



DesignNews

Secure MCUs and RTOSs

DAY 2 : Secure Microcontroller Solutions

Sponsored by



Webinar Logistics

- Turn on your system sound to hear the streaming presentation.
- If you have technical problems, click “Help” or submit a question asking for assistance.
- Participate in ‘Group Chat’ by maximizing the chat widget in your dock.

THE SPEAKER



Jacob Beningo

Visit 'Lecturer Profile'

Beningo Embedded Group - President

Focus: Embedded Software Consulting

An independent consultant who specializes in the design of real-time, microcontroller based embedded software.

He has published two books:

- [Reusable Firmware Development](#)
- [MicroPython Projects](#)
- [Embedded Software Design](#)

Writes a weekly blog for DesignNews.com focused on embedded system design techniques and challenges.

Visit www.benigo.com to learn more ...

Visit 'Lecturer Profile' in your console for more details.

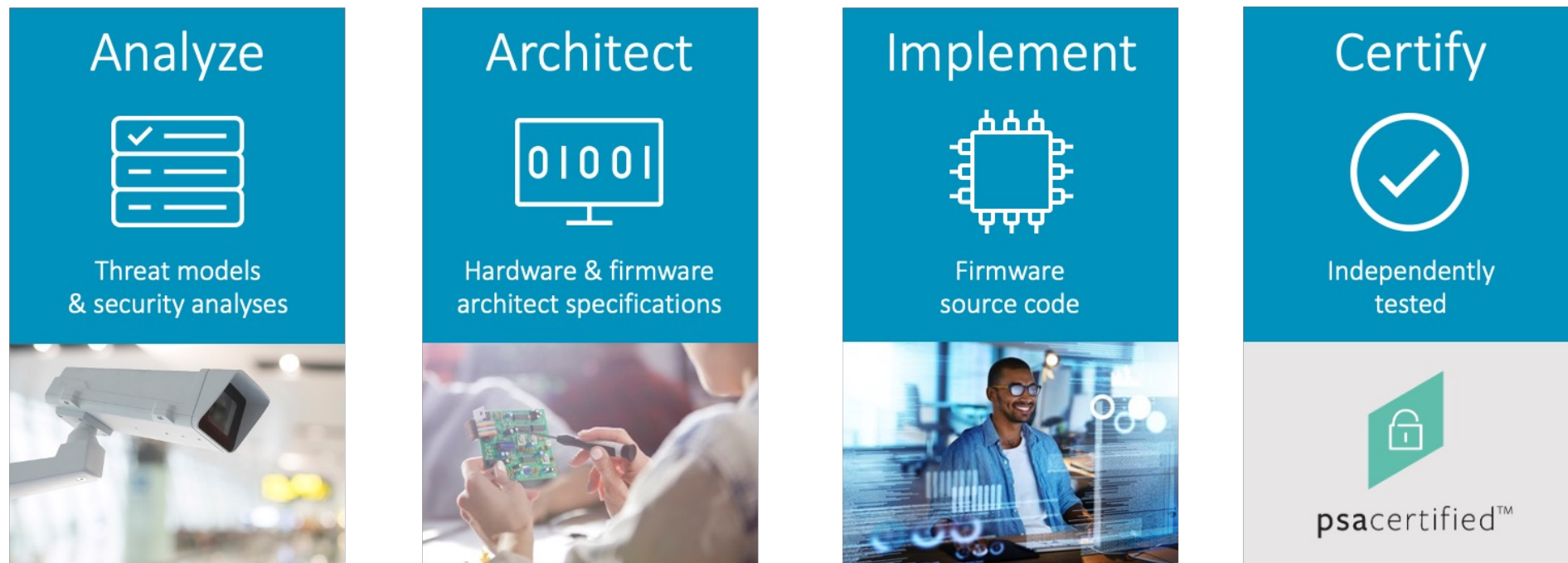
Course Sessions

- Threat Model Security Analysis (TMSA)
- **Secure Microcontroller Solutions**
- Arm TrustZone
- Secure Boot and Firmware Updates
- Secure RTOSes

1

Platform Security Architecture (PSA)

Platform Security Architecture (PSA)



Platform Security Architecture (PSA)

PSA Certification – A certification program based on openly published threat models, specs and open-source reference code.

