MPU Product Line Presentation

MPU Team

June 2016

Atmel

Introduction

- **Microchip and Atmel were Competitors**
  - ➡ **Now We Build a Single Team**
- The Atmel MPU32 portfolio has been acquired by Microchip
  - Atmel MPUs have a lot in common with MCUs
    - Similar structure
    - peripherals are compatible
    - Ease of use…

➡ **Let's take a look at similarities and differences within the MPU portfolio**

If you have questions, don't hesitate to ask in real-time!

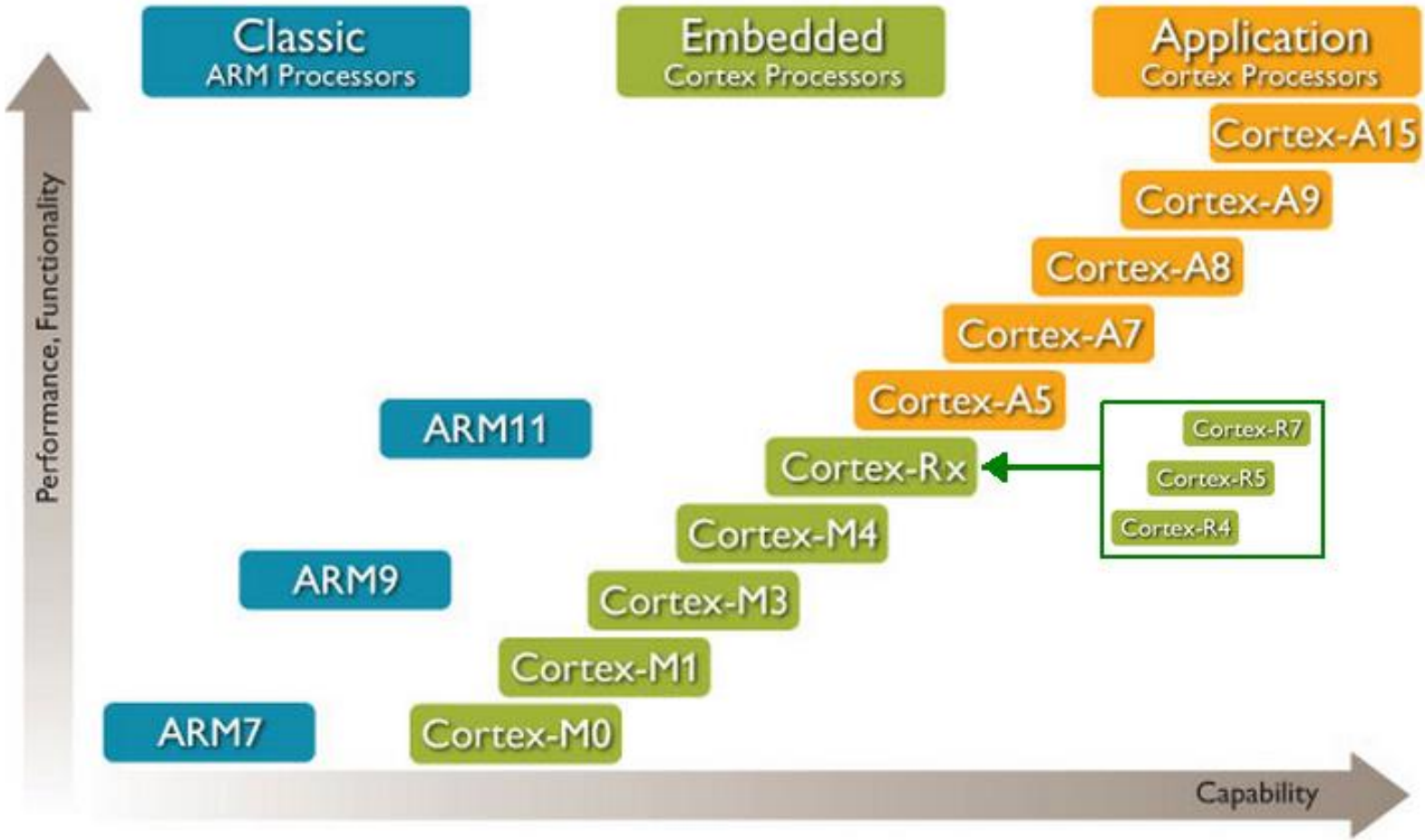
Part 1

Part 1	• **ARM926 Core** • **SAM9 Products** • **Common Blocks** • **Peripherals** • **External Memories**
Part 2	• Cortex-A5 Core • SAMA5 Products • High-speed Peripheral Features • External Memories
Part 3	• Boot Process • Performances and Power Consumption • Security Features

ARM926 Core

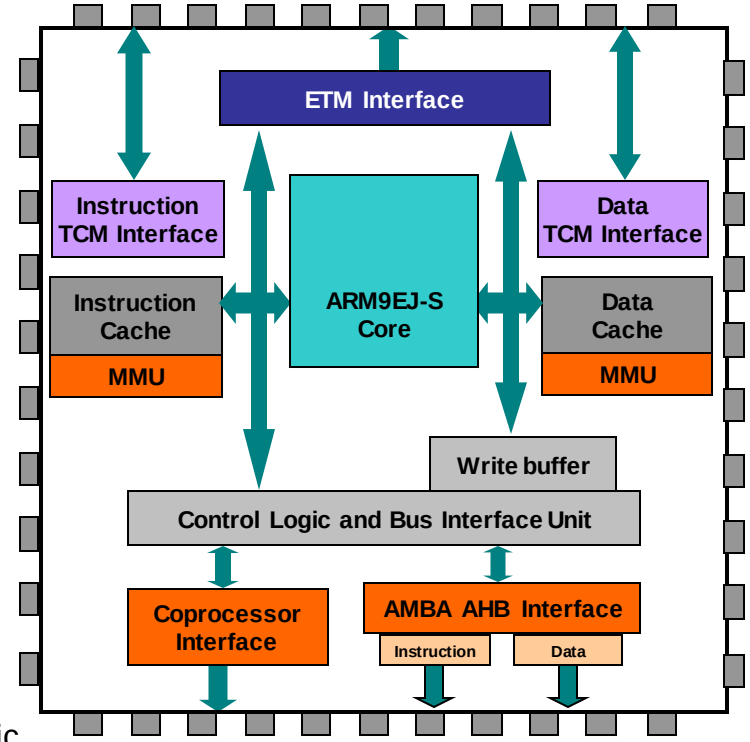
ARM cores

- ARM family



ARM926EJ-S

- **ARM926EJ-S™ ARM® Thumb® Processor**
  - 16-Kbyte Data Cache
  - 16-Kbyte Instruction Cache
  - **1.1 MIPS/MHz**
  - V5TEJ Instruction Set
  - Java Enhancement
    - Java byte code acceleration achieved by hardware
  - DSP Enhancement
    - Multiply instructions using a single-cycle 32*16 implementation
    - Multiply or Multiply Accumulate (MAC) instructions
    - Pipeline allows one multiply to start each cycle
  - Memory Management Unit (MMU)
  - TCM Interfaces
    - Separate interface for instruction and data
    - Single access for data and instruction
    - Used to store critical code and data which deterministic access times are required
  - 5-stage Pipeline
  - 6 Modes: User, Supervisor, IRQ, FIQ, Abort, Undef



Cache

- Main Memory is Slower than CPU (ex: SDRAM)
- Cache Memory is the Solution
- Automatically Keeps Copies of Most Frequently Used Memory Locations in Fast Memory (but expensive)

	Instruction Cache	Data Cache
AT91SAM9263	16 Kbytes	16 Kbytes
AT91SAM9261	16 Kbytes	16 Kbytes
AT91SAM9260	8 Kbytes	8 Kbytes
AT91SAM9G20	32 Kbytes	32 Kbytes
AT91SAM9XE	16 Kbytes	8 Kbytes
AT91SAM9RL	4 Kbytes	4 Kbytes
AT91SAM9G45	32 Kbytes	32 Kbytes

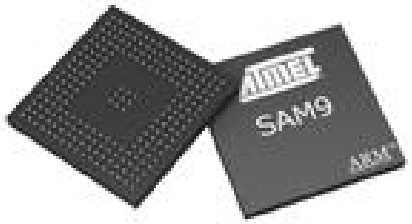
Memory Management Unit (MMU)

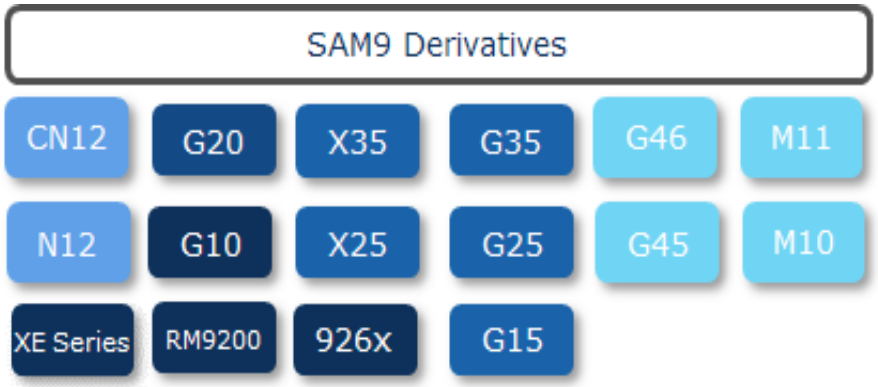
- **The ARM9 MMU**
  - Is a class of hardware components responsible for handling memory accesses requested by the CPU
  - Provides virtual memory management and protection features required by OS such as Symbian OS, WindowsCE, VxWorks, and Linux
- At reset the MMU is turned off, no address mapping occurs, and all regions are marked as non-cachable and non-bufferable
- Programming is performed using an ARM coprocessor register (CP15)
- Must be enabled to use Data Cache

