	Wireless	www.ti.com/wireless-apps
RF/IF and ZigBee® Solutions	www.ti.com/lprf		
	TI E2E Community Home Page		e2e.ti.com

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265