PSA Certification Level	Silicon	OS	OEM
Level 3 Months	✓		
Level 2 1 month	✓	Third-party evaluation schemes	
Level 1 1 day	✓	✓	✓

Three assurance levels

Level 1: Document & Declare with lab check

- Security Model goals, government requirements
- IoT threat models – SFRs
- Lab check of questionnaire

Level 2: Mid-level assurance/robustness

- Time-limited white box testing
- PP, eval methodology and attack methods

Level 3: Substantial - Root of Trust

- More extensive attacks
e.g. side-channel, perturbation
- Higher assurance

Platform Security Architecture (PSA) – Selecting an MCU

Secure MCU Features

- Encryption
 - Digital signature
 - eFuses
 - Isolated execution environment for trusted applications
 - Secure element functionality
- } **PSA**



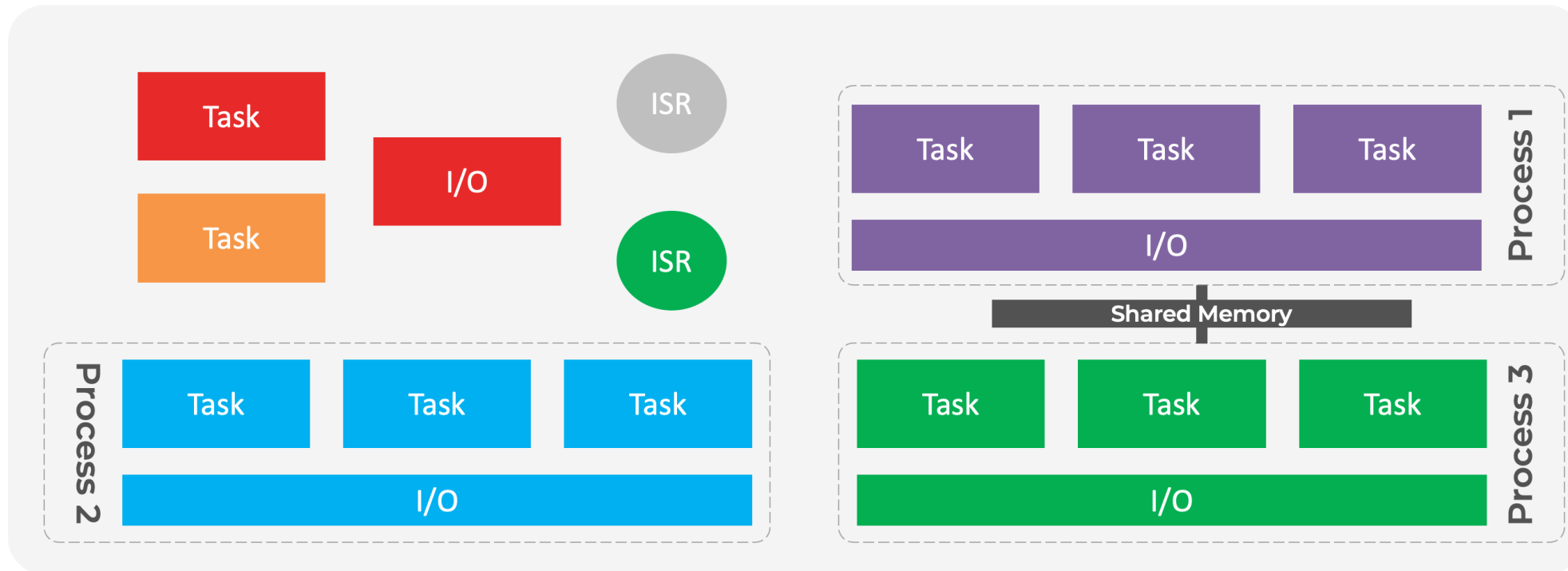
What PSA step is optional for embedded products?