SAM9 Products

SAM9 Series

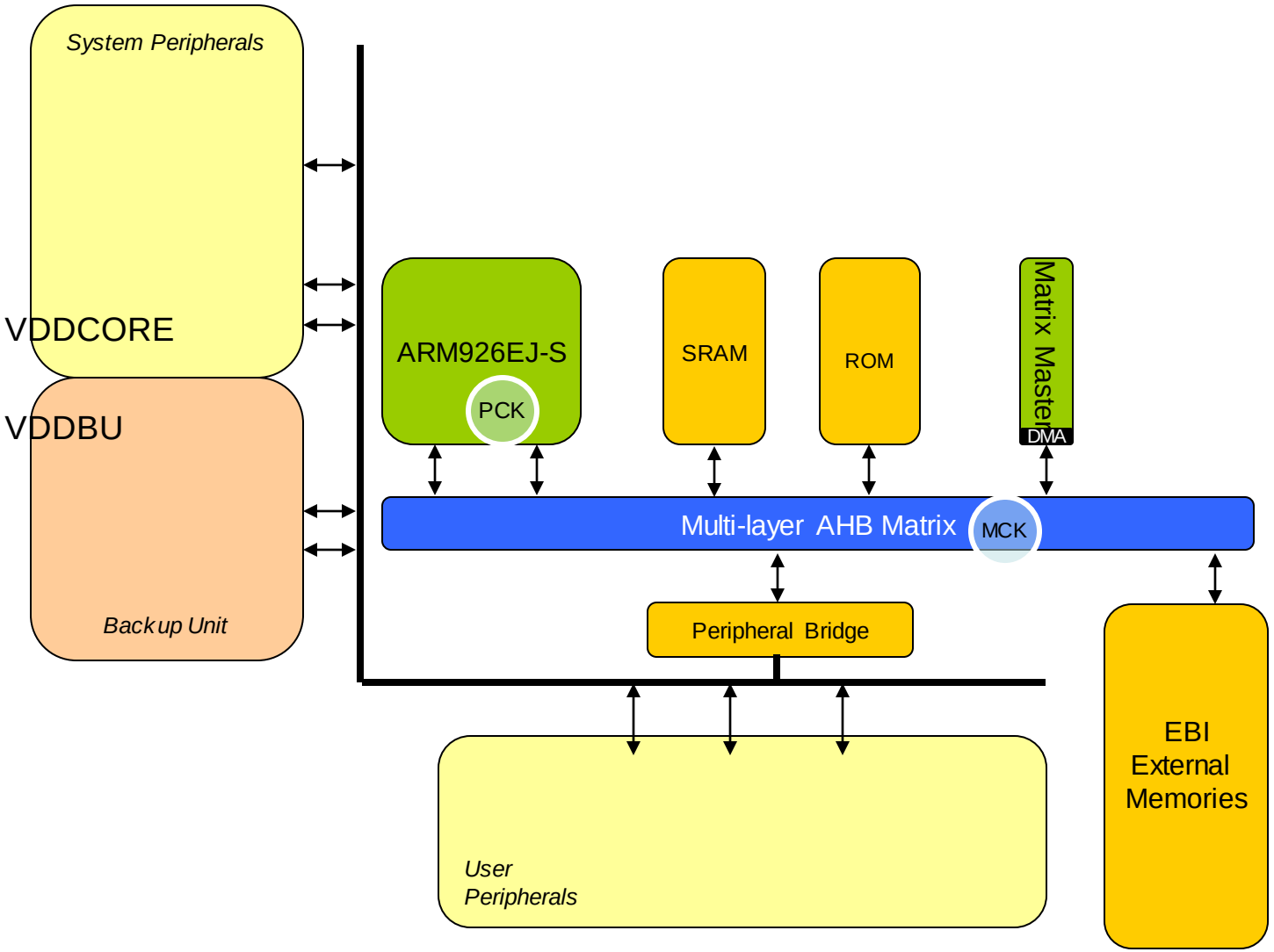
- **ARM926EJ-S Core**
  - Up to 400 MHz
- **Memory Type Support**
  - SDRAM, (LP)DDR/2
  - Raw MLC NAND - 24-bit ECC
  - SDCard / Managed NAND support
- **Industrial Solution**
  - Dual CAN
  - Dual EMAC (SAM9_5Series)
  - x3 USB Ports
- **User Interface**
  - 24-bits LCD Interface
  - Graphics Acceleration
  - Camera Interface
- **Small Footprint and Die Business**
  - 15x15 or 10x10 packages





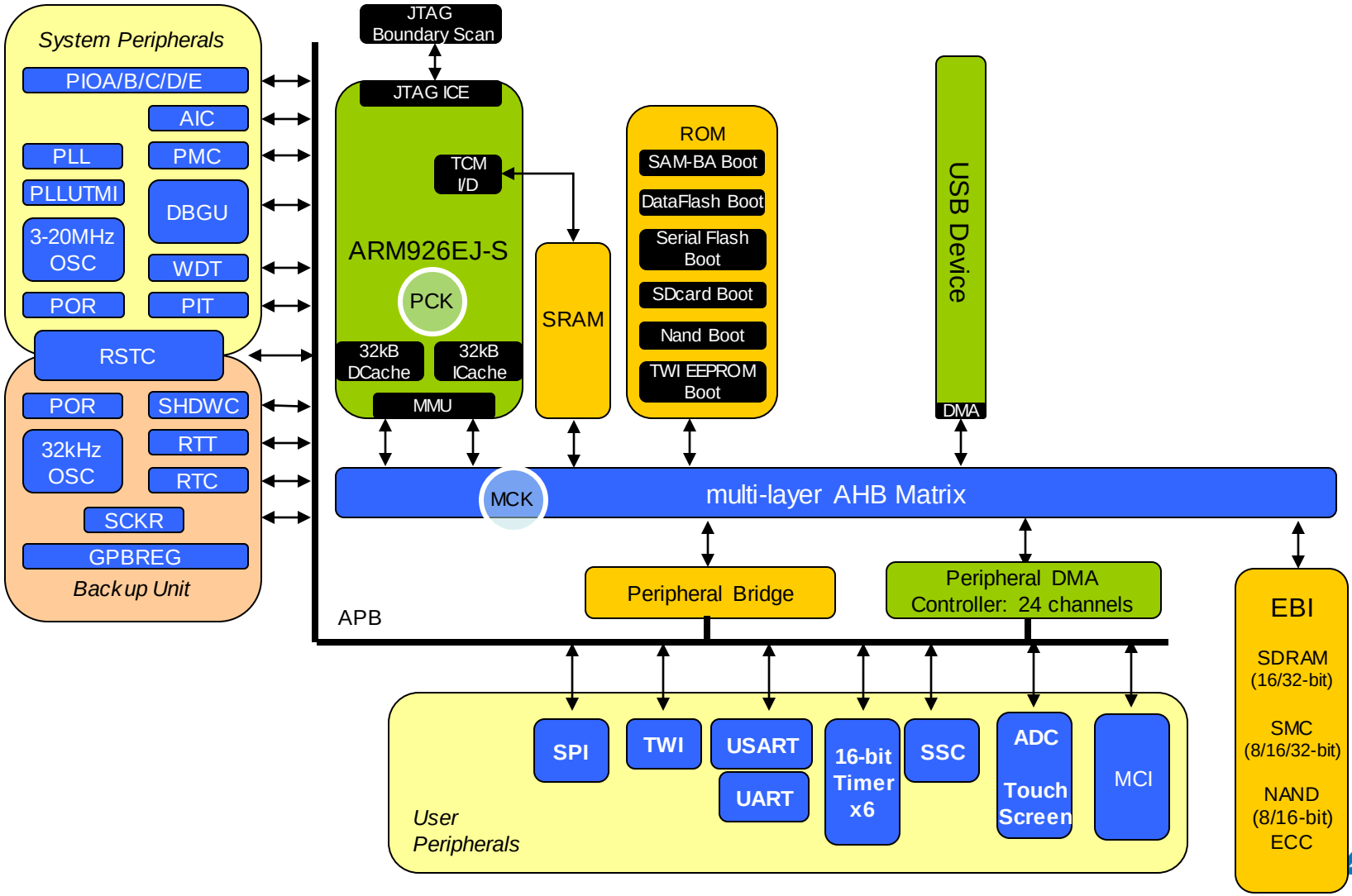
Common Blocks
Block Diagrams

SAM9 Architecture



Peripherals

SAM9 Common Features



Peripherals

DMA Support

- **SPI**
  - 4 NPCS, working at up to MCK/2 (66MHz)
- **USART**
  - Modem, RS485, IrDA, working at up to MCK/2
- **TWI**
  - ATMEL I2C, Master and slave, Fast mode up to 400 kHz
- **ADC**
  - 10-bit, up to 16 channels, resistive touchscreen, 380 Ksps
- **Timer Counter**
  - 16-bit, Capture or Wavegen Mode
- **SSC**
  - Atmel IP, highly-configurable for audio I2S, TDM

High-Speed Peripherals

- **DMA**
  - 8 channels, built-in FIFO, supports mem-to-mem, per-to-mem, mem-to-per
- **USB**
  - Device and Host, High-speed 480 Mbit/s, Full-speed, embedded transceiver
- **MCI**
  - Supports MMC, SDCard up to 52MHz
- **LCD**
  - 1280x860 (WXGA) real RGB frame buffer, up to 24 bits per pixel
- **EMAC**
  - 10/100 Mbit/s, MII/RMII, 128-byte FIFO
- **ISI**
  - Atmel Camera interface, up to 2k x 2k, pixel clock up to 74 MHz, supports YUV 4:2:2, preview path for LCDs, 3x8-bit in RGB, 12-bit in grayscale

Have their own DMA

External Memories

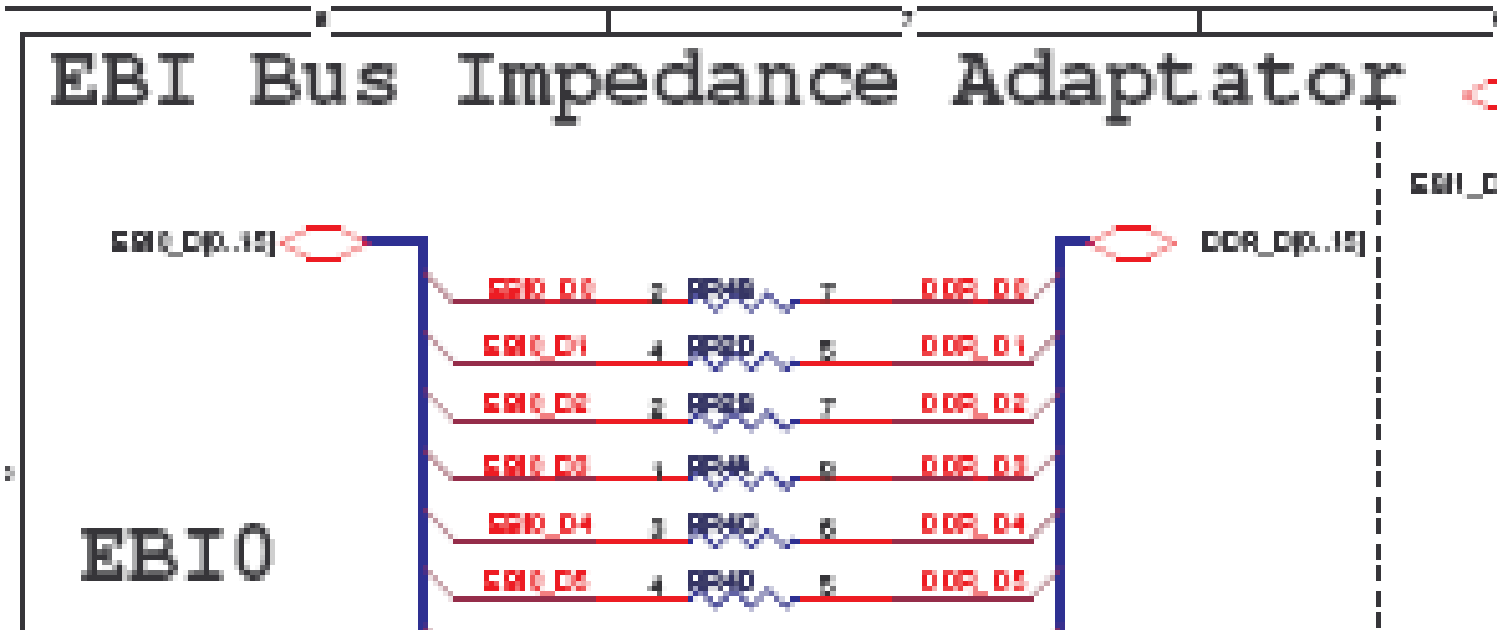
Memories

- **All SAM9 have External Bus Interface**
  - 16-bit DDR2, 16-bit LPDDR, 16-32-bit SDR , 16-32-bit LPSDR (depending on products)
  - NAND Flash (SLC and MLC Devices, DMA channel for automatic block transfer) with up to 24-bit ECC computation
  - Static Memories (Static RAM, NOR Flash, PSRAM, FPGA)

- **Some have Additional DDR2 Controller**
  - DDR CLK and DDR #CLK is up to 133 MHz, Data Rate is up to 266 MHz

EMC Improvement

- Programmable I/O Slew Rate
- Bus impedance adaptation using the IBIS model, 27 Ohms on the EK



