CEC Continuing Education Center

DesignNews

Secure MCUs and RTOSs

# DAY 3 : Arm TrustZone

Sponsored by

Digi-Key ELECTRONICS

BENINGO EMBEDDED GROUP

informa markets

# 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.beningo.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 TrustZone Introduction

# TrustZone Introduction

**Security extension for the Armv8-M architecture**

- Security architecture for deeply embedded processors
- Enables containerisation of software
- Simplifies security assessment of embedded devices.

**Conceptually similar and compatible with existing TrustZone technology**

- New architecture tailored for embedded devices
- Preserves low interrupt latencies of Cortex-M processors
- Provides high performance cross-domain calling.

# TrustZone Introduction

arm TRUSTZONE

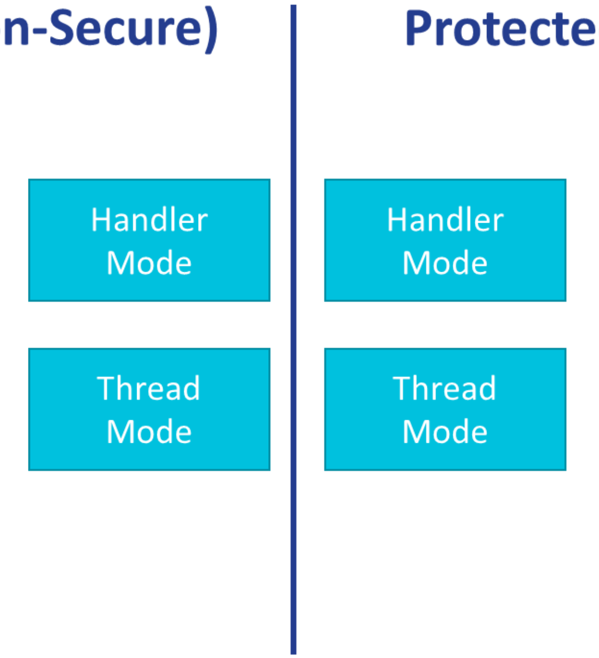
## Normal environment (Non-Secure)

