SYNOPSYS®
Predictable Success

Synopsys & Texas Instruments

Synopsys Delivers Software Developer Productivity Gains and Reduced Development Cycles

The Synopsys Virtual Platform is a superb tool for pre-silicon development, which allows software developers to create and test software more rapidly. By working with Synopsys, we are able to improve our software development schedules, resulting in productivity gains and allowing TI to deliver more complete solutions to wireless customers."

Avner Goren
TI Worldwide Director of Marketing, Cellular Systems

Texas Instruments (TI), headquartered in Dallas, is the world leader in wireless technology with operations in more than 25 countries. Among its many products, the company provides innovative DSP and analog technologies to meet real-world signal processing requirements.

TI's Cellular Systems group employed Synopsys Virtual Platforms to develop its OMAP™ processors and OMAP-Vox™ solutions for the rapid development of mobile devices such as 2.5G and 3G wireless handsets. Manufacturers adopting TI OMAP processors and OMAP-Vox solutions can rapidly deploy cutting-edge wireless applications that include streaming audio and video, multimedia messaging, gaming, security, speech recognition, location-based services and mobile commerce. The TI OMAP and OMAP-Vox platforms have been selected by leading manufacturers of 2.5 and 3G wireless devices including Nokia, NEC, Fujitsu, LG Electronics, Motorola, Hewlett-Packard, Samsung, HTC and more.

Challenge: Security Requirements and Limited Samples Complicate Tight Secure ROM Code Development Schedule

TI's M-Shield™ security solution is embedded in OMAP processors and OMAP-Vox solutions to deliver security to a wide range of mobile applications (see Figure 1). This hardware-based security solution incorporates advanced security hardware features that enable digital rights management, firewall and antivirus support, enterprise and financial security like point of sale transactions and secure storage of credit card information. In particular, TI M-Shield security technology includes a secure on-chip ROM, secure execution environment and security hardware accelerators. Refer to www.ti.com/m-shield for further information about TI's M-Shield security technology. The Secure ROM Code is the first code implemented on any OMAP processor or OMAP-Vox solution. Developing and debugging this code is uniquely challenging because the security hardware prevents tra-ditional debug access and limits visibility into the hardware.

Using Synopsys worked out well for everyone on this project, and the excellent results have convinced the TI team that we made the right choice in selecting Synopsys as our development platform."

Erdal Paksoy
Software Development Product Architecture Team Manager for TI's Cellular Systems Solutions

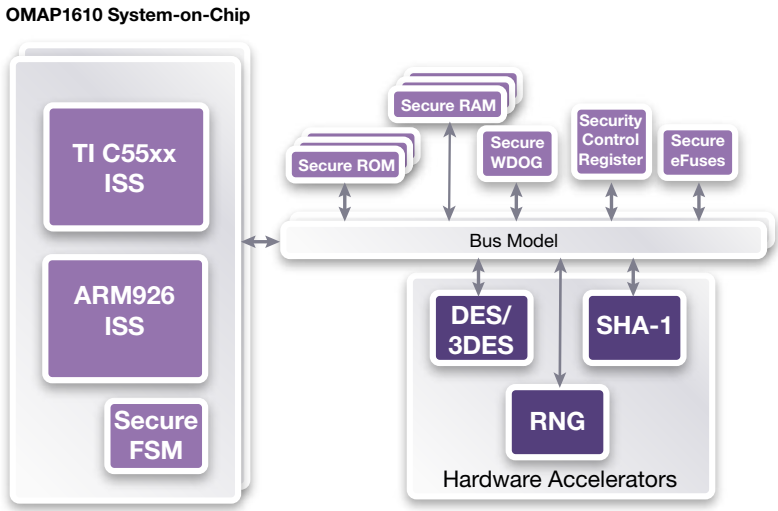

Figure 1: Block diagram of TI OMAP1610 SoC

Solving these challenges was imperative for TI because they could cause TI to miss key development deadlines. In the mobile phone arena, market leadership is only as good as the latest product innovation. As a result, TI required development solutions that would enable software developments to dramatically get ahead of silicon developments collapsing the typical development timeline to keep pace with the demand for more functionality in increasingly shortened product life cycles. The Synopsys Virtual Platform was just the solution TI needed.

Solution: Synopsys Virtual Platform ProvidesHigh-Performance Development Environment

Texas Instruments selected the Synopsys Virtual Platform as the development environment for the Secure ROM Code and initial base port code. The Synopsys Virtual Platform is a high-performance software simulator designed to integrate with the software developer's preferred development tools and provide a complete desktop development environment to maximize productivity. With advances in the Synopsys relationship, Synopsys was able to deliver TI an early silicon evaluation system model based upon TI hardware specifications that could boot an operating system and run application code months ahead of hardware availability, enabling concurrent hardware and software development, and expediting the total solution delivery.

The security firmware team leveraged many capabilities of the Synopsys Virtual Platform that would not be available during silicon development and till the complete validation of the platform silicon. First, the Virtual Platform gave the security team enhanced visibility into hardware, existing only in specification form, allowing much earlier evaluation of the software and hardware specifications before full implementation on the complete hardware-software system (see Figure 2). That provided advantages like setting hardware breakpoints which allowed single-stepping through the OMAP multi-core hardware design with high visibility debuggers like Metrowerks CodeWarrior™ for Symbian® (OEM Edition). Many first time develop-ments occurred with this project such as being able to easily define full system breakpoints that allowed superior visibility into the multi-core software/hardware simulation and running the simulation close to real target speeds on a PC.