SAM9 Family Overview

SAM9	CPU 400 MHz	USB* Device	USB Host	Ethernet	EBI	Camera	LCD	ADC Touch Screen	CAN	AC97
SAM9261(S)	-	FS	X	-	X	-	X	-	-	-
SAM9263	-	FS	X	X	X (x2)	X	X	-	X	X
SAM9260	-	FS	X	X	X	X	-	-	-	-
SAM9G20	X	FS	X	X	X	X	-	-	-	-
SAM9XE	-	FS	X	X	X	X	-	-	-	-
SAM9RL64	-	HS	-	-	X	-	X	X	-	X
SAM9R64	-	HS	-	-	X (16-bit)	-	-	-	-	-
SAM9G45	X	HS	HS	X	X (x2)	X	X	X	-	X
SAM9G15	X	HS	HS	-	X	-	X	X	-	X
SAM9G25	X	HS	HS	X	X	X	-	-	-	X
SAM9G35	X	HS	HS	X	X	-	-	-	-	X
SAM9X25	X	HS	HS	X (x2)	X	-	X	X	X (x2)	X
SAM9X35	X	HS	HS	X	X	-	X	X	X	X

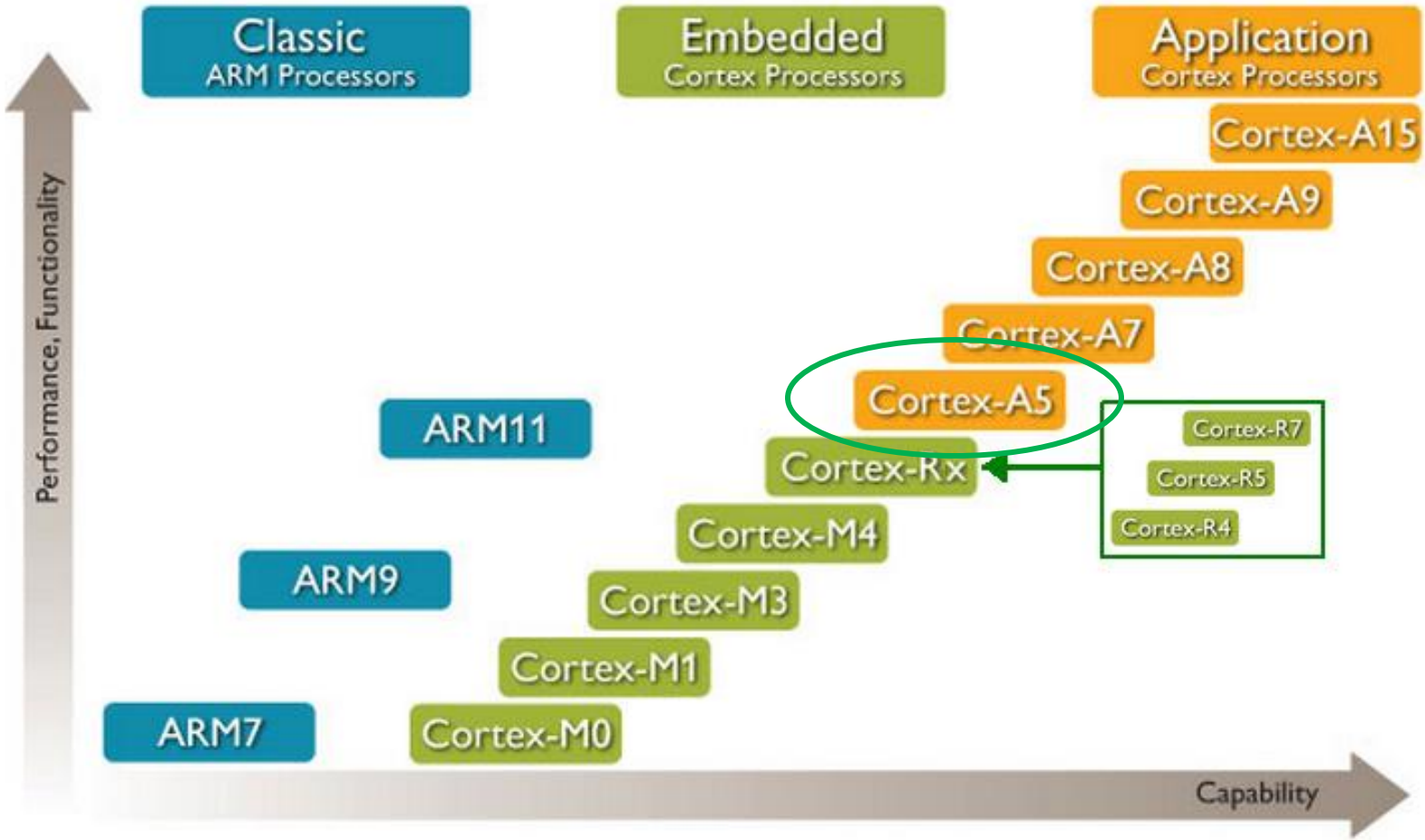
Part 2

Part 1	• ARM926 Core • SAM9 Products • Common Blocks • Peripherals • External Memories
Part 2	• **Cortex-A5 Core** • **SAMA5 Products** • **Peripherals** • **External Memories**
Part 3	• Boot Process • Performances and Power Consumption • Security Features

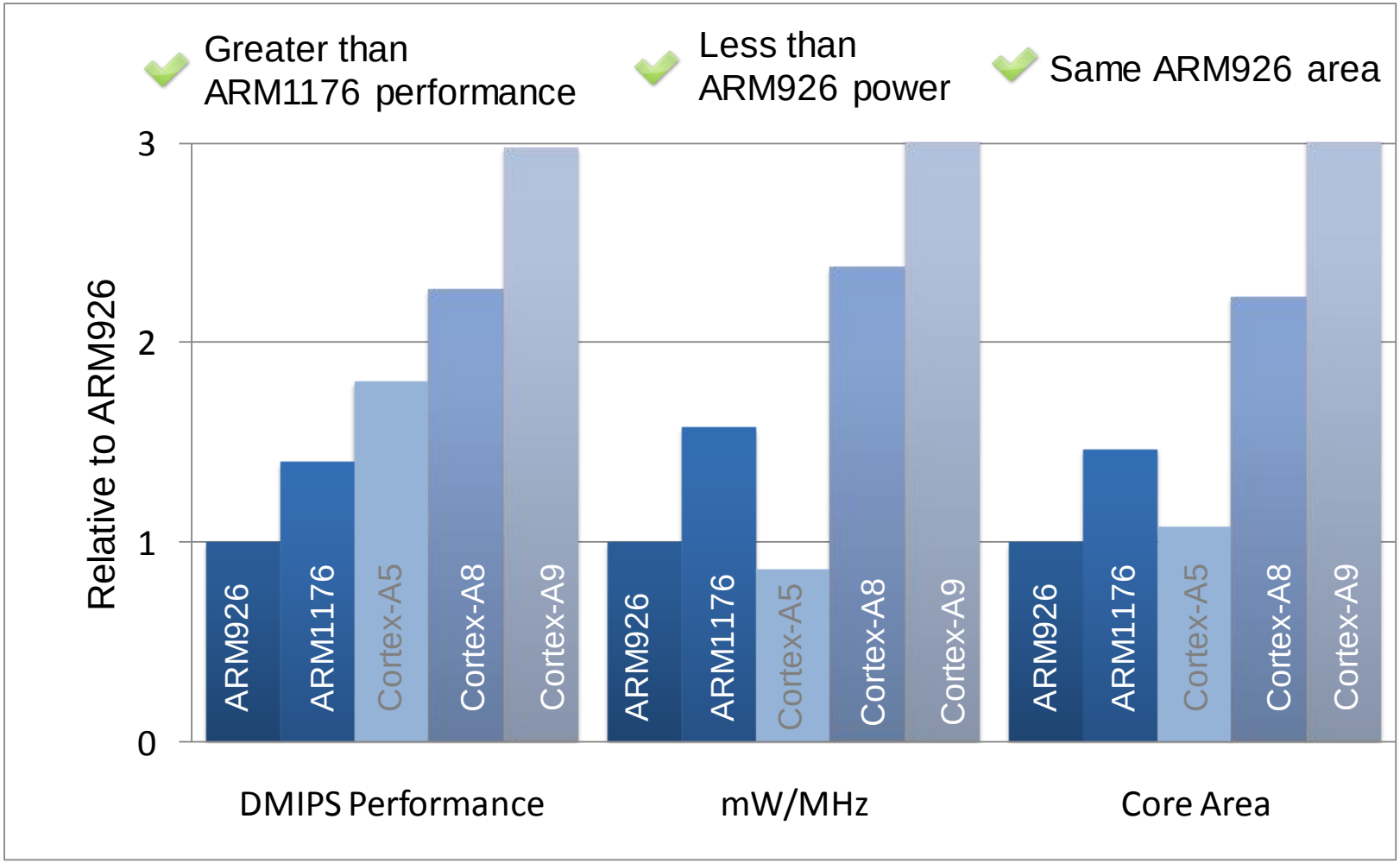
Cortex-A5 Core

ARM cores

- ARM family



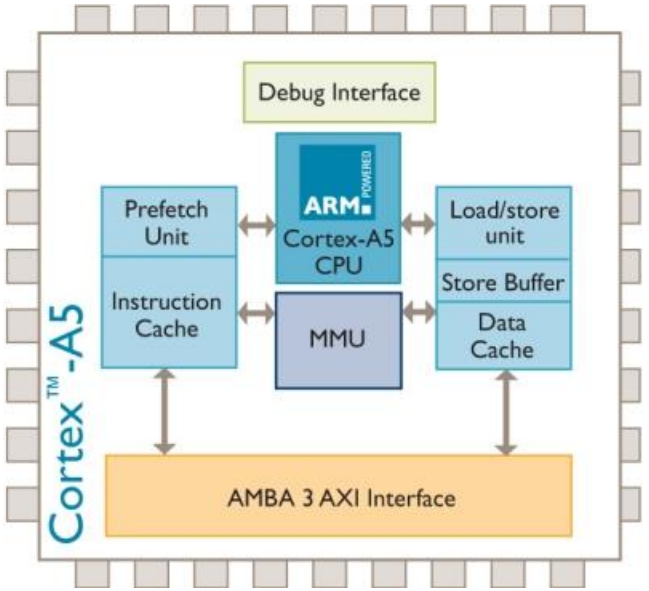
Cortex-A5 Core



Area is integer core only, no NEON, no cache

Cortex-A5 Core

- **Harvard Level 1 Memory System with a Memory Management Unit (MMU)**
  - 32 Kbytes Instruction Cache
    - Two-way set associative
    - Virtual addresses
  - 32 Kbytes Data Cache
    - Four-way set associative
    - Physical addresses
  - Prefetch Unit with Branch Prediction
    - 256-entry pattern history table



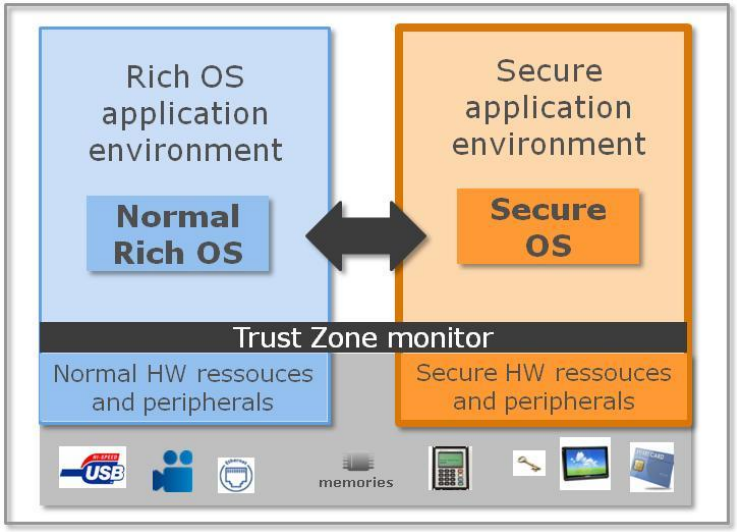
- **8-stage Pipeline + Branch Prediction => 1.57 MIPS/MHz**
- **Level 2 Memory Interface**
  - 64-bit AXI Master Interface
    - Instruction /Data share the same master
- **V7 Instruction Adds one Mode: Monitor (for TrustZone)**