- Analyze
- Architect
- Implement
- Certify

2

MCU Security Solutions

MCU Security Solutions - MPUs



MCU Security Solutions – Multicore Processors

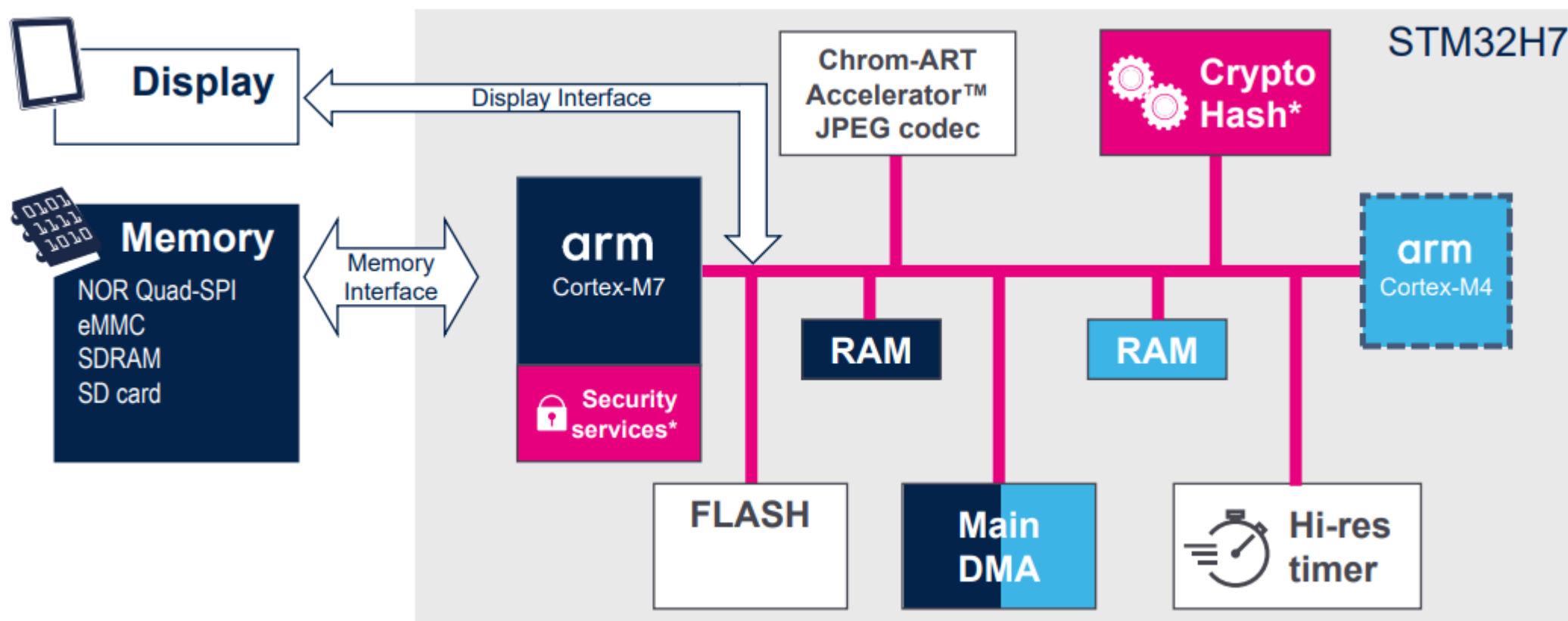


Image Source : STM32H7 MCUs for rich and complex applications, Slide 28

MCU Security Solutions – TrustZone

arm TRUSTZONE

Normal environment (Non-Secure)

Application Examples

- User applications
- RTOS
- Device drivers
- Protocol stacks

Normal Resources

- General peripherals

Handler
Mode

Thread
Mode

Protected environment (Secure)

Secure Software Examples

- Secure Boot
- Cryptography libraries
- Authentication
- RTOS support APIs / RTOS