I used Synopsys Virtual Platforms and Metrowerks CodeWarrior together to complete my security and baseporting effort. The two tools formed a powerful development platform that very substantially reduced the overall effort by making the hundreds of baseporting issues go quickly. My baseport effort simply could not have been conceived of, occurring in the timeframe it did, without advanced tools such as these."

Steven C. Goss
Texas Instruments, Cellular Systems Security CTO Office

When the breakpoints hit with Synopsys Virtual Platform initiating complete hardware-software system freeze, the system was fully exposed providing full views of component states such as the MMU with intricate memory management states, hardware security states, and crypto accelerator states. For single-stepping of the multi-core system, Synopsys enabled preservation of system state integrity. The tool provided a significant advantage compared to the traditional developments with JTAG and physical hardware, where breakpoints can occur on one core but let other cores continue to run and making real hardware extremely difficult to trouble-shoot multi-core software interactions.

Second, the security team benefited from Synopsys's trace and logging features that were not available in physical hardware. Trace pods are limited in bandwidth, but the Synopsys Virtual Platform is unlimited in its ability to generate real-time ETM traces.

Figure 2: Synopsys VPOM-1610 debugging security peripherals.

Finally, flash and ROM updates are instantaneous on the Synopsys Virtual Platform, compared to the several minutes delay required to physically flash a development board, allowing developers to retain focus increasing development efficiencies to 100% towards task completion.

Synopsys Virtual Platform delivered many key benefits to the TI security team, applicable to their secure software development, including:

Enhanced Visibility of System and Security States

- Detailed visibility into the state of all security hardware peripherals
- Convenient control of security states through backdoor access
- Use of existing third-party IDE and debugger, including Metrowerks CodeWarrior™

Easier Development Environment than Hardware

- Security violation resets can be stopped prior to erasing the violation cause and system state
- Easily updated eFuse and secure ROM content

Customized Security Reporting & Logging

- Easy tracking of security violation causes through platform security reporting
- Added custom security logging to simulation C-models with the Synopsys Platform Development Kit (PDK)
- Simulated security control violations through scripting for testing and validation

Results: Reducing Development Cycle Translates to Millions of Dollars

Leveraging Synopsys, TI's security software development team was able to complete the secure code development and debug two months prior to receiving silicon samples, enabling early software delivery. This achievement was essential to project success because any delay in the Secure ROM Code and other security software would have caused delays in all additional software development tasks, including base ports, BSP, codecs, and application development.

"On our 1st security project, our alpha version ROM Code which was required to be embedded in first silicon prototypes restricted certain security developments," confirmed Steven Goss, Cellular Systems Security CTO Office at TI. "We chose Synopsys because the next scheduled silicon release was due in three months. Synopsys allowed enhancing the Secure ROM Code on time, testing, and continuing developments without waiting the three months for the evaluation platform.

"My job was not HLOS base porting, typically done at TI by a team of baseport professionals. To develop the needed software component on the baseport to enable the M-Shield secure execution environment, I took on the baseport effort, myself, and provided a useable development Symbian baseport in six weeks. That allowed our secure software development to be on schedule. That task, in the timeframe I delivered, was only possible with the help of Synopsys and CodeWarrior OEM high productivity tools," Goss added. "Seeing Symbian securely boot with our first generation silicon based security and drivers on the new device in the short timeframe was very thrilling. After that, Synopsys Virtual Platforms became broadly used by other teams within TI.

"Synopsys helped remove a significant roadblock from our program, where no workable hardware development platform was available in our development timeframe, with the exception of Synopsys' VPOM-1610 emulating our OMAP1610 silicon product. Synopsys exceeded our expectations because:

- Synopsys Virtual Platforms provided more visibility into what the OS & hardware drivers were really doing than what real hardware development platform could have.
- Virtual Platforms allowed debug turn-around times that were a small fraction of what real hardware would take.
- Synopsys allowed software load times that were a small fraction of what real embedded hardware would be.
- Synopsys and Metrowerks allowed excellent debugging visibility at source code level from the first instruction at boot time to the last piece of code that just blew up in my face, regardless of whether stepping assembly code or whether stepping high level C++ code.
- Code changes and fixes were occurring "real time" at more than 15 per day most days of the project. This with just with myself working on the project."

TI estimates that by utilizing the Synopsys Virtual Platform, the team completed the software development project at least three months earlier than would have been possible without Synopsys.

After hearing about the TI Security Team's remarkable success, other software development teams across business divisions at Texas Instruments adopted Synopsys Virtual Platforms to start their development early on software projects such as:

- OS base ports and new OS kernel development
- Driver development for basic peripherals/storage devices/ connectivity devices (USB, 1394)/multimedia devices
- Inter-Processor Communication (IPC) software development
- DSP development, including CODEC development
- Power management drivers and optimizations

Based on the outstanding results of this project, Texas Instruments has standardized on the Synopsys Virtual Platform as the development environment for all mobile phone software. The TI Security Team demonstrated that a Synopsys Virtual Platform enabling pre-silicon software development is an excellent alternative to normally sequential software development activities. TI's use of Synopsys development tools enabled them to meet product schedules and reduce project risk, translating into increased revenue and reduced costs. Consequently, pre-silicon software development using Synopsys Virtual Platforms is now a core competency of TI's software development teams.

See www.synopsys.com/virtualplatform for more information on Synopsys Virtual Platforms and contact Synopsys to see how you can get similar results with Synopsys Virtual Platforms.

Synopsys, Inc. • 700 East Middlefield Road • Mountain View, CA 94043 • www.synopsys.com