Atmel Cortex-A5 Implementation

Features	SAMA5D3 Implementation	SAMA5D4 Implementation	SAMA5D2 Implementation
Core Implementation	Uniprocessor (UP)	Uniprocessor (UP)	Uniprocessor (UP)
FPU - Floating Point Unit	✓	✓	✓
MMU - Memory Management Unit	✓	✓	✓
NEON™ Advanced SIMD	✗	✓	✓
ETM Interface	✗	✗	✓
TrustZone®	✗	✓	✓
IEM – Intelligent Energy Management	✗	✗	✗
L2-Cache	✗	✓ (128 KB)	✓ (128 KB)

ARM TrustZone

- **ARM TrustZone® Allows the Processor to Run in Two Different Modes**
  - One secure environment to execute critical security/safety software
  - One normal environment to run a Rich OS application software such as Linux
- **This System Approach Allows**
  - Control access of DMA, CPU, peripherals, memories (on chip and off chip) with programmable secured regions
  - Secure peripherals to ensure they can be protected from software attack
  - Isolate critical software from the application OS

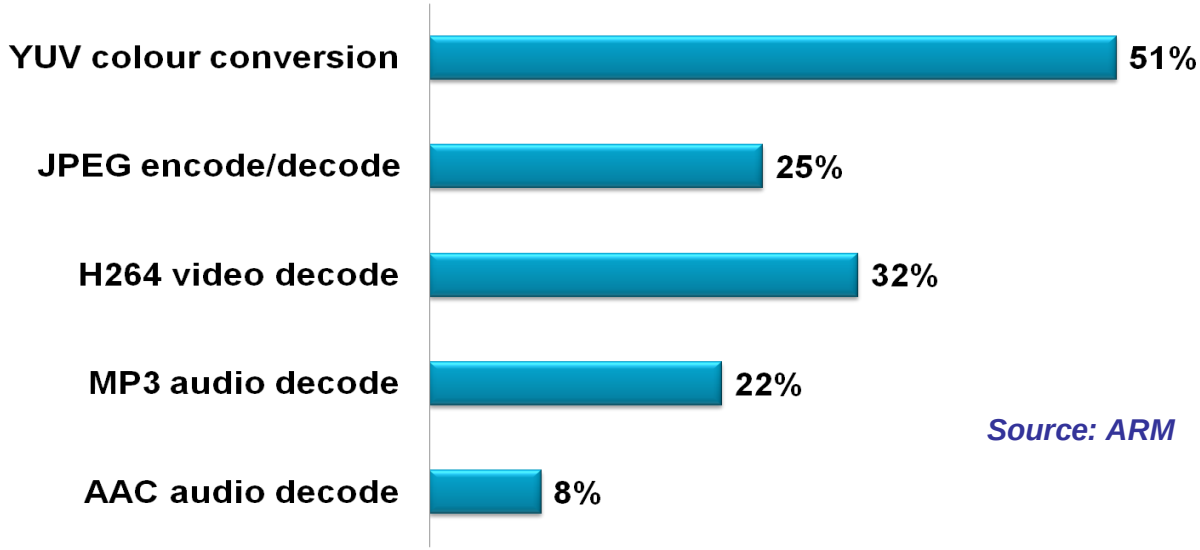


Performance Increase with NEON™ Media Processing Engine

- Up to 75% time reduction Compared to SAMA5D3 on FFT Algorithms

FFT type	C time (us)	NEON time (us)	Saved time
FFT, 256 point, 16 bit, Real-valued	366	92	75%
FFT, 256 point, 16 bit, Complex-valued	550	183	66%

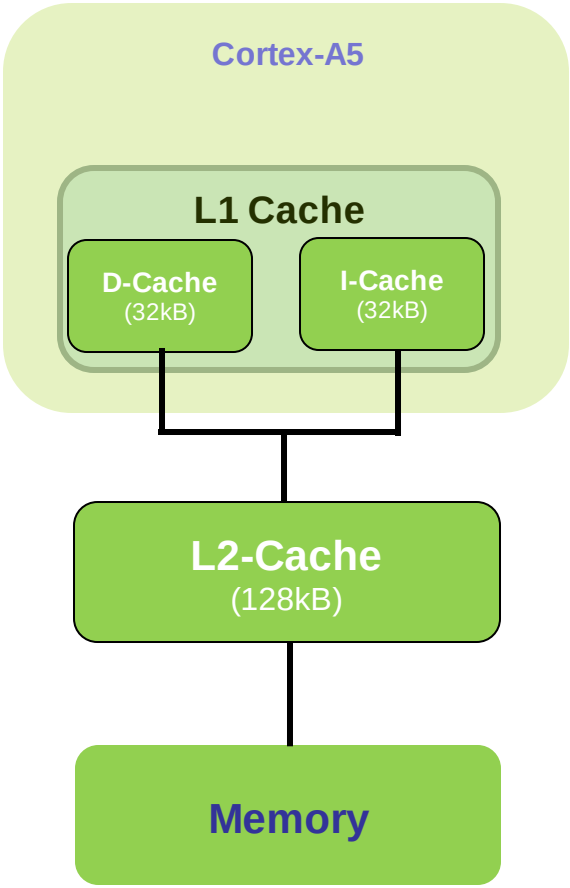
- H264 Encoding Improvement Based on ITTIAM Codec



Relative comparison of NEON media algorithms based on OpenMax DL libraries

System Architecture – L2 Cache

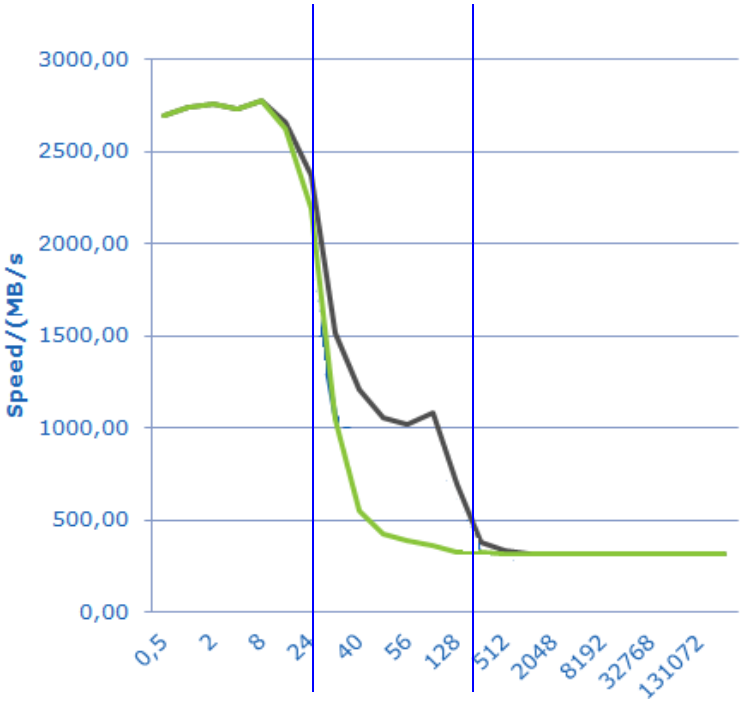
- **Improve Performances when Heavy Memory Traffic is Required**
  - Reduces number of external memories accesses
- **Controlled by the L2-Cache Controller (L2CC)**
  - External to the core
  - Unified, physically addressed and tagged
- **8-way Set Associative Cache Architecture**
- **Operates at MCK Frequency**
  - Slower than L1-Cache (inner cache)
- **No Hardware L1/L2-Cache Coherency**



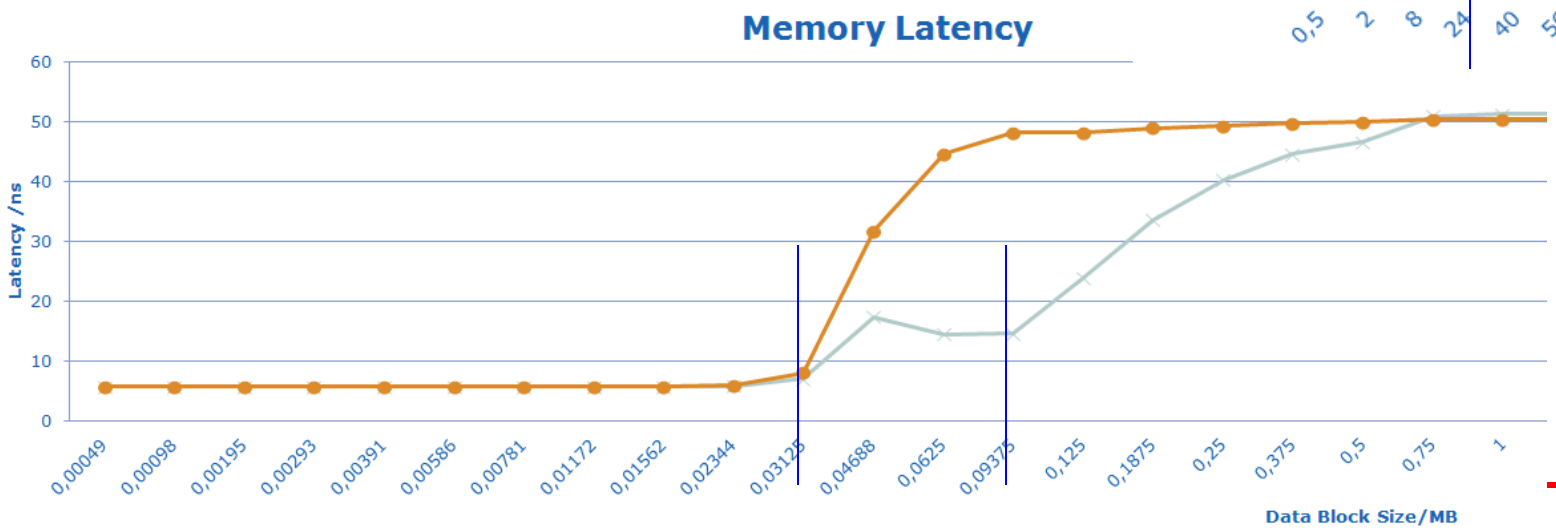
System Architecture – L2 Cache

- **SAMA5D4/D2 with L2-cache vs. SAMA5D3 (no L2-cache) Comparison Using Lmbench**

	Read Speed	Write Speed
SAMA5D4	x1.5	x2



- **L2-cache Improves Latency (Divided by 3) with Block Data up to 750 kB**



ETM upgraded

- **Real-time Instruction And Data Tracing of the Processor**
  - Trace and debug your system execution in real-time
  - Non-intrusive and cycle accurate
- **ETM Uses JTAG Pins**
- **8 Kbytes of Embedded Trace Buffer (ETB)**
- **32-bit Data Width**

