



## Clock Generator PLL and DDR DLL Hard Macros

True Circuits, Inc. develops and markets a broad range of award-winning PLLs, DLLs and other mixed-signal hard macros for ICs for the semiconductor, systems and electronics industries. TCI's reputation is built on providing quality standardized and full-custom timing and other mixed-signal IP to the world's most demanding customers. TCI's robust state-of-the-art circuits, methodical and proven design strategy and its cl

TCI's complete family of standardized clock generator, deskew, low-bandwidth and spread-spectrum PLLs and DDR DLLs spans nearly all performance points and features typically requested by ASIC, FPGA and SoC designers. These high-quality, low-jitter, silicon-proven timing hard macros are available for immediate delivery in a range of frequencies, multiplication factors, sizes and functions in TSMC, UMC and Chartered processes from 0.25um to 90nm.

### Clock Generator PLL Features

- Designed as a very flexible clock multiplier capable of multiplying an input clock from 1 to 4096 with very small period jitter while operating at the highest possible bandwidth.
- Delivers optimal jitter performance over all multiplication settings.
- Optionally provides multiple output phases that precisely subdivide the output clock period.
- Includes LockNow! Technology to dramatically improve PLL lock times.
- Available in small sizes for easier integration.
- Ideal for most system clock generation applications.

### Clock Generator PLL Sample Specifications

- Divided reference frequency range 550KHz - 1.1GHz
- /1 output frequency range 220MHz - 1.1GHz
- Reference divider values 1-64
- Feedback divider values 1-4096
- Output divider values 1-8
- /1 output multiples of div. reference 1-4096
- Feedback signal delay (max) n/a (FB internal)
- Output duty cycle (nom, tol) 50%, +/-2%
- Static phase error (max) n/a
- Number of PLL supply pkg. pins (VDDA/VSSA) 2 (preferred usage)

- Process technology TSMC CL013LVOD 0.13um
- Supply voltage (nom, tol) 1.2V, +/-10%
- Junction temperature (nom, min, max) 70C, -40C, 125C

### DDR DLL Product Features

- Designed for high-speed DDR style interface applications.
- Generates precise delays that can be programmed from 0 to 360 degrees of the reference period.
- Delays multiple periodic or aperiodic signals independent of voltage and temperature.
- Delivers optimal jitter performance over a wide frequency range.
- Available in flexible form factors for easier integration.

### DDR DLL Sample Specifications

- Reference input frequency range 66MHz - 330MHz
- Slave delay adjustment range 0% - 100% of reference cycle

- Slave delay adjustment resolution 0.62% of reference cycle
- Number of slave adjustment steps 160 (8 bits)
- Slave delay equation  $ADJ[7:0]/160 * Tref$
- Number of slaves in cluster 2
- Added core supply package pins 1 VDD and 1 VSS
- Process technology TSMC CL013LV 0.13um
- Supply voltage (nom, tol) 1.0V, +/-10%
- Junction temperature (nom, min, max) 70C, -40C, 125C

### Deliverables

- GDSII, LVS Spice netlist, behavioral, synthesis, and LEF models, and extensive user documentation.
- Extensive support to ensure a successful tapeout (included in standard design license fee).

### Availability

- Hard Macros are available for immediate delivery in TSMC, UMC and Chartered processes from 0.25um to 90nm.
- Silicon proven in many ARM cores.

For more information: [www.truecircuits.com/support](http://www.truecircuits.com/support)



## netHSM

### netHSM / Redefining the ROI for cryptographic hardware

- Shareable HSM
- FIPS 140-2 Level-3 validated security
- Multi-layer security architecture
- Secure network communications
- Secure User Interface
- Strong authentication of requesting servers
- High performance cryptographic processing – up to 1600 TPS
- Space efficient 1U Rack mount form factor

The netHSM is a highly secure, network-attached Hardware Security Module (HSM) that provides a shareable cryptographic resource for multiple servers.

Authorized applications that require access to hardware-protected cryptographic keys – from PKI and authentication systems to Web services and SSL – can share access to the netHSM over secured connections. Although dedicated HSMs are appropriate for security applications and servers that demand guaranteed availability and/or processing power, the netHSM provides a cost-effective deployment option for a variety of typical scenarios. The netHSM allows your investment in 'hard security' to be spread across multiple applications or servers.