Application Examples

- User applications
- RTOS
- Device drivers
- Protocol stacks

Normal Resources

- General peripherals



## Protected environment (Secure)

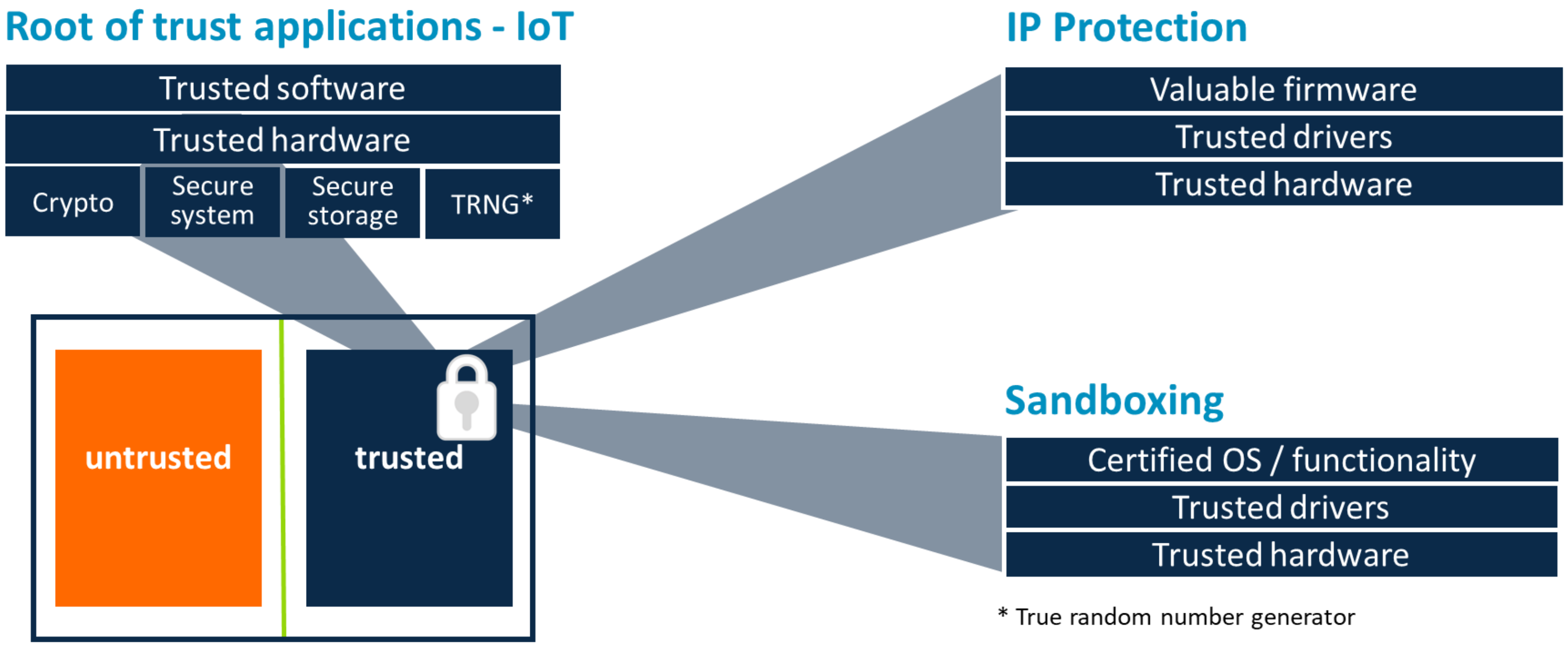
Secure Software Examples

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

Secure Resources

- Secure storage
- Crypto accelerators

# TrustZone Introduction



### Root of trust applications - IoT

- Trusted software
- Trusted hardware
- Crypto
- Secure system
- Secure storage
- TRNG*

untrusted

trusted

### IP Protection

- Valuable firmware
- Trusted drivers
- Trusted hardware

### Sandboxing

- Certified OS / functionality
- Trusted drivers
- Trusted hardware

* True random number generator

How much experience do you have working with TrustZone?

- None
- A few experiments
- Use it daily
- An expert

# 2 TrustZone MCUs

# TrustZone MCUs – Cortex-M23

### Smallest area, lowest power

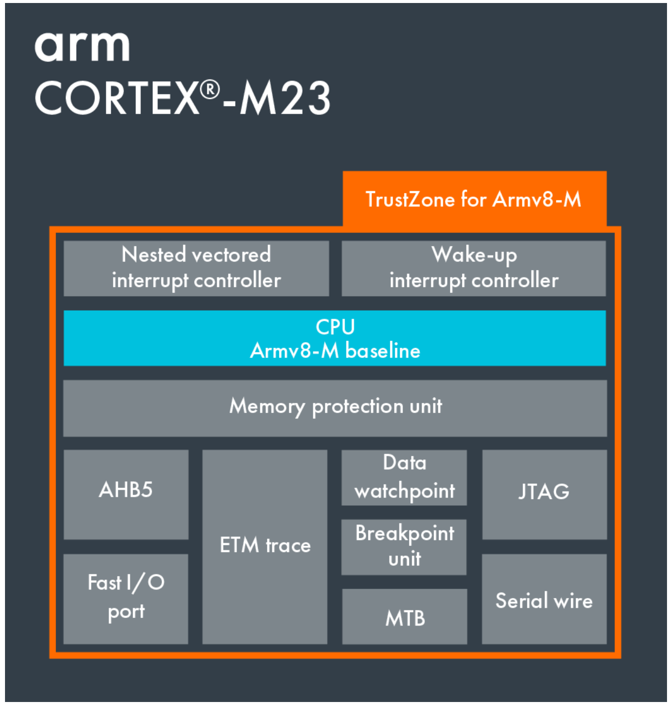
- With TrustZone, same energy efficiency as Cortex-M0+

### Ultra-high efficiency

- Flexible sleep modes
- Extensive clock gating
- Optional state retention

### Enhanced capability

- Increased performance
- Multi-core system support
- 240 interrupts
- Hardware stack checking



### Security foundation

- System wide security with TrustZone technology

### Enhanced memory protection

- Easy to program
- Dedicated protection for both secure and non-secure states

### Enhanced & secure debug

- Security aware debug
- Simplified firmware development
- Embedded trace macrocell