GPIO I/O Sets

- **For SAMA5D2 only**
- **An I/O Set Defines the Pin Assignment of Communication Peripherals**
  - To be defined at startup in the Boot Configuration Word
  - Each peripheral's ports have one or more different I/O sets
  - Outputs and inputs can be duplicated
  - Up to 6 functions can be multiplexed on the same line
  - Different speed depending on the function, up to 133MHz
- **HW Schematics Must be Aligned with the Selected I/O Set**
  - GPIO assignment for each I/O set given in the datasheet

Peripheral	IO Set	Signal	GPIO
SPI_0	1	SPCK	PIOA14
		MOSI	PIOA15
		MISO	PIOA16
		NPCS0	PIOA17
	2	NPCS0	PIOA30
		MISO	PIOA31
		MOSI	PIOB0
		SPCK	PIOB1

SAMA5 Products

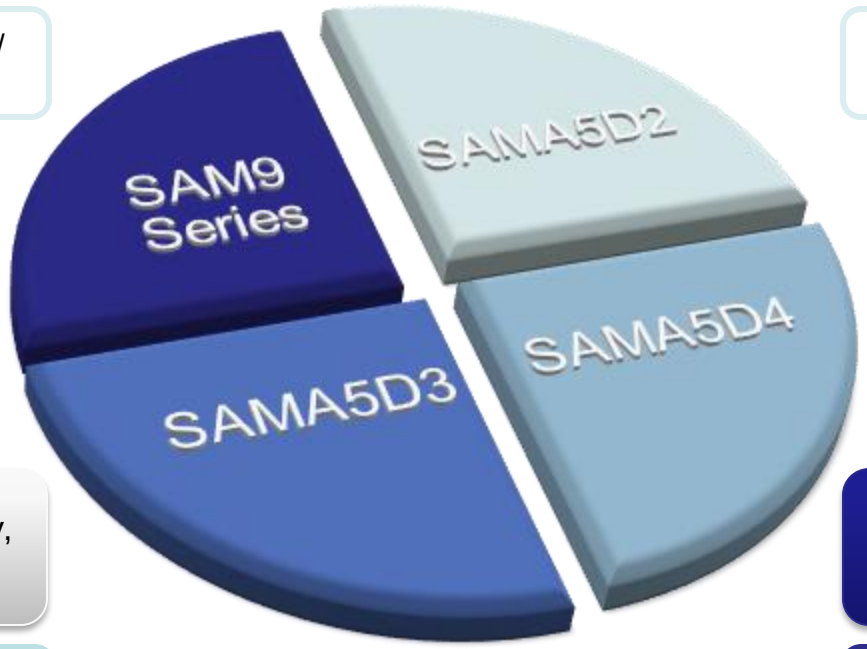
Product Portfolio

Entry Level MPU, Price, SDRAM

Entry Level UI Applications / Basic Linux Machine

DDR3 Support, Low Power, **Low system cost** High Grade Security

Secure Gateway, Payment, Battery Operated Applications



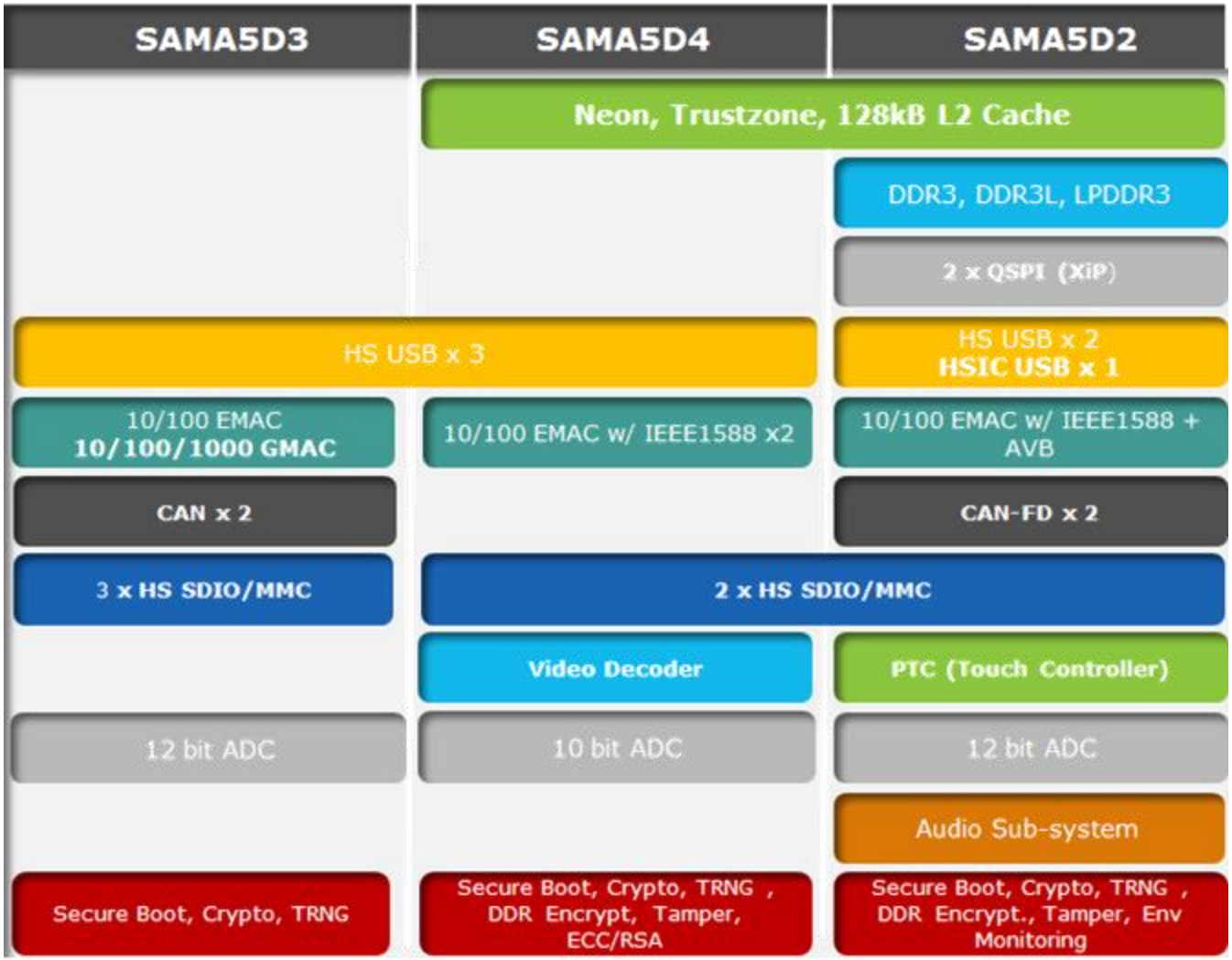
Low Power, Connectivity, **Large number of I/Os**

Battery Operated Applications, Gateway

HW **Video Decoder**, **Performance**, Advanced Security

UI with Video applications, Secure Gateway

SAMA5 Features



Shared Features

- **Cortex A5 with vFPU 500-600MHz**
- **L1 Cache (2 x 32kB) 128kB SRAM**
- **DDR2, LPDDR, LPDDR2**
- **24-Bit LCD**
- **Camera Interface**
- **USART, SPI, I2C, I2S**
- **Linux BSP**

SAMA5D3 Derivatives

Features	SAMA5D31	SAMA5D33	SAMA5D34	SAMA5D35	SAMA5D36
package	BGA324 (15x15,0.8mm pitch or 12x12, 0.5mm pitch)				
I/Os	160				
LCDC	✓	✓	✓	–	✓
GMAC	–	✓	✓	✓	✓
EMAC	✓	–	–	✓	✓
CAN0&1	–	–	✓	✓	✓
Camera int.	–	✓	–	✓	✓
SD/MMC 2	✓	–	✓	✓	✓
Cryptography	✓	✓	✓	✓	✓
Secure boot	✓	✓	✓	✓	✓

SAMA5D2 Derivatives

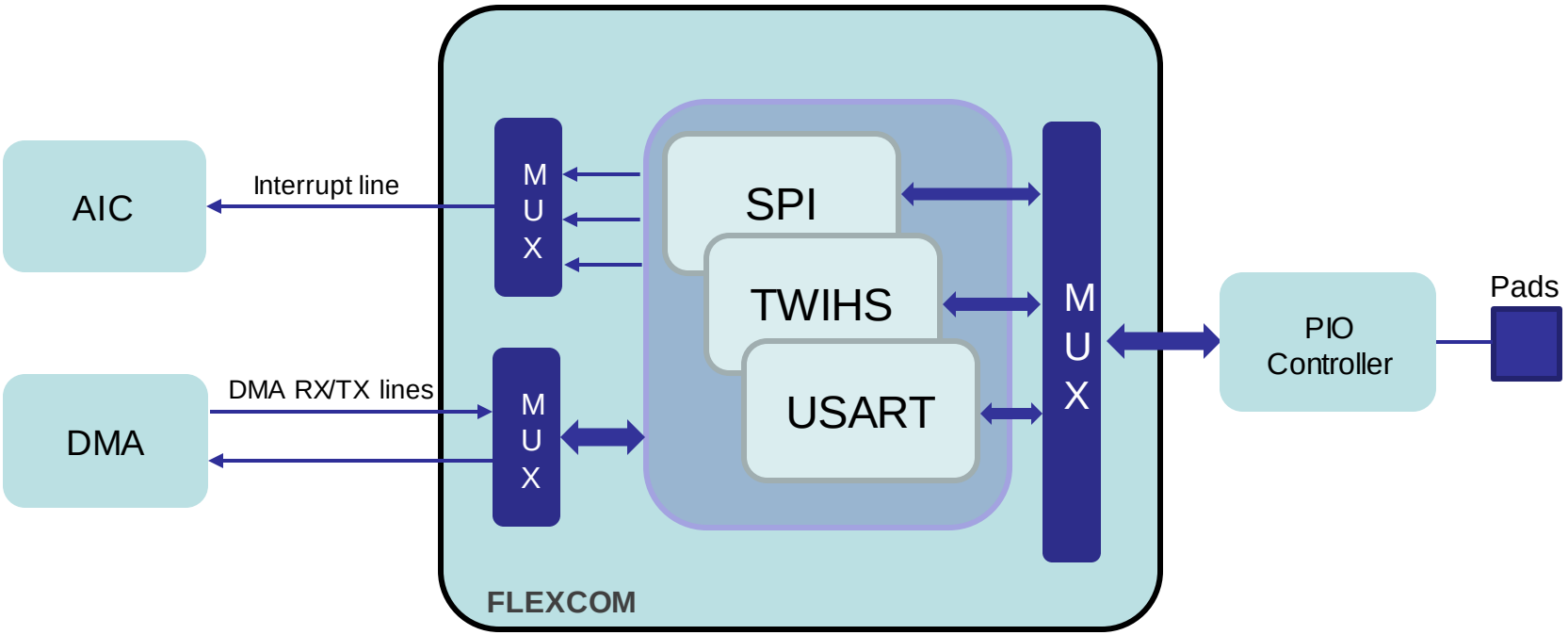
	SAMA5D21	SAMA5D22	SAMA5D23	SAMA5D24	SAMA5D26	SAMA5D27	SAMA5D28
Package	BGA196 (11x11, 0.75mm pitch)			BGA256 (8x8, 0.4)	BGA289 (14x14, 0.8)		
IOs	72			105	128		
DDR bus	16-bit	16-bit	16-bit	16/32-bit	16/32-bit	16/32-bit	16/32-bit
Ext. Temp. option	–	✓	✓	–	✓	✓	✓
CAN-FD	–	✓	✓	–	–	✓	✓
USB HSIC	–	–	–	✓	–	✓	✓
Secure Boot, Tamper	–	✓	✓	✓	–	✓	✓
Enc/Dec OTF	✓	✓	✓	✓	✓	✓	✓
Security monitors, die shield	–	–	✓	–	–	–	✓