- Shareable cryptographic resource – provides flexible security for multiple servers and multi-site installations, lowering the overall cost of deploying cryptographic hardware
- FIPS 140-2 Level 3 validated security boundary – proven certified security boundary meeting cryptographic best practice

- Unlimited key storage – utilizes nCipher's Security World key management framework to promote scalability, allowing limitless key storage
- Compatibility with nCipher's dedicated HSMs – seamless integration with the range of nCipher HSMs enables mixed HSM environments to suit individual requirements and protects existing investments
- Strong access and authorization control – authorization for key use can be specified, on a per-key basis, and can be configured to require smart-card credentials to be presented enabling dual control and split responsibility
- High Availability – the inter operability of nCipher HSMs allows failover and load balancing between multiple netHSMs or mixed configurations of dedicated and network connected units
- High Performance – performance for 1024 bit keys extends to 1600 TPS in 1U form-factor, minimizing expensive rack space requirements
- Enhanced application level security – the secure execution of custom application software inside the netHSM's internal hardware FIPS security boundary, creates a trusted hardware perimeter for critical security processes



For more information: [www.ncipher.com/nethsm/index.html](http://www.ncipher.com/nethsm/index.html)





### EMBASSY Trusted Computing Software

Wave Systems has developed a range of advanced security products and technologies under the EMBASSY (EMBedded Application Security SYstem) Trusted Computing brand. Trusted hardware designs, such as the new ARM TrustZone architecture, including the ARM defined software support for TrustZone, are key elements for the security models supported by the EMBASSY technologies. Wave's EMBASSY products support the open standards for new hardware security solutions from the Trusted Computing Group (TCG). The TCG is working on specifications covering a wide range of platforms including PCs, peripherals, cell phones, PDAs, and other devices.

Wave's EMBASSY family of trusted computing products, technologies, and experience include the following elements

- Secure Applications and Services
- Application Development Tools
- Trust Infrastructure Servers
  - Device Management and Authentication
  - Secure Application Life Cycle Management
  - Key Management Services

Wave Systems is focused on development, licensing, and reseller relationships in the emerging trusted computing ecosystem based on the ARM TrustZone architecture.

For more information:

<http://prodcust.wavesys.com/CSC/Home/FAQ.html>



### ARM ATC

Through ARM ATC, ARM recruits and works with a network of approved Partners who are trained, qualified, and equipped with ARM materials and software tools. This enables ATC Partners to provide high-quality, certified training to their own markets and regions.

"Local designers require education that will enable them to survive in the highly competitive world of embedded systems," said Johnson Lee, general manager. "Partnering with ARM makes it possible for us to offer high-quality certified training. This ensures that our customers are able to get their designs completed as efficiently as possible and reduce the time to market for their products."

Beijing Winsilicon provides a host of products and services for developers working with ARM core-based systems. Serving China's growing high-tech sector, the company offers customers high-quality certified, as well as RISC Embedded Solution.

The Embedded solution offer integrated application-ready hardware platform with OS solution base on RISC architecture. With our great expertise in ARM-based technology, Winsilicon design RISC platform provided the most optimized solution to meet the customer's application requirements. These include automotive, consumer entertainment, networking, wireless, and communication.

#### WS-330

\*\*SYSTEM  
CPU:S3C2410 200MHz  
64MB NAND Flash  
64MB SDRAM  
\*\*Interface  
UART?ADC?USBHost?USB Slave?SD?IIC?RTC?IIS?LAN?IDE?IIS

#### WS-430

\*\*SYSTEM  
CPU:AT91RM9200 200MHz  
4M Byte Flash  
32M Byte SDRAM  
\*\*Interface  
UART?LAN?USB Host?USB Slave? Audio?I2C?RTC

#### WS-810

\*\*SYSTEM  
CPU: Intel Xscale PXA255 400MHz  
SMI: 100MHz  
RAM: 8M-64M(optional)(32M optimized)  
ROM: 8M-64M(optional)(32M optimized)  
\*\*Interface  
PCMCIA/CF  
UART(COM): 6 RS232 port  
USB:2 USB1.1  
Audio: AC'97

I2C/I2S  
JTAG  
GPIO:16  
LAN: 10/100M  
MMC control line  
PWM  
RTC  
PSAM  
LPT  
PS/2  
IrDA  
\*\*Display  
LCD 6.4" LVDS TFT color LCD, 800\*600  
Touch screen 6-10.4" TFT\_LCD  
\*\*Packing List  
Support CD with user manual  
Linux support CD  
JTAG cable

For more information: [www.winsilicon.com](http://www.winsilicon.com)



### EyeQ Vision System on Chip

Mobileye is the world leader in development of vision-based applications for driver assistance. The wide range of applications covered by the company and the proprietary automotive grade EyeQ™ ASIC provide a low cost and high performance solution for implementation of driver assistance systems. A full vision system for driver assistance applications consists of the EyeQ™ processing unit and a single (monocular) camera sensor.