# TrustZone MCUs – Cortex-M33

### 32-bit processor of choice

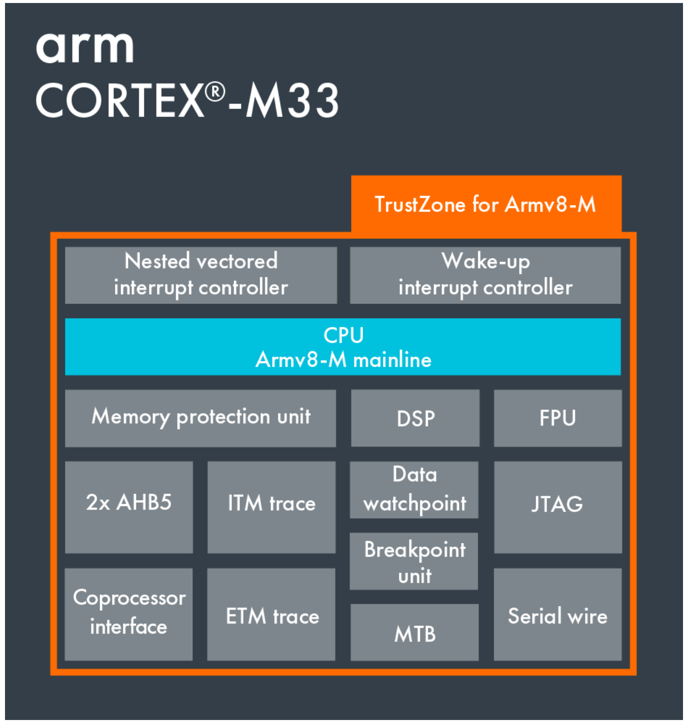
- Optimal balance between performance and power
- 20% greater performance than Cortex-M4
- With TrustZone, same energy efficiency as Cortex-M4

### Digital signal control

- Bring DSP to all developers
- FPU offering up to 10x performance over software

### Extensible compute

- Co-processor interface for tightly-coupled acceleration



### Security foundation

- System-wide security with TrustZone technology

### Enhanced memory protection

- Easy to program
- Dedicated protection for both secure and non-secure states

### Enhanced & secure debug

- Security aware debug
- Simplified firmware development

# TrustZone MCUs – Cortex-M55

### 32-bit processor of choice

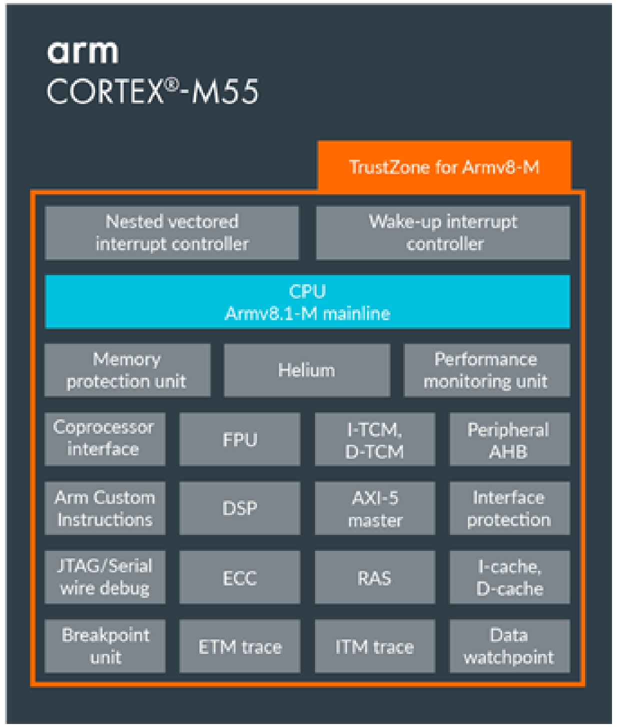
- Optimal balance between performance and power
- 20% greater performance than Cortex-M4
- With TrustZone, same energy efficiency as Cortex-M4

### Digital signal control

- Bring DSP to all developers
- FPU offering up to 10x performance over software
- Helium vector processing technology