Please refer to datasheet for CPN list

Peripherals

FLEXCOM

- **Three Configurable Modes**
  - TWIHS master/ high-speed slave with 16 bytes FIFO, up to 3.4 Mbit/s
  - SPI master/slave with 32 bytes FIFO
  - USART with 32 bytes FIFO supporting LIN, ISO7816, RS485 and IrDA

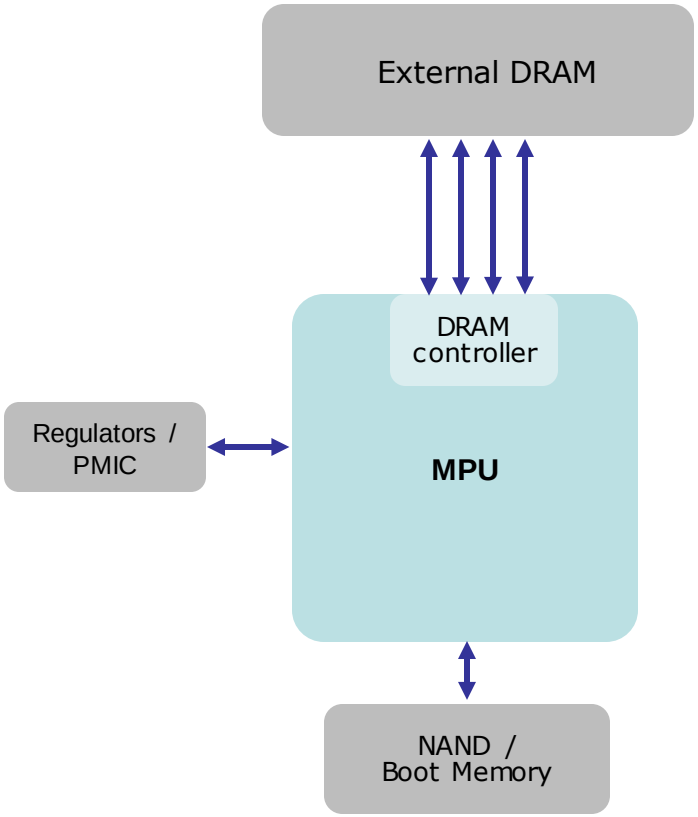


Quad SPI (QSPI)

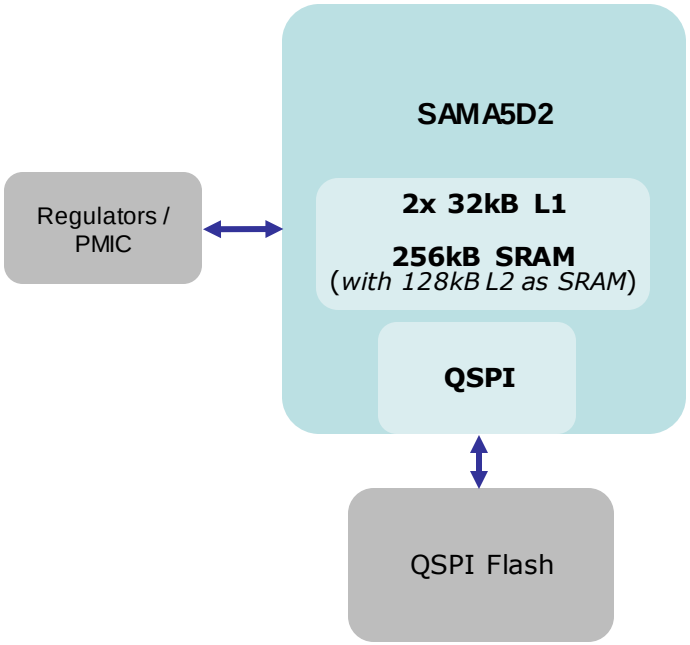
- **Two Quad SPI Ports**
  - Operating in Single-bit SPI, Dual SPI and Quad SPI
  - 32-bit address mode (default is 24-bit address) to support Serial Flash memories larger than 128 Mbits
  - Up to 133MHz
- **Supports “Execute In Place” (XIP)**
  - Code execution by the system directly from a Serial Flash Memory
  - Supported by the BootROM
  - Leads to DDR-less System
- **On-The-Fly Scrambling/Unscrambling Capability**
  - Zero penalty on data rate
- **On-the-fly Encryption/Decryption using AESB**

QSPI eXecute In Place (XiP)

- **XIP Support for Low-cost / RTOS-optimized Configuration**



Standard MPU Configuration



SAMA5D2 DDR-less Configuration
(L2 cache configured as SRAM)

SAMA5D2 Audio Subsystem

- **Fractional-N Audio PLL with Dedicated Clock Output**
  - Enables Audio Master clock generation for external devices (DACs, CODECs, etc.)
  - Saves one on-board crystal (12.288 MHz or 11.2896 MHz)
- **Up to 4x I²S Ports**
  - **2x SSC**
    - Feature-rich audio interface (fully programmable)
    - Supports I2S or TDM transmissions
    - Asynchronous RX and TX
  - **2x I²S**
    - Left or I²S justification, 8 to 32 bits per channel
    - RX and TX share the same bit and frame clock
- **PDM Interface (PDMIC)**
  - Supports 16-bit resolution sampling for microphone applications
  - Hardware x64/x128 decimation filters
- **CLASS D Amplifier**
  - Output power from 500mW to ~5W. Depends on output stage
  - Saves 0.5$ in BOM

High-Speed Peripherals

Have their own DMA

- **DMA -> XDMA**
  - Up to 24 channels, built-in FIFO, supports mem-to-mem, per-to-mem, mem-to-per
- **USBHS**
  - Full digital High-Speed Inter-Chip (HSIC), no PHY is needed, can replace SPI/I2C
- **MCI -> SDMMC**
  - Supports MMC up to 120 MHz, SDIO up to 104 MHz, SDXC, SDHC up to 52 MHz
- **LCD**
  - 720p (up to 30fps), video overlays with rotation, composer with alpha blending
- **EMAC -> GMAC**
  - Gigabit on D3, 10/100 Mbit/s, MII/RMII, 4 kB FIFO, wake-on-LAN, Precision Time Protocol IEEE1588, AVB
- **ISI -> Image Sensor Controller**
  - Camera interface, pixel clock up to 96 MHz, Raw Bayer input format

External Memories

External Memories

SDRAM Type	“old” SAM9	SAM9x5	SAM9G45	SAMA5D3	SAMA5D4	SAMA5D2
Core Freq (MHz)	200	400	400	536	600	500
Bus Freq (MHz)	100	133	133	178	200	166
SDR 3.3V LPSDR 1.8V	32-bit	32-bit	32-bit	-	-	-
DDR2 1.8V LPDDR1 1.8V	-	16-bit	16-bit (dual)	32-bit (only)	32-bit	32-bit
LPDDR2 1.2V	-	-	-	32-bit (only)	32-bit	32-bit
DDR3 1.5V DDR3L 1.35V LPDDR3 1.2V	-	-	-	-	-	32-bit
NAND Flash 1.8V / 3.3V	x	x	x	x	x	x
Static Memory	32-bit	32-bit	32-bit	16-bit	16-bit	16-bit
Data Scrambling	-	-	-	x	x	x
Data Cyphering	-	-	-	-	x	x
Auto Adaptative Pads	-	-	-	x	x	x

SAMA5Dx DDR Summary

- **8-bank Support**
  - DDR CS has been extended to 512 MB
- **32-bit Width**
- **Data scrambling**
- **Data cyphering**
- **Auto Adaptative Pads**
  - No overshoots, EMI is reduced
  - No need for serial resistors, BOM is reduced
  - Lower consumption on I/Os due to edges that are less sharp
  - DDR_CAL pins

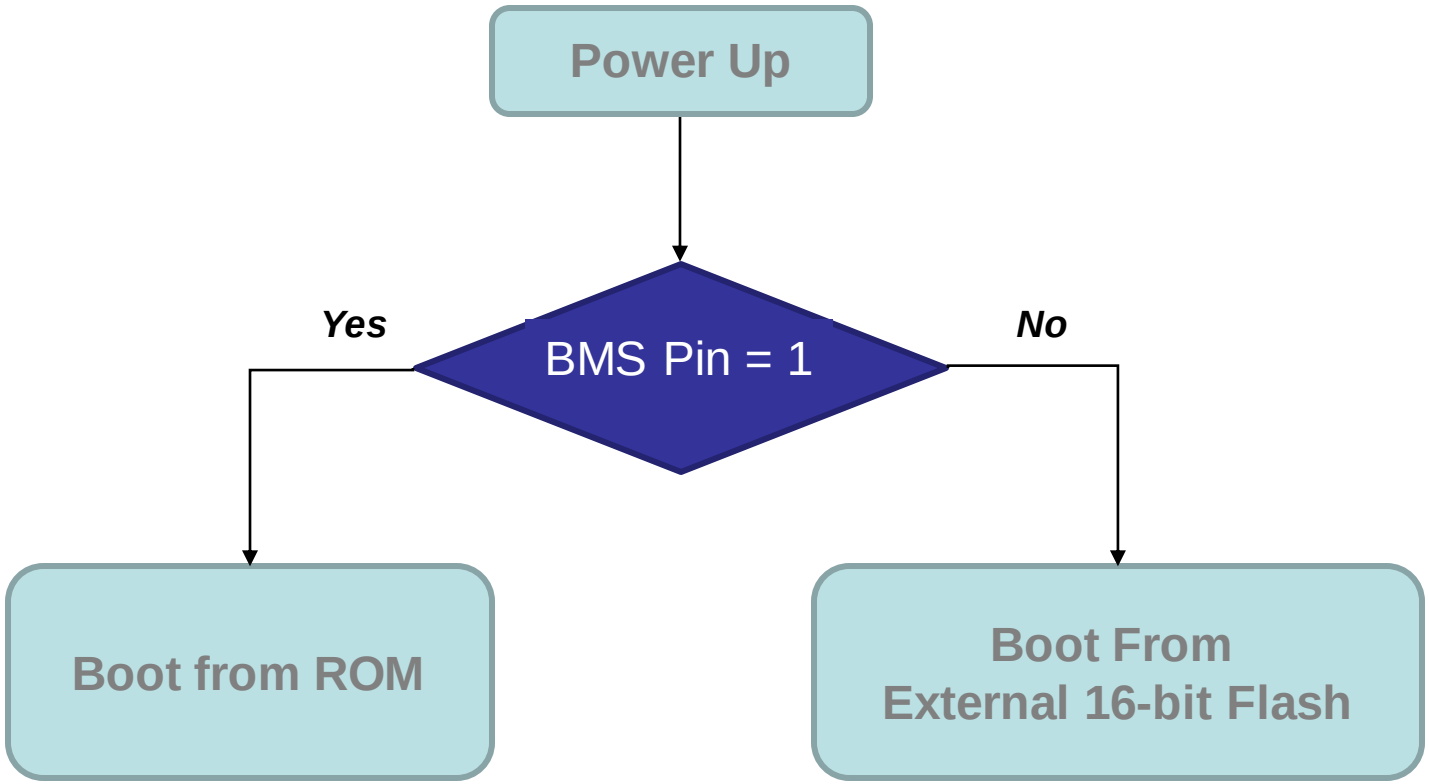
Part 3

Part 1	• ARM926 Core • SAM9 Products • Common Blocks • Peripherals • External Memories
Part 2	• Cortex-A5 Core • SAMA5 Products • Peripherals • External Memories
Part 3	• **Boot Process** • **Performance and Power Consumption** • **Security Overview**