Secure Resources

- Secure storage
- Crypto accelerators

Handler
Mode

Thread
Mode

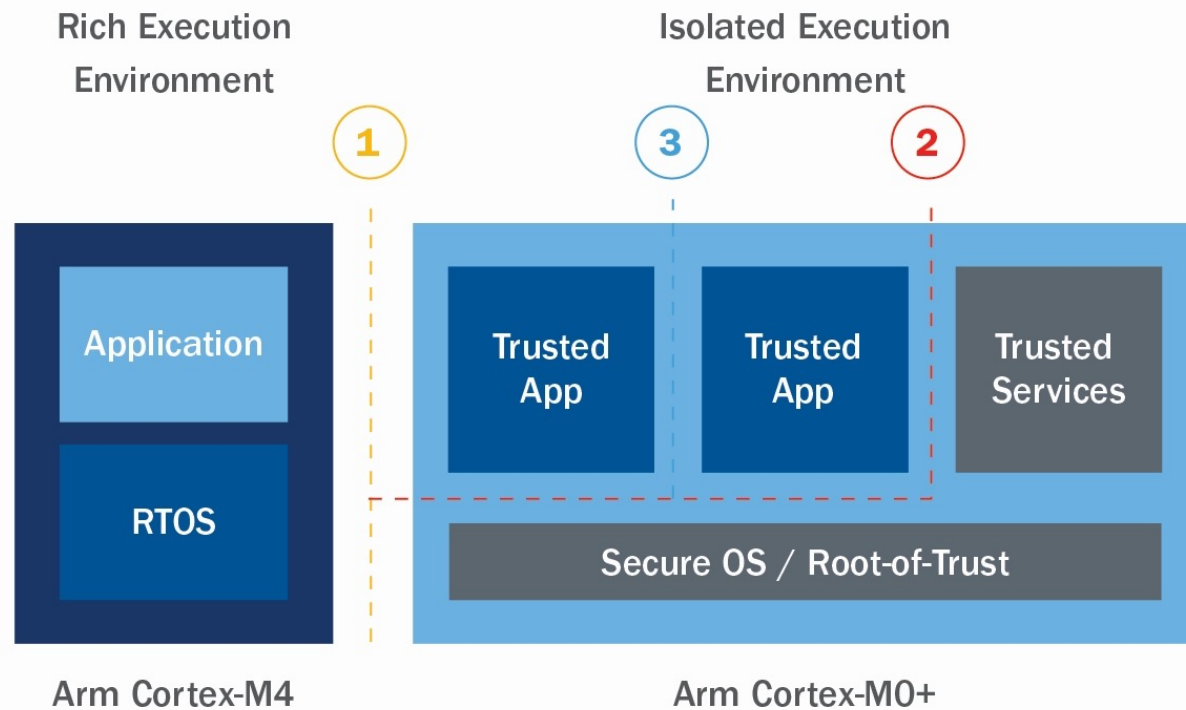
What security tools are familiar with using in an embedded environment?

- MPU
- Secure peripherals
- Multicore MCU
- TrustZone
- All the above
- Other

3

Example MCUs

Example MCUs – PSoC64





Hardware based isolation within PSoC 64 Secure MCUs enables secure element functionality and reduces the attack surface

