February 2015 Volume 1, No. 1

ANDES in Sight

ANDES TECHNOLOGY Newsletter, US Edition

Contents

ANDES Technology USA
5201 Great America Pkwy., Suite 320,
Santa Clara, California, 95054
Business: info@andestech.com

Publisher: Andes Technology Corporation
Chief Editor: Jonah McLeod

ANDES Technology Solutions to IoT Security Vulnerabilities

Embedded processors in intelligent sensors within IoT chips are now popular targets for hackers. They can easily change program code and system parameters to alter the operation of the sensor or use the system for their own purposes. Another vulnerability of these embedded processors is theft of the software IP for the purpose of cloning the function or using it to shorten time needed to develop a competitive offering.

The first point of vulnerability to hackers in an embedded system is the JTAG interface, which is used for debugging software of the system. A hacker able to put the system into debug mode has complete control of the system. He has complete access to the CPU's registers, program memory and any other memory in the system.

To provide protection of embedded software and program data while keeping the debugging capability, Andes Technology's secure debugging feature requires pass code validation. Anyone accessing JTAG port must provide a pass code, which can be provided in a static or dynamic form. A static pass code is stored in non-volatile memory in the chip. Anyone attempting to access the JTAG interface must provide the stored code. The other alternative is storing the pass code on a remote server and anyone accessing the JTAG port must acquire the pass code from the server.

Chip vendors can also burn in their software and turn off JTAG completely before shipping the chips. Debugging capability is convenient for field diagnostics and/or system vendors' continual development. But, without secure debugging support, some chip vendors choose to disable JTAG in favor of protection.

The other point of vulnerability in an embedded system is the memory interface brought out to the pins on the packaged part to access external memory. By probing the interface pins with a logic analyzer, hackers can capture all the traffic passing between external memory and the embedded CPU.

To secure the memory interface, the Andes secure MPU scrambles the data and/or address thus displaying random information to a logic analyzer probe and making it difficult to copy the memory contents without the encryption key. (See "Andes: 32-bit MCUs Way to Go for IoT" for more.)

Combating The Differential Power Analysis Hack

The differential power analysis is a popular technique used against smart phones. Taking smart phone applications as an example, there are a number of keys stored on the phone, keys for the phone company, others for financial transactions. Hackers probe the power profile of the MPU within smart devices looking for repeating patterns. For example, a power trace from a MPU performing a DES encryption can clearly be seen.

One of Andes solution is to randomize the power profile to eliminate the repetitive patterns, thus making the CPU less vulnerable to this type of hacking. One technique used to achieve this result includes a hardware random-bit generator that randomizes the internal clock signal. Another technique is to use a hardware random-bit generator to schedule per instruction cycle between two or more threads of execution that run on the MPU's register sets.

Andes continues to develop hardware solutions to ensure its customers can create embedded systems that are difficult for hackers to defeat.

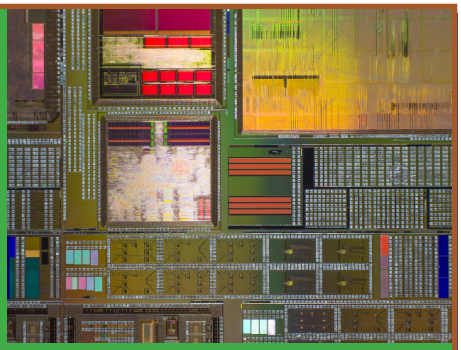
Innovative CPU IP Core Memory Subsystem Boosts Performance, Reduces Power

With Gartner estimating that product and services for the Internet of Things will generate over $300 billion in 2020, the number of designs for new "things" continues to increase. Most are built around microcontrollers but most CPU architecture within these MCUs lack the memory system architecture that reduces power while increasing performance. Andes Technology Corp., a CPU IP company, was founded in Taiwan in 2005 to achieve these goals by developing the AndeStar™ architecture, now in its third version.

The objective was to build a CPU architecture for a wide range of applications. Architecture innovations allow implementation of a series of highly performance-efficient CPU cores with compact code size to address more specific markets, for example, networking, storage, connectivity, human-machine interface, security, etc. While the performance-efficient nature of an entry-level Andes Core fits perfectly for portable applications and IoT devices, high end Andes CPU cores serve Linux-based networking applications with efficient compute power.

One innovation, FlashFetch, is particularly well suited for portable applications and IoT devices, which rely on flash and one-time programmable memory like the eMemory Technology Inc. NeoBit ULP NVM IP for program and data storage. The CPU in a microcontroller directing a control device in an IoT application, spends a good deal of time waiting for interrupts to process—temperature or pressure sensor reaches a threshold, a lock is engaged or unlocked, and so on.

FlashFetch consists of a tiny cache and a prefetch buffer. The loops where the CPU spends most of its time execute from high speed tiny cache and are loaded automatically as they get executed. Between Tiny Cache and the flash and OTP containing code and data is a prefetch buffer which speeds up the fetch of code which isn't present in the tiny cache.



