ARM CPU Solutions for IoT

Phillip Burr
Product Marketing Manager CPU Group, ARM

ARM Tech Forum 2016 – Singapore
August 30th 2016

©ARM 2016
ARM architecture across IoT: from sensor to server
Enabling the widest range of possibilities

<table>
<thead>
<tr>
<th>Cortex-A</th>
<th>Cortex-R</th>
<th>Cortex-M</th>
<th>SecurCore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest performance</td>
<td>Fast response</td>
<td>Smallest/lowest power</td>
<td>Tamper-resistant</td>
</tr>
<tr>
<td>Optimized for rich</td>
<td>Optimized for</td>
<td>Optimized for</td>
<td>Optimized for</td>
</tr>
<tr>
<td>operating systems</td>
<td>high performance,</td>
<td>discrete processing and</td>
<td>physical security</td>
</tr>
<tr>
<td></td>
<td>hard real-time</td>
<td>microcontrollers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>applications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Continuum to serve wider range of applications
Cortex-A32: Ultra-efficient Cortex-A for embedded devices

- Bring rich experiences to embedded devices
  - ARM’s first Cortex-A CPU designed for embedded and IoT
  - Industrial, healthcare, home automation, SBCs, wearables

- Leverage any rich OS and related firmware
  - Full backward compatibility
  - >100 new ARMv8-A instructions

- Smallest, lowest-power ARMv8-A CPU
  - >25% power efficiency vs. Cortex-A7
  - ASIL-B to address safety requirements
Cortex-A is everywhere in the embedded market

ARM market share in rich embedded

Example market segments and products

- Industrial and Retail
- Smart Home
- Wearables

>70%

Source VDC (CPU & SoC unit volume in embedded, excluding mobile, tablets, and networking)
Cortex-A: #1 Embedded ecosystem

Rich OSes
- Linux
- Ubuntu
- Red Hat
- Android
- Windows IoT
- Google Brillo OS

RTOSes
- QNX
- FreeRTOS
- Wind River
- Mentor Embedded
- Micrium
- SCIOPTA

Tools
- Arm DS
- SEGGER
- Mentor Embedded
- Z-System
- IAR Systems
- Green Hills Software
- Linaro

Silicon Vendors
- NXP
- Toshiba
- Infineon
- Allwinner Technology
- Texas Instruments
- Broadcom
- Xilinx
- Renesas
- Samsung
Cortex-M: Trusted choice for embedded intelligence

- 20.6Bn Total units shipped*
- 6.4Bn Units shipped in 2015
- 3600+ Catalog parts*
- 391 Licenses*

2015: 32-bit MCU shipments surpass 4/8bit**
2016: 32-bit MCU with strongest forecast unit growth***

* Data up to end Q2, 2016
** The McClean report
*** IC Insights
Cortex-M Processors

- Highest Energy Efficiency
- Lowest Area
- 90 µm
- 15 years
- Energy-Performance Balance
- Blended MCU and Digital Signal Processing
- Highest Performance
- Scalable and Compatible Architecture
- Cortex-M0
- Cortex-M0+
- Cortex-M3
- Cortex-M4
- Cortex-M7

© ARM 2016
DesignStart: Easier access to ARM IP

Design
Prototype
Produce

ARM

Design with an ARM® Cortex®-M0...for free

Low cost FPGA prototyping

$40K fast track license

designstart.arm.com
DesignStart: Enabling Innovation in Custom SoCs

Driving a new wave of custom SoC development

- Sensor and mixed signal companies: integrated IoT solutions
- Start-ups: innovative solutions
- OEMs: reduce cost, reduce power, differentiate

- Retail
- Building Automation
- Smart Lighting
- Medical
- Industrial
- Home
- Agriculture

Medical

Retail

Building Automation

Smart Lighting

Industial

Home

Agriculture
ARM DesignStart: Fast path to silicon

- Free design & simulation of Cortex-M0
- $40k fast track, simplified commercials

- Free evaluation
- Simplified and quick access to EDA tooling

- Recommended by ARM
- Design partners you can trust

IP + EDA Tooling + Know How
IoT needs security
Security from silicon to cloud

Lifecycle Security

Communication Security
Encryption, Authentication, OTA updates

Device Security
Secure Identity, Software Identity, Isolation, Tamper Detection
TrustZone fundamentals

Separation
- Isolate trusted resources from non-trusted
- Isolate non-trusted software
- Reduce attack surface of key components

Trusted Software
- Provision of security services
- Small, well reviewed code

Trusted Hardware
- Hardware assist for cryptography
- Secure access validation built into SoC
TrustZone – The security foundation for billions of devices

Today

Authentication  Mobile Payment  Content Protection  Enterprise Security

Trusted across many applications

TrustZone for ARMv8-A*
TrustZone CryptoCell

* Fully compatible with TrustZone for ARMv7-A and ARMv6
Bringing security to the smallest devices

Tomorrow

**ARMv8-M architecture**
The ARM architecture for ARM Cortex-M processors

Provides a security foundation with TrustZone

New AMBA 5 AHB5 specification
Extends the security foundation through the ultra-low power SoC
TrustZone: IoT security foundation

Isolates trusted software, data and hardware

- Example use cases:
  - Protection of critical assets
  - Safe crypto implementations
  - Secure remote firmware update
  - Firmware IP protection
  - Secure debug

Enables device integrity and system recovery

Non Trusted
- software
- data
- hardware

Trusted
- software
- data
- hardware

debug

Isolates trusted software, data and hardware
ARMv8-M: Security in small, real-time embedded

Optimised for small real-time processors

Hardware based security state switch

Fully programmable in C

Transparent to the software developer

Low, deterministic interrupt latency

Efficient – every cycle counts

No hypervisor code and processing overhead

Easy to program easy to debug

Transition via a standard function call

Transparent to the software developer

Efficient – every cycle counts

No hypervisor code and processing overhead

Easy to program easy to debug

Transition via a standard function call
ARMv8-M: Tool support from ARM

**ARM KEIL**
Microcontroller Tools

- Includes Compiler, Debugger, IDE
- Secure and non-secure program development side by side

**CMSIS COMPLIANT**
ARM® Cortex® Microcontroller Software Interface Standard

- MCU Software foundation
- Offers standard software APIs easing portability
- Now includes security RTOS API definition

**ARM Models**
Virtual Prototyping

- Productive software development for ARMv8-M
- Integrated with Keil MDK
- Toolkit for creating custom virtual platforms
Ever-expanding world’s #1 embedded ecosystem

TrustZone development support

- ARMv8-M compilers
- Debuggers
- Operating systems
- Development environments
- Security implementations

ARMv8-M early ecosystem partners
Summary

From sensor to server - ARM is the architecture for the IoT

DesignStart makes it even easier to get started with custom SoCs

ARMv8-M Architecture, AMBA 5 AHB5 and CryptoCell, bring TrustZone technology to the smallest of embedded and IoT devices