### Extensible compute

- Co-processor interface for tightly-coupled acceleration



### Security foundation

- System-wide security with TrustZone technology

### Enhanced memory protection

- Easy to program
- Dedicated protection for both secure and non-secure states

### Enhanced & secure debug

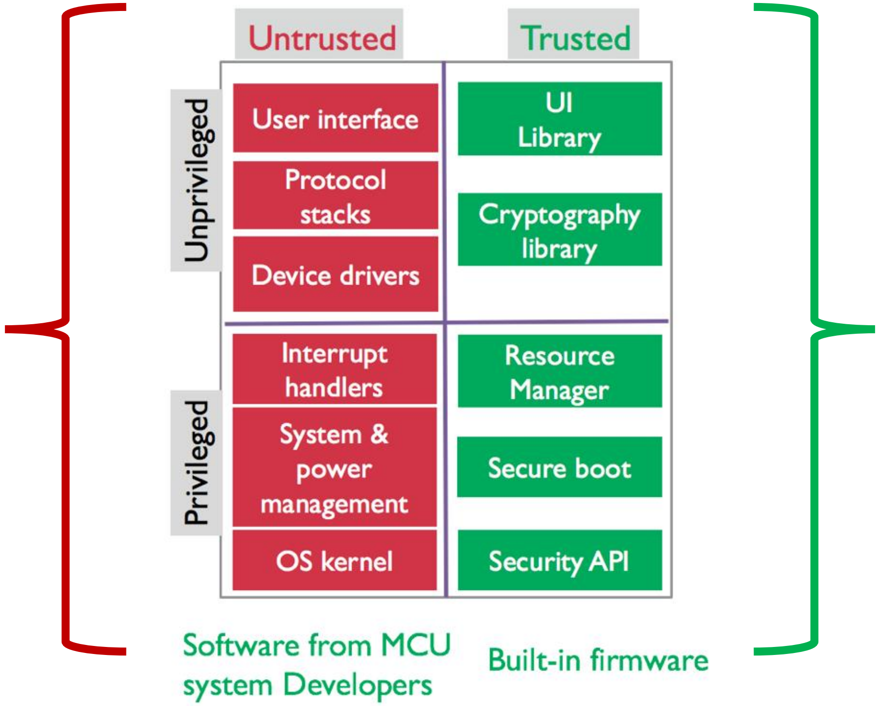
- Security aware debug
- Simplified firmware development

What typical MCU space do you select your parts from?
- Low-energy
- General computing
- High performance
- Digital signal processing
- Other

# 3 TrustZone Software

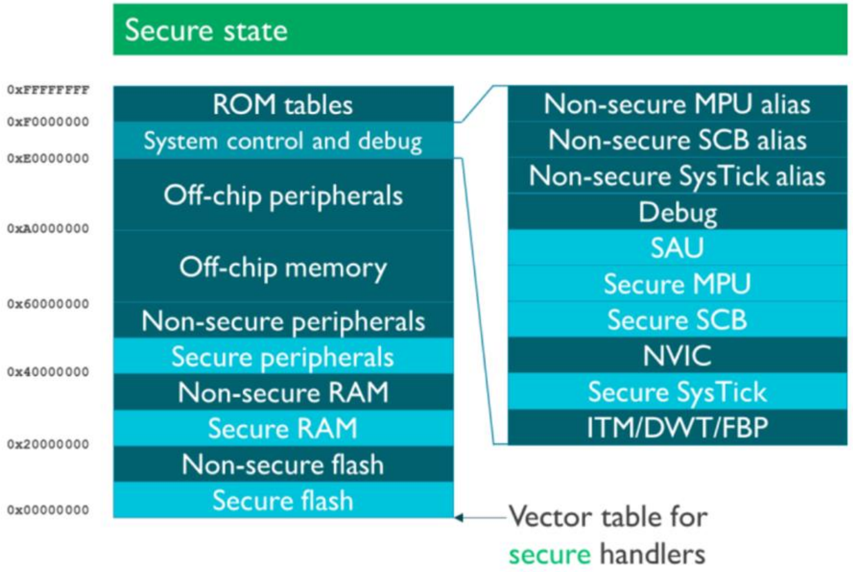
# TrustZone Software – Component Organization