Mobileye offers a complete range of vision applications for driver assistance and for safety related applications including:

- Adaptive Cruise Control (ACC)
- Lane Departure Warning (LDW)
- Pedestrian protection
- Lane keeping / Heading control
- Fusion with Radar/Lidar Applications
- Pre-crash active safety
- Forward collision warning (FCW) and Headway monitoring
- Lane Change Assist and Blind Spot detection
- Smart airbag deployment – passenger classification and out-of-position

Mobileye's core technologies include detection of all types of licensed vehicles (cars, trucks, motorcycles, etc) as well as

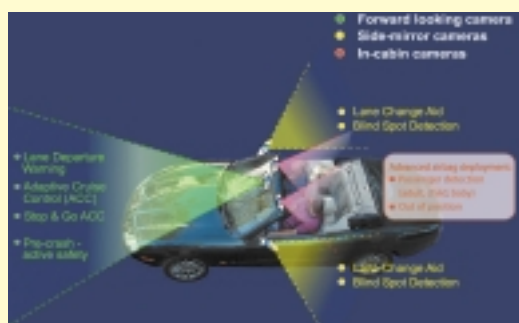
pedestrian detection, detection of lane markings and road geometry estimation. Range and range rate to targets is measured using a single camera rather than a stereo camera pair allowing for simple installation and calibration. Sensor fusion capabilities support Radar and Lidar range sensors.

Mobileye's EyeQ system-on-a-chip solution includes proprietary high data bandwidth design and technological-specific silicon cores for achieving real-time video rate computing.

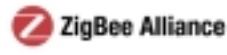
#### Benefits of system architecture:

- System-on-chip technology – Translates to low costs in production
- Single camera architecture – Low cost and easy to produce
- Automatic calibration in production line and during use
- Highly integrated functionality (ACC + LDW +FCW) using a single sensor and chip.
- Ability to work with a wide range of image sensors (CCD, CMOS, NIR, FLIR).

For more information: [www.Mobileye.com](http://www.Mobileye.com)



Endorsed by:



In association with



9-10 November 2004

Santa Clara Convention Center,  
Santa Clara, USA

# wireless

CONNECTIVITY *AMERICAS*



IMPROVING MOBILITY WITH WIRELESS CONNECTIVITY

America's Largest Showcase of Wireless Connectivity Solutions

This high level conference & exhibition will cover ALL wireless connectivity technologies including:

Bluetooth, UWB, WiFi, WiMax, Wireless USB, ZigBee, RFID, IrDA and NFC.

Visit Wireless Connectivity Americas and we guarantee in just 2 days you will be fully equipped with the knowledge you need to implement a wireless strategy for cheaper, more efficient and effective mobility!

Meet ALL the key players in the wireless connectivity market place under 1 roof. For further details and to view the full show agenda please visit

Organized by:



[www.wiconamericas.com](http://www.wiconamericas.com)

Part of:





### Passport SDK

With Passport SDK, developers can empower mobile subscribers with the security needed to conduct personal and commercial transactions from their wireless device applications.

Designed to be downloaded and executed on Java MIDP and C supported wireless devices, the applications that are built using the Passport SDK are client-server applications. Developers can use the SDK to provide security functionality to mobile subscribers (client side) and server applications (server side).

On the client side, developers can use the Passport SDK to provide security functionality to mobile subscribers who communicate with application servers. To build a Java MIDP or C/C++ client-side application, developers can use the lightweight cryptographic API functions contained within the Passport SDK.

Using the Diversinet RSA Library, the API functions of Passport SDK offer Java developers the lightweight cryptographic algorithms they need to design their client-server applications with capabilities for key-pair generation (password protected), digital signature, and public-key encryption.

