WHITE PAPER

Tom Flanagan,
Director Technical Strategy
Ellen Blinka,
Marketing Manager
Texas Instruments

TEXAS INSTRUMENTS

Differentiating AM5K2E02 and AM5K2E04 SoCs from alternate ARM® Cortex®-A15 devices

Introduction

The open and pervasive ARM® ecosystem with its reputation for low power has made ARM cores a popular choice for a wide variety of applications. Texas Instruments (TI), as a leading supplier of ARM-based devices, has a deep experience pool to draw from when designing its devices; experience that allows TI's ARM-based devices to stand out from the crowd. This paper discusses some of the differentiating features of TI's AM5K2E02 and AM5K2E04 processors based on ARM Cortex®-A15 MPCores and TI's KeyStone™ architecture. TI's AM5K2E02/04 processors are dual- or quad-core devices utilizing the ARM Cortex-A15s as the primary programmable processing elements. These devices are well-suited for embedded industrial and computing applications that require a high level of performance, reliability and power efficiency.

The value challenge

When product designers are selecting a processing platform for their application they are ultimately looking for value. Ideally the designer looks to meet all performance and business targets (e.g., time to market, supply reliability, etc.) and looks at the system level rather than simply looking at components. One solution to the system-level value analysis is the development of System on Chips (SoCs). SoCs deliver high value by integrating many formerly discrete functions onto cost-effective silicon and by balancing the integration with appropriate processing performance.

Selecting a device for an application from a range of suppliers when all the suppliers use the same or essentially the same processing cores is a challenge to equipment designers. In the days of monolithic single-core processors, understanding differentiation was more straightforward. Clock rate and price provided reliable and easily understood metrics that gave a first order indication of relative performance. Multicore makes this analysis more challenging and as many multicore implementations have demonstrated, system performance is not simply correlated to the central processing unit (CPU) speed and the number of cores. In today's multicore world, the differentiation lies in the chip architecture and how the architecture either enables or inhibits processing by the cores.

Full processing entitlement

TI devices using the KeyStone architecture deliver full processing entitlement, meaning every processing element is able to operate at nearly its full capacity all of the time. Nothing in the architecture imposes blocking or latency that negatively impacts the ability to achieve full processing entitlement.

Cores and memory

The AM5K2E02 and AM5K2E04 processors feature ARM Cortex-A15 cores operating at frequencies ranging from 1.25GHz to 1.4GHz. TI uses the standard Cortex-A15 cores as provided by ARM. Some manufacturers of ARM-based devices license the core IP from ARM and then change it in an attempt to gain a marginal performance advantage over the standard product. However, these custom cores, though they are derived from ARM's IP, are not necessarily fully compatible with the ecosystem of ARM development tools and software necessitating custom tools and development efforts. So, from the start they are missing one of the key advantages of using ARM cores; the vast ARM ecosystem of software and tools.

TI enhances core performance in the KeyStone architecture by expanding the ability to move data into and out of the cores rather than by changing the cores themselves. This is achieved by augmenting ARM's 128-bit AMBA® bus interface with TI's 256-bit CorePac interface. The CorePac's 256-bit interface connects with KeyStone's Multicore Shared Memory Controller, (MSMC). The CorePac to MSMC interface operates at the core's clock rate while ARM's AMBA interface typically operates at one third of the core clock rate. MSMC's doubling of the bus width and clock rate effectively doubles the throughput of every A15 core in the system.

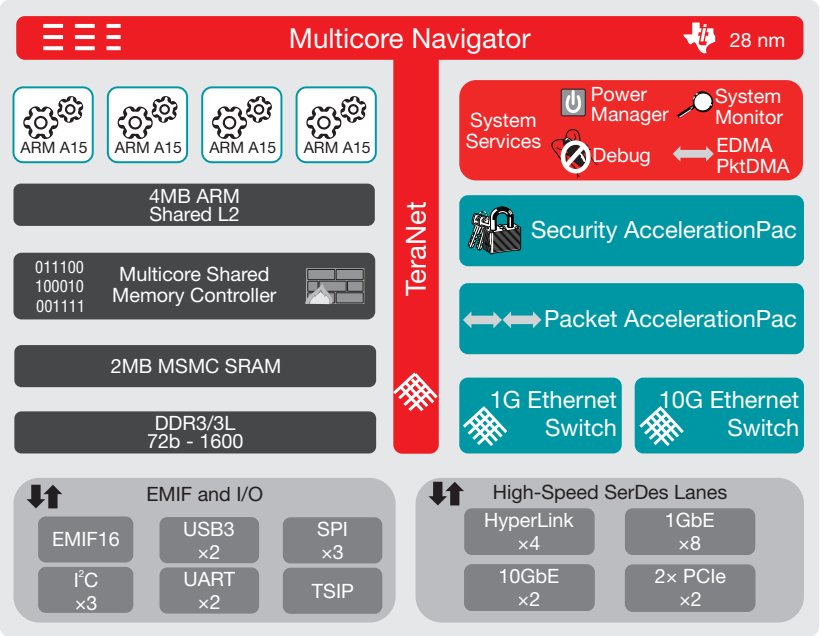
Although the AMBA interface is altered to double the throughput, the multicore cache coherency provided by ARM is maintained. In fact, KeyStone extends coherency to encompass all of the SoC's high-performance I/O. The CorePac provides 4 MB of L2 cache and the MSMC provides an additional 2 MB of shared memory for an on-chip total of 6 MB. Off-chip memory access is supported through MSMC's 64-bit DDR3 interface [72 bits with Error Correcting and Checking (ECC)]. The substantial enhancement to the A15's processing capacity provided by TI's KeyStone CorePac and MSMC are summarized below:

- CorePac's core clock rate and 256-bit interface doubles the on-chip interconnect bandwidth
- Fully coherent memory for the A15 cores
- Fully coherent SoC I/O
- 6MB on-chip memory
- 64-/72-bit DDR3 with ECC, 8GB addressable memory

Input/Output

The function of I/O interfaces is to bring data to the processing elements then physically affect an external element or to transmit modified data. The AM5K2E02/04 processors have a variety of high-performance interfaces to accomplish this including:

- Eight 1Gbps switched Ethernet ports
- Two 10Gbps Ethernet ports (AM5K2E04)
- Two PCIe gen2 controllers with two lanes each
- Four Hyperlink ports



AM5K2E02/04 block diagram

The AM5K2E02/04 processor also has the following low speed interfaces:

- EMIF 16
- Dual USB3 ports
- Three SPI interfaces
- Three I^2C interfaces
- Dual UARTs
- TSIP

As mentioned earlier the I/O ports are cache coherent which greatly simplifies the programmer's memory-management tasks. But there is quite a bit more that differentiates how these interfaces acquire the process and transmit their data that is discussed in the following sections covering TeraNet and the packet and security accelerators.

TeraNet

TeraNet is a hierarchical 2.2Tbps on-chip network that provides interconnection between the processing elements and I/O of the SoC. The hierarchical feature allows full connectivity without the high power consumption of an any-to-any switch fabric. TeraNet operates in parallel to MSMC's path to external memory so that the on-chip data movement is not hindered by simultaneous memory access. TeraNet's power efficiency and high capacity are critical to AM5K2E02/04 processor's ability to deliver full performance entitlement.

Packet accelerator

Accelerators are the processing elements for the KeyStone architecture that are designed to offload the ARM Cortex-A15 cores from repetitive, MIPS-intensive processing tasks. The packet accelerator autonomously performs network switching and packet routing. Once an origin and destination path are known, all subsequent packets with known address pairs are switched or routed by the packet accelerator without any intervention by the A15 cores. Additional functions such as IP reassembly, firewall, address validation and check sum calculation and recalculation are also performed by this high-performance hardware subsystem.

Security accelerator

Closely coupled with the packet accelerator is a security accelerator. This hardware subsystem performs autonomous authentication, decryption and encryption for the following encryption standards in protocols such as IPSec and SRTP:

- 3DES
- AES
- CCM
- GCM
- DES CBC
- Kasumi
- Snow3G
- and more

Together the accelerators offload a tremendous amount of processing freeing the A15 cores for value added application and control processing. The AM5K2E02/04 processors support 1.5 Mpps and 4.2 Gbps. These accelerators are configurable processing elements and like the A15 cores, the KeyStone architecture is sized to support operation of the accelerators at close to their full capacity all of the time; in other words, to deliver full processing entitlement.

Designed for industrial applications

The AM5K2E02/04 processors are targeted at “headless” industrial applications; those with no locally attached user interface screen. Many industrial applications have stringent reliability requirements so the devices incorporate the following features:

- All significant memories are ECC protected
- Industrial class FIT Rate (Failure in Time) and Soft Error Rate
- Standard industrial temperature range: –40 – 100°C (case temperature)
- Lifecycle of 100K power on hours (POH) at Tjxn = 105°C and nominal voltage
- Compact 27mm × 27mm packaging

Industrial applications also commonly have higher security needs than commercial applications due to end equipment being safety- or security-critical. To meet these needs, AM5K2E02/04 devices support security features, such as secure boot, aimed at preventing software IP theft and device takeover.

The secure device versions of AM5K2E02/04 processors include hardware features to support security within the part, enabling critical code to be executed on ARM or DSP within a secure environment, separate from non-secure applications that may be running at the same time. These capabilities include secure boot, secure storage and runtime security which include the following:

- Ability to execute ARM or DSP code in a secure state from secure RAM
- Configurable hardware firewalls to protect L1, L2, shared memory and peripherals
- One-time programmable memory to hold customer-specific keys and data
- JTAG port disabled to prevent outside influences from modifying customer software, data or execution flow

The secure boot model on the AM5K2E02/04 processors does not involve TI knowledge of customer secure boot keys; the customer instead will boot the device with a one-time-use boot image from TI and then program their own keys into the device. This method is more secure as the customer does not have to share the keys with TI.

Conclusion

ARM cores are becoming increasingly popular in embedded applications, especially in industrial markets, due to their open and large ecosystem. As the largest supplier of ARM cores, TI has not only developed expertise around incorporating standard ARM cores into SoCs, we have also incorporated innovative features into our KeyStone II architecture to improve the overall performance of the SoC. These innovations, including increased memory bandwidth, high speed switch fabric, accelerators and security features, truly set KeyStone II ARM SoCs apart from other ARM offerings on the market today.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

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

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license 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 significant portions 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. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

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

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

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

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