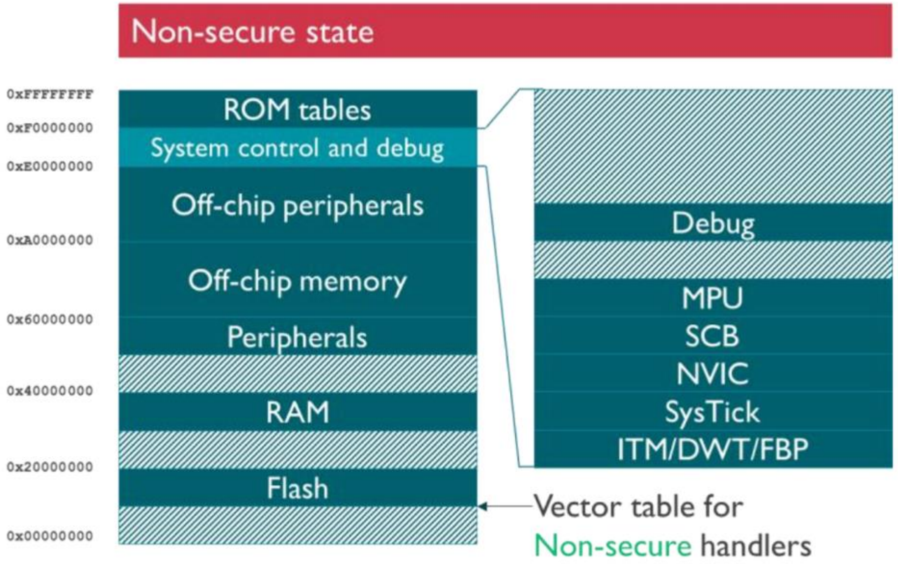
Traditional Developer Design



New additional security

# TrustZone Software – Programmers Model

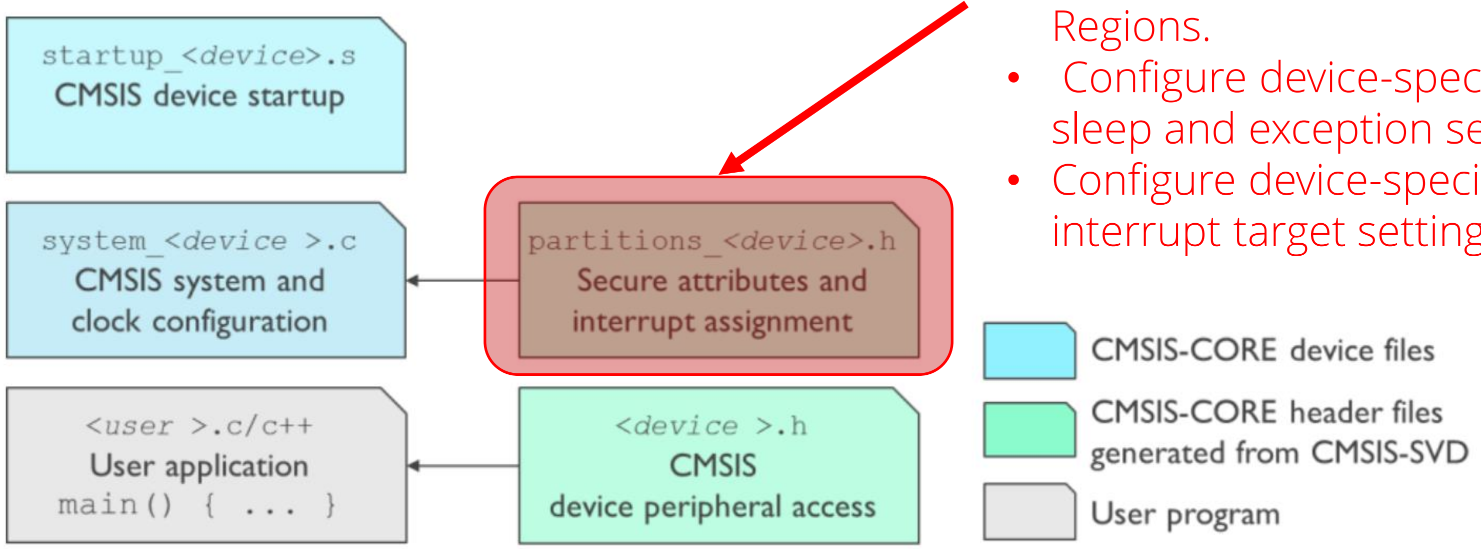




# TrustZone Software – Programmers Model

Initial setup of the non-secure memory map

- Provide settings for the SAU CTRL register.
- Configure the SAU Address Regions.
- Configure device-specific deep sleep and exception settings.
- Configure device-specific interrupt target settings.