#### SDK Features:

- X.509 certificate format Version 3
- PKCS certificate management protocols, such as PKCS#7 and #10
- PKCS crypto standards, such as PKCS #1 and #5
- Digital Signatures, such as RSA and DSA
- Key transport/Key agreement, such as RSA and Diffie-Hellman
- Asymmetric Encryption algorithms, such as RSA

- Symmetric Encryption algorithms, such as DES, 3DES, RC2@ block cipher, RC4@ block cipher, RC5™ block cipher, and AES
- Hash Functions, such as MD2, MD5, SHA-1 and HMAC
- Random Number Generator

For more information:

[www.diversinet.com/extra/support.asp](http://www.diversinet.com/extra/support.asp)



### Jbed

Esmertec provides high-performance software solutions for embedded devices such as mobile phones, PDAs, set-top boxes, iTVs, residential gateways and machine-to-machine platforms. Our J2ME™ compliant runtime software solutions are specifically designed to extract maximum computing performance and services delivery capabilities from hardware environments with very limited computing, memory and energy resources. With Esmertec's embedded Java solutions, handset manufacturers, operators and application developers can deliver highly adaptable and customizable mobile multimedia services at mass-market price points to consumers worldwide

Esmertec Java solutions include best-in-class J2ME runtime platforms Jbed™ Advanced, Jbed CLDC and Jbed CDC. Esmertec also provides a comprehensive portfolio of engineering and support services to customers and partners.

#### Jbed Advanced

Jbed Advanced is the new product line of Esmertec.

A high-performance, modular Java execution platform, Jbed Advanced has been specifically designed to support different execution engines within a unified platform architecture.

Esmertec FastBCC™ (ByteCode Compiler using load-time algorithm) or FastDAC (Dynamic Adaptive Compiler) compilation engines can be easily deployed at platform build time, while leveraging a single set of libraries and porting modules.

Jbed Advanced provides Java multitasking capabilities to CLDC 1.1 (Connected Limited Device Configuration) / MIDP 2.0 (Mobile Information Device Profile) compliant solutions for resource constrained mobile devices. It allows concurrent execution of multiple Java applications.

Available with Jbed Advanced is Jcap™ Brand Manager. Jcap Brand Manager provides build time customization as well as Over the Air (OTA) personalization capabilities of MIDP 2.0 look & feel without requiring any modification to the Java application software. An open API (Application Programming Interface) feature will enable the harmonization of the Java- and the native user interface. Jcap Brand Manager also allows end user personalization with pre-installed or Over-The-Air (OTA) themes and wallpapers.

#### Jbed CLDC

Jbed CLDC, a full-featured JVM platform, has been successful

implemented by market leading chipset, operating systems and reference design platforms. Jbed CLDC supports CLDC 1.1 (Connected Limited Device Configuration) / MIDP 2.0 (Mobile Information Device Profile). The Jbed CLDC platform features the latest standard J2ME service profiles such as JTWI, as well as operator specific extensions.

#### Jbed CDC

Jbed CDC is a world-class JVM platform for Personal Java and Connected Device Configuration (CDC). Jbed CDC supports the CDC profiles and interactive multimedia middleware standards such as MHP. Jbed CDC is available with Esmertec's FastDAC technology. Jbed CDC technology has been shipping on multiple models of PocketPC devices including Compaq iPAQ, NEC PocketGear, Toshiba eGenio, Samsung Nexio and Dell Axim under the Jeode brand name.

For more information: [www.esmertec.com](http://www.esmertec.com)



### GNU Toolchain for ARM

CodeSourcery provides releases of the GNU Toolchain (GCC, G++, and related tools) targeting ARM cores. CodeSourcery works closely with ARM to ensure that its releases provide support for the latest ARM cores.

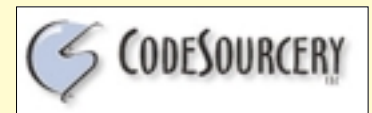
Binary releases of the GNU Toolchain for use on Windows, Solaris, and GNU/Linux host systems are available at no charge from CodeSourcery's web site at:

[http://www.codesourcery.com/gnu\\_toolchains/arm.html](http://www.codesourcery.com/gnu_toolchains/arm.html)

CodeSourcery provides support (including rapid-turnaround defect correction) for these releases. CodeSourcery's support is priced on a per-seat, subscription basis with a minimum group size of five developers.

For more information visit:

[http://www.codesourcery.com/gnu\\_toolchains/arm.html](http://www.codesourcery.com/gnu_toolchains/arm.html) or send email to: [info@codesourcery.com](mailto:info@codesourcery.com)



### GenuineAct

GenuineAct is an encryption/decryption/certification technology that runs on any device beginning with ARM7 16MHz.

#### Technical Features:

- Minimum processor: ARM7 16MHz
- Based on SHA and RSA (2048 bits)
- Code Size: 8 KB
- RAM Usage: 1 KB

- Specific enhancement for content protection on memory cards

#### Typical applications are:

- Protection of multimedia contents for mobile phone
- Protection of contents on memory cards, against illegal copy or alteration
- Protection of contents for consumer electronics devices

For More Information:

[www.actimagine.com](http://www.actimagine.com)