Boot Process

MPU Boot Memory Selection

- **BMS Pin is Sampled when VDDCORE is Powered**



NVM Memory Bootloader Support

AT91 / NVM	Data Flash (SPI)	Serial Flash (SPI)	Nand Flash (EBI)	SD Card (MCI)	EEPROM (TWI)	QSPI
SAM9260	X	-	SLC w/ block 0	-	-	-
SAM9261	X	X	SLC w/ block 0	X	X	-
SAM9263 rev B	X	-	SLC w/ block 0	X	-	-
SAM9G20 rev A/B	X	X	SLC w/ block 0	X	X	-
SAM9G45/SAM9M10/SAM9M11	X	X	SLC w/ block 0	X (+ SDHC)	X	-
SAM9G15/G25/G35/X25/X35/N12	X	X	SLC / MLC	X (+ SDHC)	X	-
SAMA5D3 and SAMA5D4	X	X	SLC / MLC	eMMC	X	-
SAMA5D2	X	X	SLC / MLC	eMMC	X	X

- If no valid boot found, ROM code embeds SAM-BA Boot
  - Monitor that provides In-System Programming solutions through different communication channels
    - DBGU Serial port interface
    - USB Device port

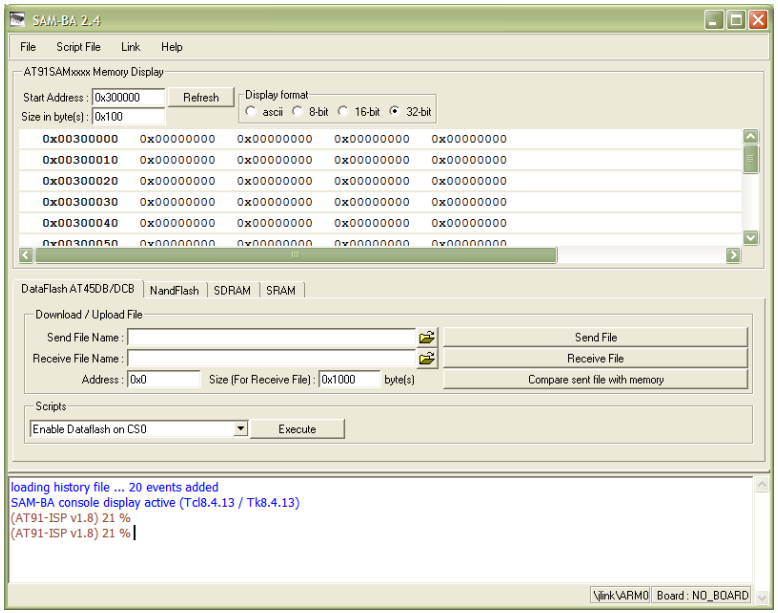
Atmel SAM-BA 2.X GUI

- **Customizing SAM-BA 2.X is Possible by Adding or Modifying TCL Scripts Files**

Create your own board

Add memory modules

Modify memory algorithms



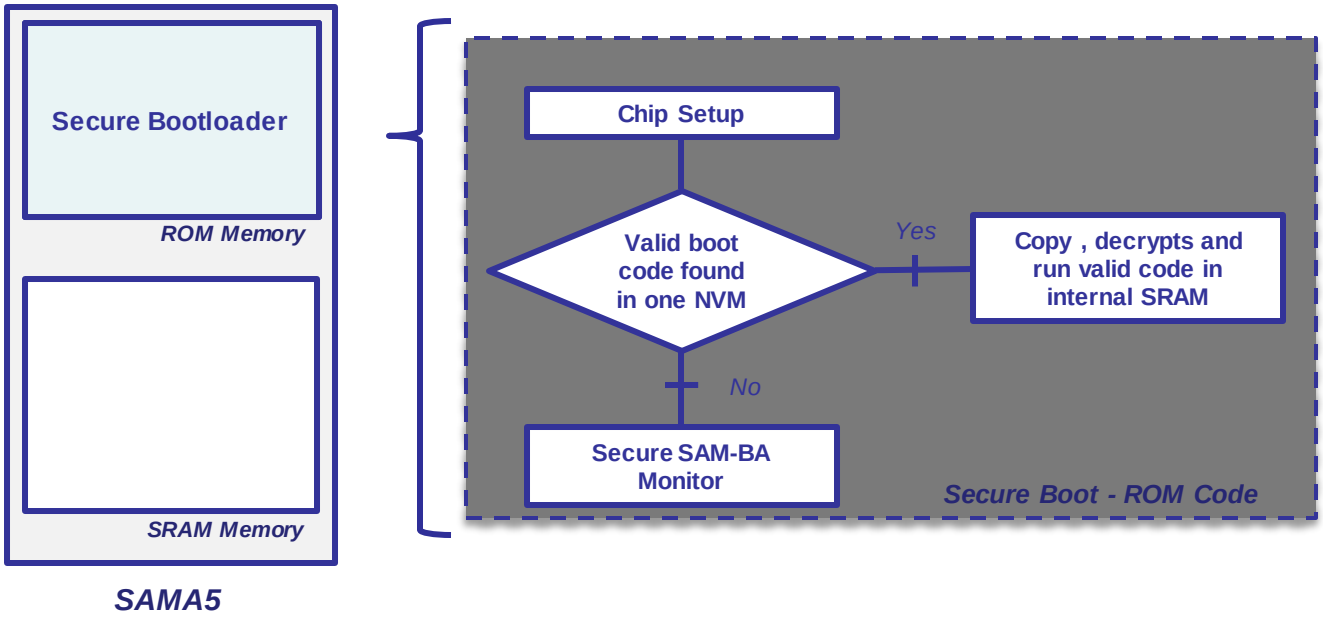
- **Command Line Mode Allows Memory Programming without any GUI Interaction**

- **New version is SAM-BA v3.1 in command line only**

Secure Boot

ROM Boot Secure

- Similar Process to Standard Boot (except for BMS)
- ROM Code Searches for a Valid Boot Code in NVM
- Authenticates, Decrypts and Copies the Valid Boot Code into Internal SRAM and Runs Code
- If No Valid Code is Detected, Secure SAM-BA Monitor is Executed



SAMA5D2 Secure Boot Features

- **SAMA5D2 Features**
  - Array of 544 OTP bits (512 for SAMA5D4)
  - Bits in special register to forbid ROM and OTP read accesses

- **Secure Bootloader is Used to**
  - Store the customer key and hash in OTP area
  - Store an encrypted bootstrap in a Non-Volatile Memory (NVM)
  - Checks the customer bootstrap's signature
  - Decrypt the customer bootstrap prior to launching it

- **Atmel Provides Tools to Cypher and Sign Bootstrap and Application**

Performance and Power Consumption

Typical Power Management

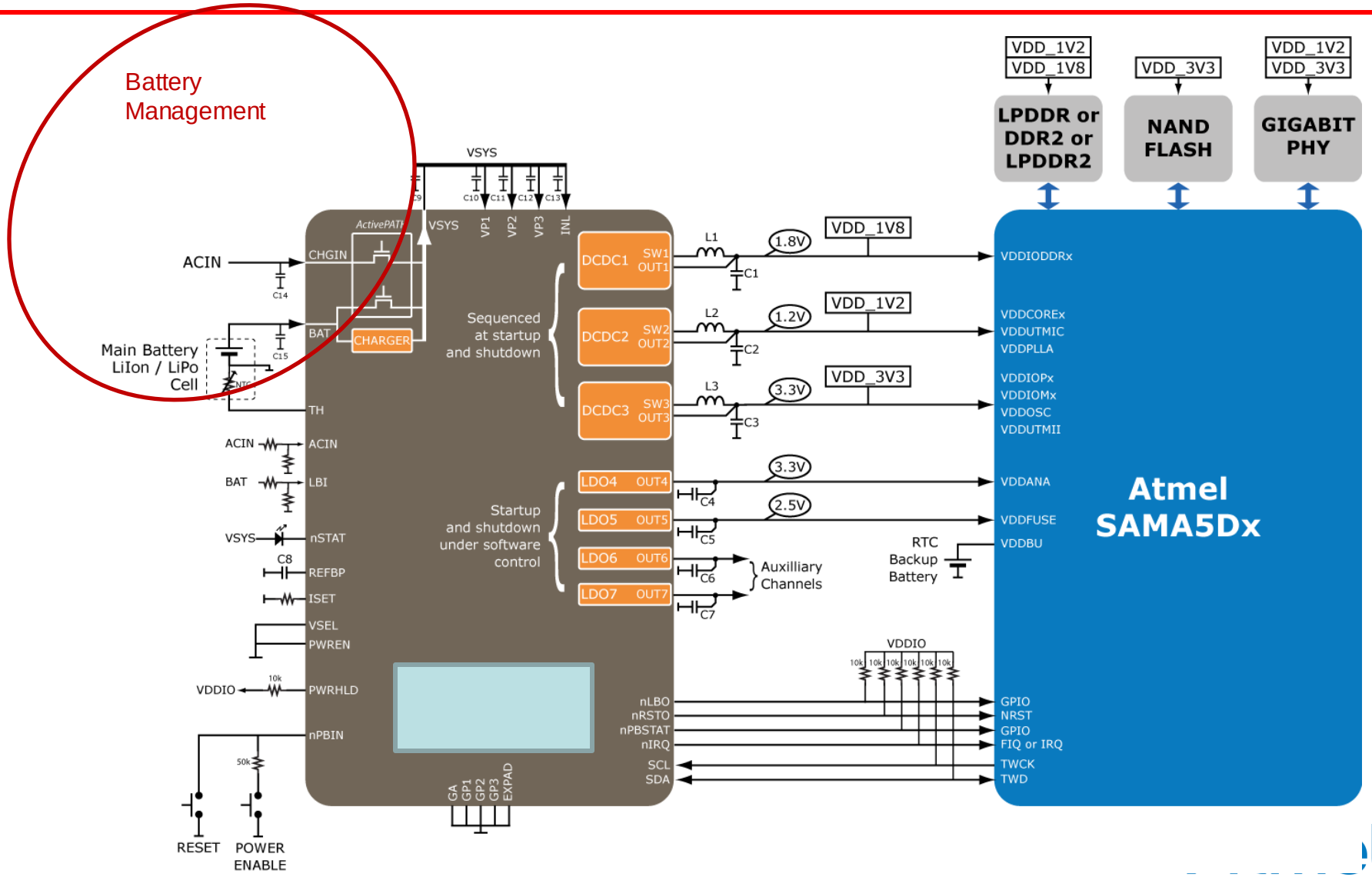
Power Rail	Voltage	Associated Ground
VDDCORE	1.10V – 1.32V, 1.20V	GNDCORE
VDDPLLA	1.10V – 1.32V, 1.20V	GNDPLLA
VDDUTMIC	1.10V – 1.32V, 1.20V	GNDUTMII-> USB
VDDUTMII	3.00V – 3.60V, 3.30V	GNDUTMII
VDDOSC	1.65V – 3.60V	GNDOSC
VDDIODDR	1.70V – 1.90V, 1.80V	GNDIODDR
	1.14V – 1.30V, 1.20V	
	1.29V – 1.45V, 1.35V	*For DDR3(L), SAMA5D2 only*
	1.43V – 1.57V, 1.50V	
VDDIOPx	1.65V – 3.60V	GNDIOPx
VDDANA	1.65V – 3.60V, 3.30V	GNDANA
VDDFUSE	2.25V – 2.75V, 2.50V	GNDFUSE
VDDBU	1.65V – 3.60V	GNDBU
VDDHSIC	*1.10V – 1.30V, 1.20V*	*GNDUTMII*
VDDISC	*1.65V – 3.60V*	*GNDISC*
VDDSDMMC	*1.65V – 3.60V*	*GNDSDMMC*
VDDAUDIOPLL	*3.00V – 3.60V, 3.30V*	*GNDAUDIOPLL/GNDDPLL*