startup_*<device>*.s
CMSIS device startup

system_*<device >*.c
CMSIS system and clock configuration

partitions_*<device>*.h
Secure attributes and interrupt assignment

*<user >*.c/c++
User application
main() { ... }

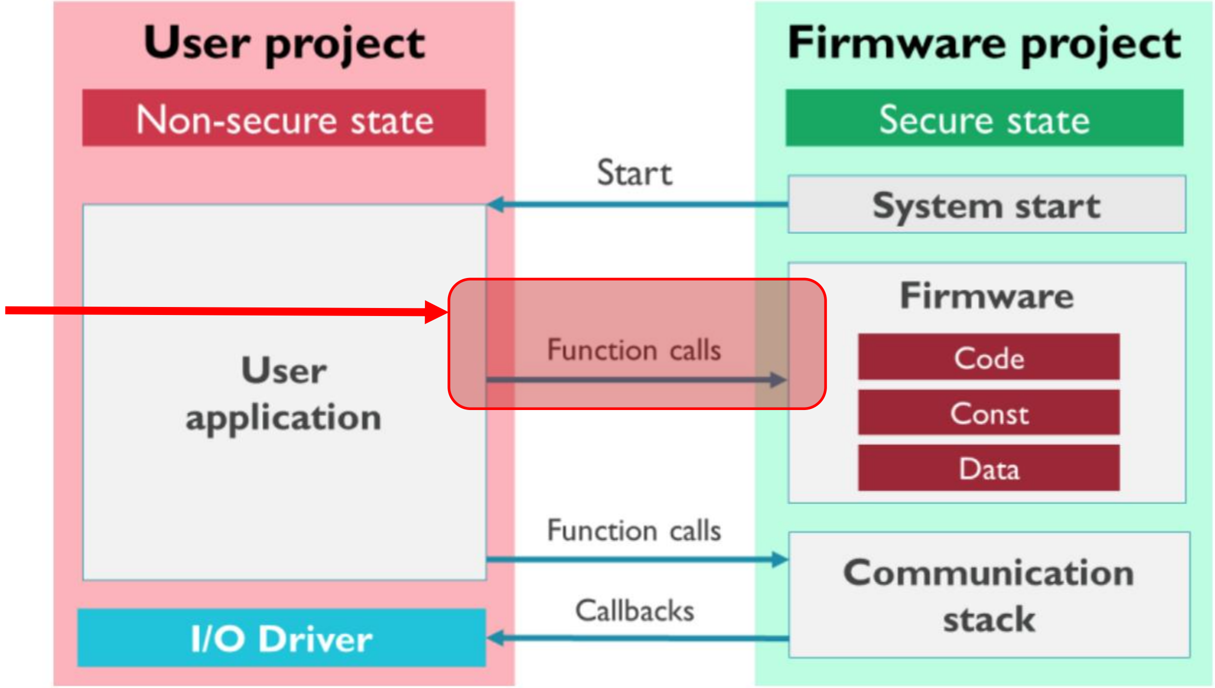
*<device >*.h
CMSIS
device peripheral access

- CMSIS-CORE device files
- CMSIS-CORE header files generated from CMSIS-SVD
- User program

# 4 Application Example

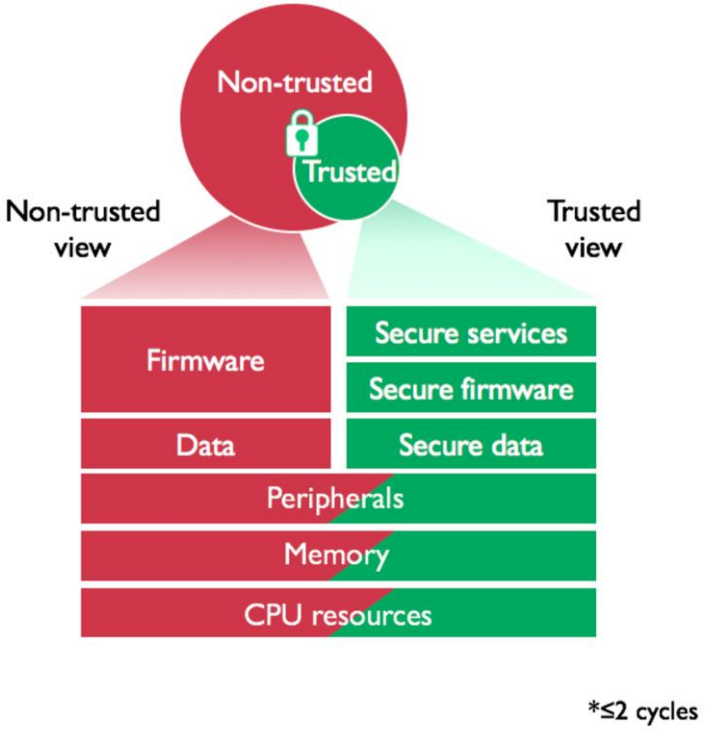
# Application Example

Function Calls Only!

