TrustZone added to cores

The ARM1176JZ-S and ARM1176JZF-S cores and PrimeXsys Platform are the first products to implement the ARM TrustZone architecture.

This is designed to enable a trusted computing platform for consumer devices such as DTV, smart phones, PDAs and wireless solutions to support the growing demand to conduct e-commerce transactions and securely download content through these devices.

The ARM1176JZ-S and ARM1176JZF-S core-based PrimeXsys Platform includes an AMBA 3.0 AXI system bus for higher memory bandwidth and simplified interconnect design.

The ARM Intelligent Energy Manager technology which reduces processor energy usage by up to 75 percent.

The ARM1176JZ-S core and the ARM1176JZF-S core are based on the ARMv6 instruction set architecture and are targeted at service providers and operators that need to deliver products that support e-commerce and secure download of content through these next-generation of consumer devices.

ARM TrustZone technology enables protection of code and data across the entire memory architecture, for the first time in the embedded, portable and consumer computing market space.

The cores and platform also integrate support for the new ARM Intelligent Energy Manager (IEM) technology which reduces processor energy usage by up to 75 percent providing extended battery life or talk time for mobile users.

The AMBA 3.0 AXI System Bus Interface is included to provide a higher memory bandwidth, simplified interconnect design and to reduced the time to design a system. Both cores integrate ARM Jazelle technology for efficient embedded Java execution.

The ARM1176JZF-S core also includes a floating-point co-processor, which makes it particularly appropriate for embedded 3D graphics applications. Both cores are synthesizable and are expected to achieve 333-550MHz worst-case performance on a range of 0.13-micron processes.

Together, the ARM1176JZ(F)-S cores and the PrimeXsys Platform provide a secure, low-power design including an AMBA 3.0 AXI backbone, control for dynamic frequency and voltage scaling, and a system-level TrustZone hardware and software reference design.

The platform also includes ARM CoreSight technology (see box) to provide a debug and trace solution.

Both the ARM1176JZ-S core and the ARM1176JZF-S core include the ARM-Synopsys RTL to GDSII Reference Methodology within the deliverables.

The reference methodology streamlines the process used by ARM Partners to port synthesizable ARM microprocessor cores to their chosen silicon technologies, by potentially reducing the time required to harden and model the core.

TrustZone technology provides a secure foundation for systems running open Operating Systems (OS), such as Linux, Palm OS, Symbian OS and Windows CE. In addition, TrustZone technology complements secure application environments such as Sun Microsystems' Java technology by making security implementation on devices more efficient.

ARM TrustZone technology is implemented within the microprocessor core itself and extended into the system design, enabling the protection of on-chip memory and peripherals. Since the security elements of the system are designed into the core hardware, security issues surrounding proprietary, non-portable solutions outside the core are removed.

In this way, security is maintained as an intrinsic feature at the heart of every device, with minimal impact to the core area or performance, while enabling developers to build any additional security, for example cryptography, onto the secure hardware foundation.

Debug and trace technology

ARM's CoreSight technology is a comprehensive debug and trace solution for complete system-on-chip (SoC) designs. It provides system-wide visibility through the smallest port, significantly reducing time-to-market for developers.

The ARM CoreSight technology provides the highest standard of debug and trace capabilities and can be leveraged for all cores and complex peripherals.

CoreSight technology builds on the ARM Embedded Trace Macrocell (ETM) real-time trace module, which is capable of instruction and data tracing inside a core and adds a wider range of functionality and systems including the tracing of multiple ARM cores, ARM and DSP cores, complex peripherals and busses.

CoreSight technology, together with the ARM RealView development tools, provides the developer with an integrated solution.

It resolves different software bugs through the simultaneous tracing of multiple cores and AMBA bus activity. In addition to halting and testing all cores at once, CoreSight technology provides debug access to AMBA interconnect memory and peripherals without interrupting the processor, for hard real-time developments.

For silicon manufacturers, the ARM CoreSight technology's higher compression rates provide a solution that extends debug and trace capabilities into new, higher frequency processor technologies.

ARM CoreSight technology for the ARM11 Family for the ARM9 Family, can be licensed now, with delivery 1H 2004.

Pentek to offer eCOS RTOS on PowerPC

Pentek is the first vendor to port eCos (Embedded Configurable Operating System), to the Motorola G4 PowerPC processor. The initial target is Pentek's Model 4205 I/O Processor VME board.

To jump start development, Pentek's ReadyFlow Board Support package features pre-built eCos libraries and the GNU open-source development tools.

eCos is an open source real-time operating system for embedded applications, providing a complete runtime infrastructure necessary to support real-time applications with code footprints in the 10's to 100's of kilobytes.

The highly configurable nature of eCos allows the operating system to be customized to precise application requirements, delivering the best possible runtime performance with absolutely no associated runtime or development tool costs. Because of its efficient architecture, eCos delivers good benchmarks for real-time operations including a task switching time of less than one microsecond on a 600MHz G4 PowerPC.

The standard tool chain for board-independent eCos features GNU binary utilities, GCC C/C++ language compiler, GDB Debugger, eCos Configuration Tool, Cygwin (UNIX environment for Windows) and TFTP (Trivial File Transfer Protocol). A complete TCP/IP stack is also provided for network support.

The eCos Configuration Tool features a graphical interface to ease selection of specific modules, parametric control for many modules, and complete templates supporting specific hardware platforms. The GDB Debugger is supported with the Insight GUI to speed application development tasks. All of the tools plus the eCOS components are free software.