3 Levels of Isolation

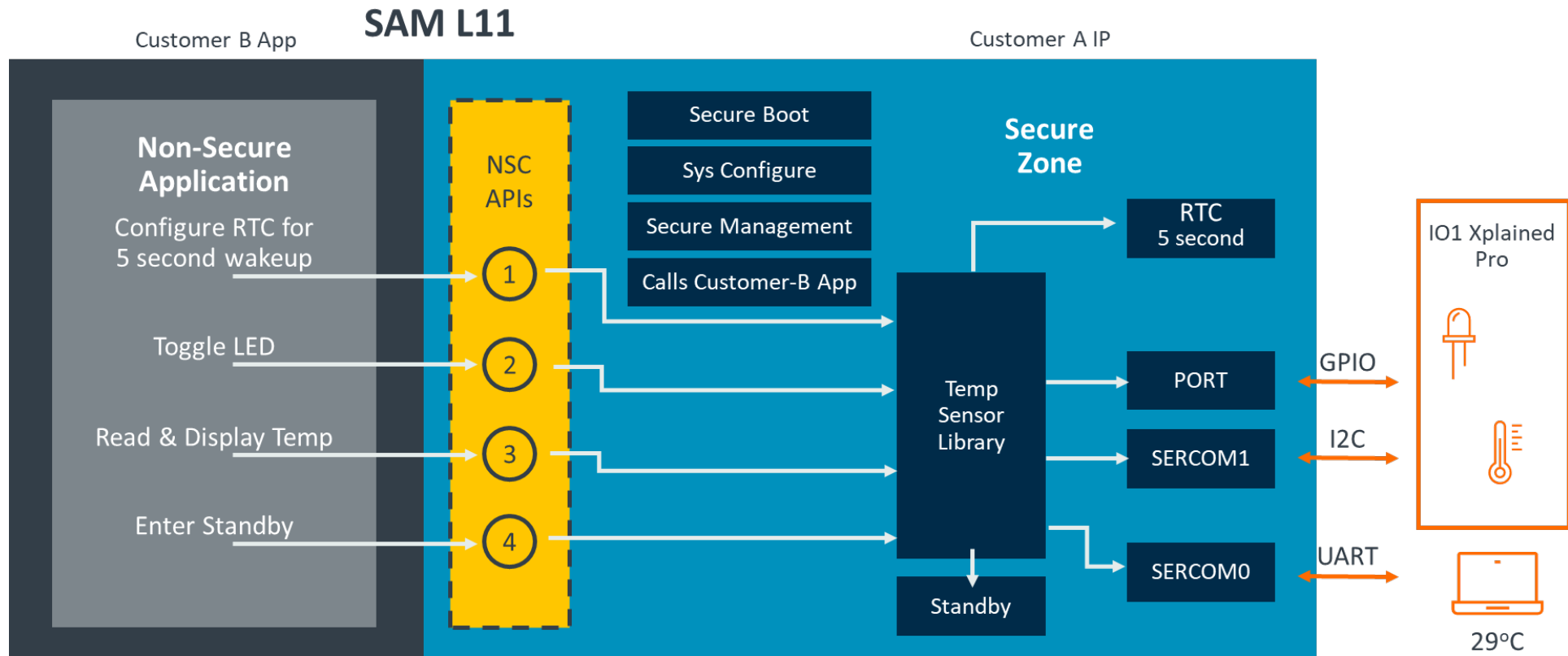
1. secure execution environment (SEE) isolated from rich execution environment
2. root-of-trust and trusted services isolation within SEE
3. Application isolation within SEE

Hardware-based Isolation within PSoC 64 Secure MCUs

Example MCUs – STM32H5

		 STM32H5 MCU Series 32-bit Arm® Cortex®- M33 (DSP + FPU) – 250 MHz 													
<ul style="list-style-type: none"> • ART Accelerator™ • USART, SPI, I²C • 16 and 32-bit timers • SHA, TRNG • DMA • DAC • Digital Temperature sensor • Low voltage 1.62 to 3.6V • V_{BAT} mode • Unique ID 	Product line	Dual bank Flash (KB)	RAM (KB)	Memory I/F	USB	12-bit ADC 5 Msps	1x Op-amp 1x Comp	CAN-FD	DCMI HDMI-CEC	Ethernet	Power Supply	TrustZone	AES/SAES PKA OTFDEC HUK ST-iRoT		
		STM32H5x3	563	1024 to 2048	640	2x SDMMC FMC 1x OctoSPI	USB FS USB UCPD	2	-	2	•	•	SMPS LDO	•	-
			573	2048	640	2x SDMMC FMC 1x OctoSPI	USB FS USB UCPD	2	-	2	•	•	SMPS LDO	•	•
		STM32H562		1024 to 2048	640	1x SDMMC FMC 1x OctoSPI	USB FS USB UCPD	2	-	1	•	-	LDO	•	-
		STM32H503		128	32	1x SDMMC	USB FS	1	•	1	-	-	LDO	-	-

Example MCUs – SAM L11



Do you use a secure MCU? (Put which one in the chat if you do)

- No
- Yes
- Currently evaluating
- Within the next 12 months

4

Going Further

Security and RTOS Resources

- [Jacob's RTOS Blogs](#)
- [Jacob's RTOS courses](#)
- [Jacob's Security Blogs](#)
- [TrustZone for Cortex-M](#)
- Embedded Bytes Newsletter
 - <http://bit.ly/1BAHYXm>

www.beningo.com

BENINGO
EMBEDDED GROUP



DesignNews

Thank You

Sponsored by



© 2022 Beningo Embedded Group, LLC. All Rights Reserved.