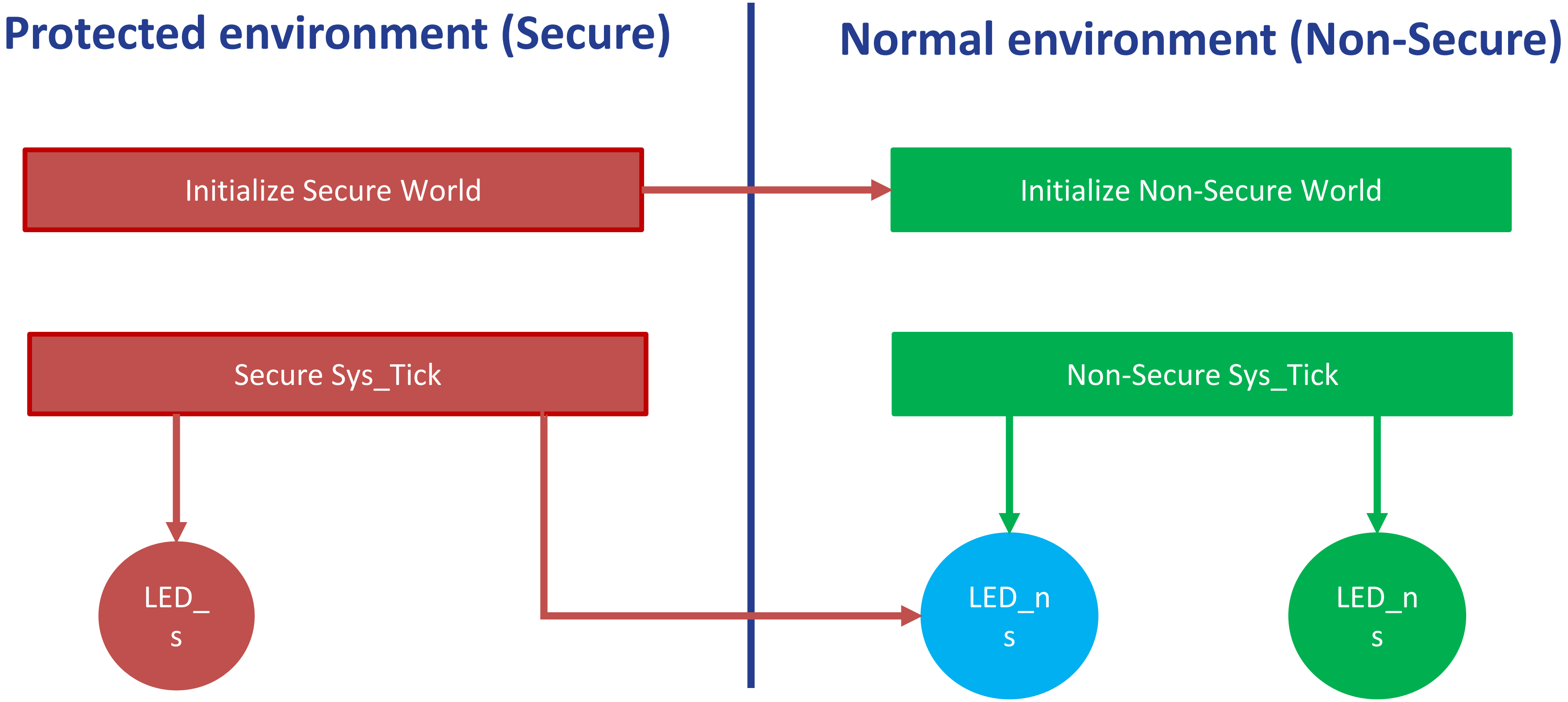


# Application Example – Real-Time Transition

- Hardware Isolation – No Software Required!
- CPU instruction automatically inserted
- Worst case overhead 2 clock cycles
- Deterministic response
- Extra overhead is application independent
  - Parameter, pointer testing
  - etc



# Application Example - LED



Protected environment (Secure)
Normal environment (Non-Secure)
Initialize Secure World
Initialize Non-Secure World
Secure Sys_Tick
Non-Secure Sys_Tick
LED_s
LED_ns
LED_ns

5

# 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

BENINGO
EMBEDDED GROUP

www.beningo.com

CEC Continuing Education Center

DesignNews

# Thank You

Sponsored by

Digi-Key Electronics

BENINGO EMBEDDED GROUP

informa markets