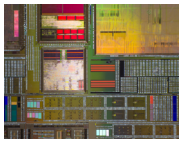
FlashFetch Performance Boost

For an AndesCore CPU, FlashFetch boosted EEMBC CoreMark benchmark performance by 125 percent, while increasing EEMBC Dhrystone DMIPS benchmark 75 percent. For power reduction, FlashFetch achieved a 55 percent improvement on the CoreMark benchmark and a 43 percent power improvement on the Dhrystone DMIPS benchmark.

FlashFetch is an example of system level enhancements incorporated in AndesCore architecture to boost performance while reducing power consumption. In the process, it enables flexibility in the memory subsystem design. Innovative CPU IP core memory subsystem that boosts performance and reduces power is now a reality.

Evaluate Andes IP Cores

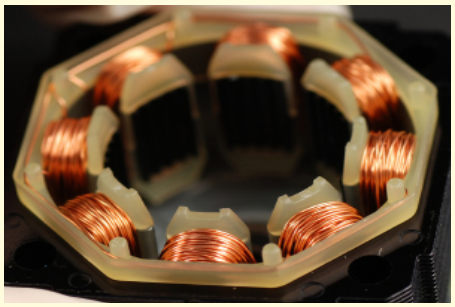
Andes has over 80 licensees and Andes-based products are shipping in more than a half a billion devices around the globe from licensees in Taiwan, Japan, Korea, and China. The company is expanding into the Americas.



If you have an SOC design in need of a low power, low cost MCU/CPU with full toolchain and peripheral support, contact us to arrange a free evaluation. Let us help with your next design. E-mail us at info@andestech.com.

Weltrend Adopts AndesCore™ N801 For Booming Brushless DC Motor Control Market

Weltrend Semiconductor, a leading fabless semiconductor company has adopted the AndesCore N801 CPU IP for a new system on chip (SoC) targeting the expanding brushless DC motor (BLDC) controller market. The N801's small gate count—less than 14k gates—and high performance—1.36 DMIP/MHz at 300MHz operating frequency—beat out competitive alternatives to win the business.



Saving die area with a small gate count while providing high performance provides Weltrend's SoC a competitive advantage as it competes for a large share of the booming electric motor control market. "The worldwide market for electric motors is expected to be worth an estimated US$120.68 billion by 2019, growing at a 6.3 percent compound annual growth rate from 2013 to 2019," predicted the market research report titled "Electric Motors Market (AC motors, DC motors, Hermetic motors) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2013 – 2019," from Transparency Market Research. "Andes has been a valued supplier of CPU IP since 2009," said Chao-Chee Ku, Ph.D., Director of Product Planning & FAE of Weltrend. "Andes has continually provided Weltrend the high quality technical support we need to design best-in-class system-on-chip solutions for our customers. Andes' N801 CPU core helped Weltrend fulfills the market needs as well as our customers' requirements."

Electric motors have a wide area of applications in numerous industries and functions such as motor vehicles, household appliances, industrial machinery, aerospace and other transportation equipment, HVAC equipments, and commercial industry," the report claims. Furthermore, the research asserts that growth is greatest in Weltrend's home market. "Asia-Pacific is the fastest-growing and largest regional market for electric motors owing to improving economies and rising purchasing power in countries such as India, Malaysia, China, and Indonesia."

"AndesCore processor families are based on a young architecture developed in the last 10 years with emerging market requirements in mind," said Frankwell Lin, President of Andes. "Not bound by the need to remain compatible by years of applications, Andes developed a product line of high performance, small size, and low power CPU cores including the N801 with its 3-stage pipeline design. These cores boosts the execution efficiency of today's computation algorithms, reduces memory usage, lowers customers' silicon cost, while providing a long-term roadmap for customers needing an upgrade path from 8-bit cores used up to now."

Andes Technology Corp.

Founded in March 2005, Andes Technology Corporation headquartered in SiSoft Research Center, Hsinchu, Taiwan is a leading Taiwan CPU intellectual property (IP) supplier, with over 80 licensees in Taiwan, Japan, Korea, and China that have shipped over a half billion units. Its products range from the entry level N7 and N8 with 2- and 3-stage pipelines, to the high-end N13 with 8-stage and longer pipelines. The mid-range N9 has the highest customer shipping volume while the mid-range N10 and high-end N13 support Linux and floating-point coprocessor. Configurable and extensible Andes cores enable designers to create unique designs. AndeSight™ IDE enable customers to efficiently develop, debug, tune and regress their software. AndeSoft™ provides customers optimized fundamental software such as OS, drivers, standard C libaries, middleware, etc. for rapid application development. The company has sales offices throughout Asia and the U.S.

2F, No.1, Li-Hsin First Road
Science-Based Industrial Park
Hsin-Chu City, Taiwan 300 R.O.C