Power Management Solutions

- **Reference Design with PMIC for SAMA5**
  - Schematics available in the SAMA5D2-XULT User Guide
  - Cost: ~1$ for 10Ku

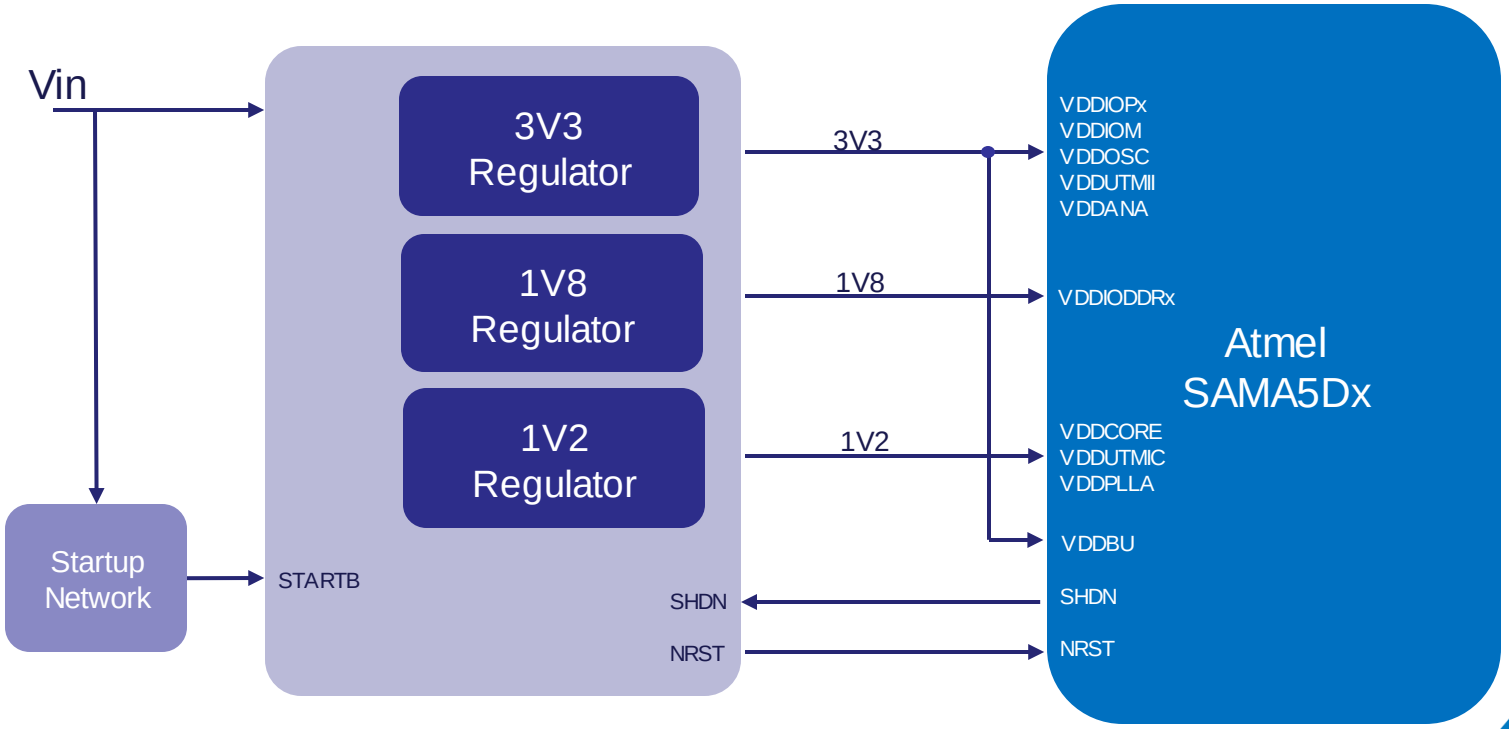
- **Solution with Discrete Components also Available**
  - Schematics available in a dedicated application note: *SAMA5D2 Discrete Power Supply Solution* available on atmel.com
  - Cost: ~1,2$ for 10ku

PMIC Typical Connection



Discrete Typical Connection

- **Based on 3 Different Voltage Regulators and a Startup Network**
- **Dedicated Application Note on atmel.com**
  - http://www.atmel.com/Images/Atmel-44022-32-bit-ARM-Embedded-Microprocessor-Discrete-Power-Supply-Solution-for-Atmel-eMPUs_Application-note.pdf
- **Cost is < 1$ for 100Ku**



Low Power Modes Definition

Mode	What is active?	Core/ Bus Frequency	Entry Mode	Wake-up Source	Wake-up Time
Idle	RC Oscillators SECURAM Secure Box Module System Bus DDR	OFF /166 MHz	WFI	Any interrupt	880ns @ 500 MHz
Ultra Low Power 0	RC Oscillators SECURAM Secure Box Module System Bus	OFF / 512 Hz	DDR self refresh + WFI	Any interrupt	300ms
Ultra Low Power 1 (SAMA5D2 only)	Same as ULP0	OFF /OFF	DDR self refresh + LPM + WFE	Wake up pins and events	15µs
Backup	RC Oscillators SECURAM Secure Box Module	OFF /OFF	SHDN pin	WKUP0 pin, PIOBU, RTC wake-up event, Analog comparison, Character Received on RXLP	Startup time
Backup with DDR Self Refresh			DDR self refresh + SHDN pin		

Active and Low Power Modes

	SAM9261	SAM9G20	SAM9-5	SAM9G45	SAMA5D3	SAMA5D4	SAMA5D2	TI AM3352	Freescale iMX7 Solo	Renesas RZ/A1 Lx
Core Freq (MHz)	188	400	400	400	536	600	500	1000	800	400
Bus Freq (MHz)	94	133	133	133	178	200	166			
Typical Core Power Supply (V)	1.2	1.0	1.0	1.0	1.2	1.8 (embedded regulator)	1.2	1.1	1.1	1.18
Core Consumption at Full Speed (mW)	70	50	110	130	150	328	**150**	1000 (600MHz)	500	450

Mode	SAM9261	SAM9G20	SAM9-5	SAM9G45	SAMA5D3	SAMA5D4	SAMA5D2			
Idle (mW)	13	20	38	55	29	58	34	-	**29**	65
ULP0 (mW)	0.3	8.0	8.0	35	0.5	8.5	**0.7**	16.5 (stdby)	2.5 (stdby)	15
ULP1 (mW)	-	-	-	-	-	-	**0.3**	-	1.8 (dsm)	-
Backup on VDDBU (µW)	3	9	8	8	4	14	**14**	40 (RTC-Only)	15 (snvs)	-
Backup + DDR in Self Refresh (µW)	-	-	-	-	-	-	**14 (VDDBU) + 120 (VDDIODDR)**	40 + ?	210	-

Security Overview

High security

Environmental Monitoring
PCI pre-certification

D23 & D28 only

Advanced security

ARM Trust Zone
DDR encryption
Tamper detection
Secret storage

ARM Trust Zone
DDR encryption
Tamper detection
Secret storage

Medium security

Secure boot

Secure boot

Secure boot

Entry level security

Hardware Crypto engines

SHA, TRNG
AES, 3DES

Hardware Crypto engines

SHA , TRNG
AES, 3DES

Hardware Crypto engines
RSA, ECC
SHA, TRNG
AES, 3DES

Hardware Crypto engines
SHA, TRNG
AES, 3DES
RSA / ECC (by SW)

SAM9

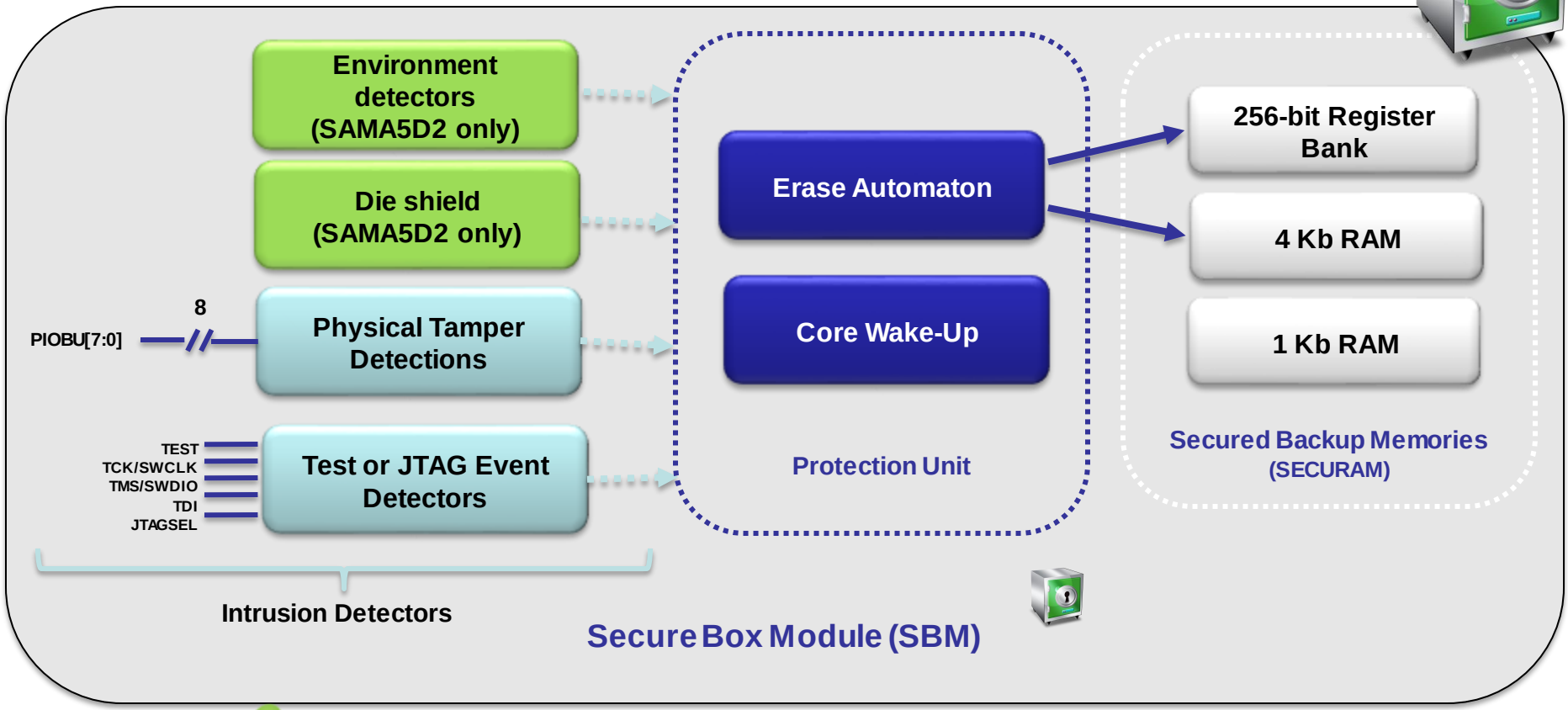
SAM9CN12 & SAMA5D3

SAMA5D4

SAMA5D2

Secure Box Module

- **Provides Permanent Monitoring to Avoid Attacks on the Device**
  - Automatic erase and core wake-up upon intrusion detection



Intrusion detection is described in the document "Secure Box Module (SBM)". This document is available under Non-Disclosure Agreement (NDA). Contact an Atmel Sales Representative for further details.

Thank you for your attention!