

# ARM Your Sensors



## Coding an ARMED and Secure IoT Sensor Node

August 29, 2018

Fred Eady

# ARM Your Sensors

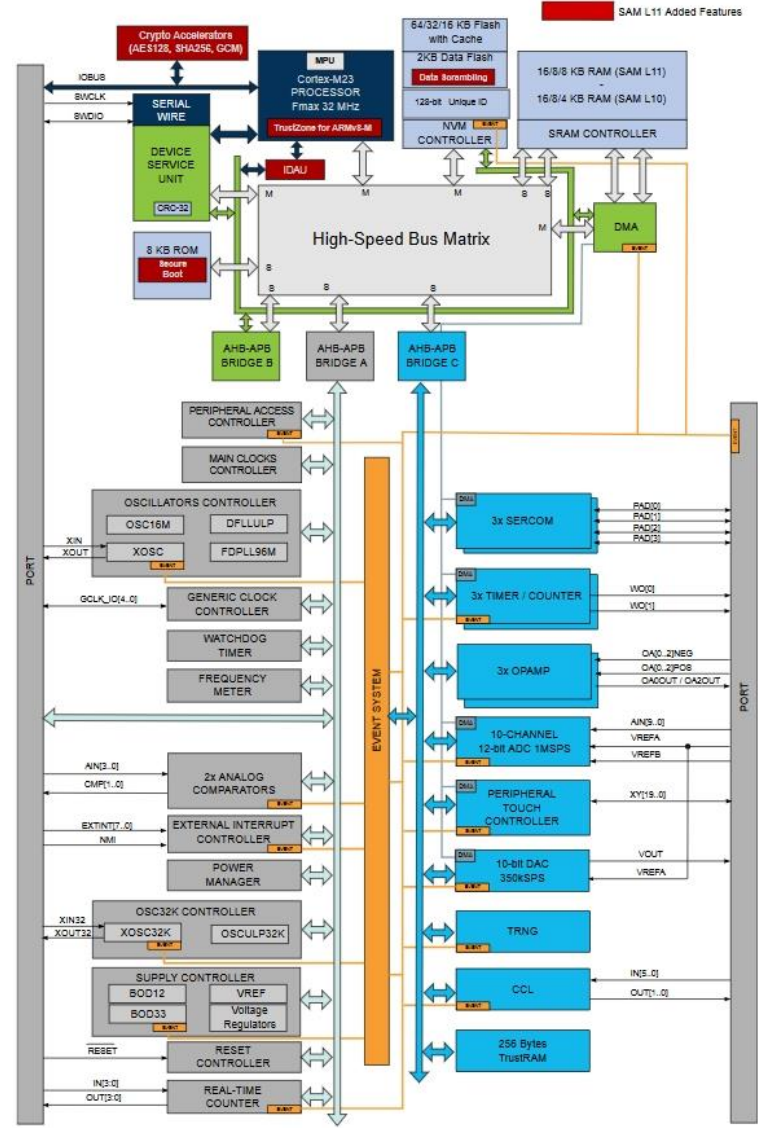
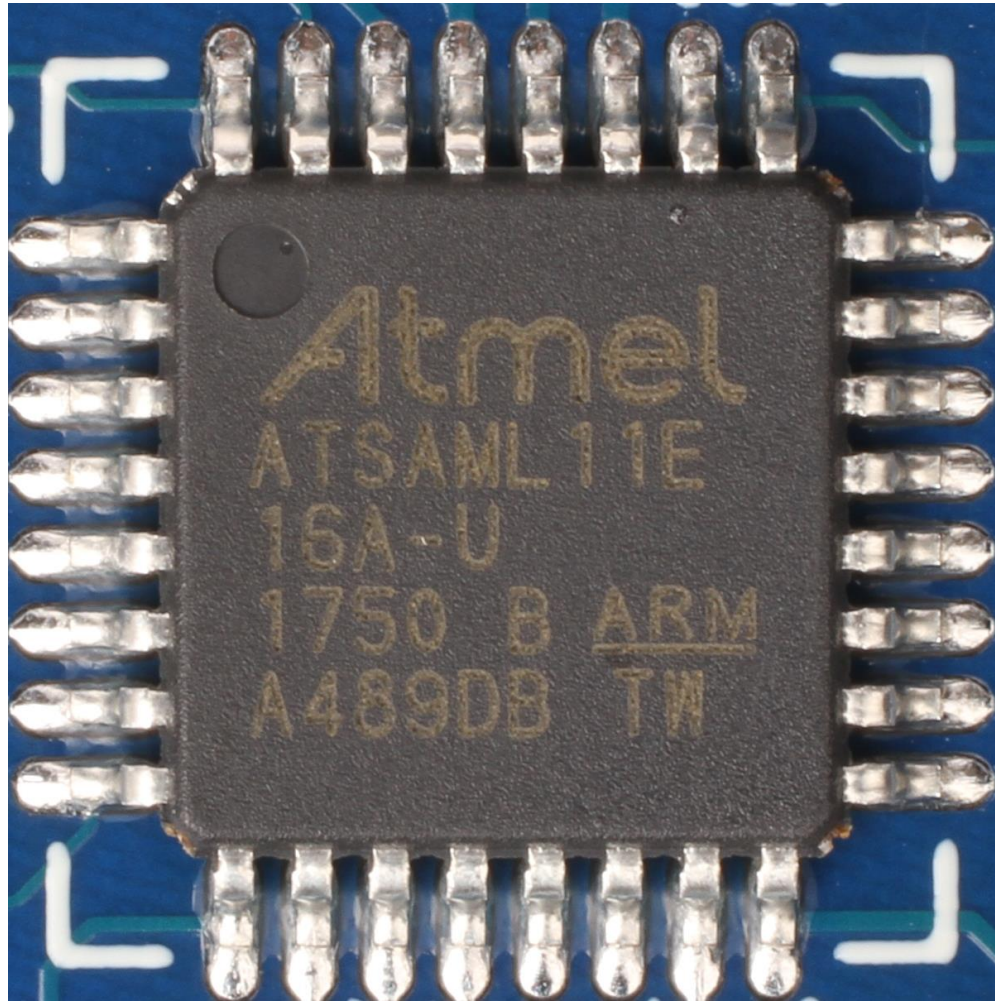
# AGENDA

- **SAM L11**
- **Secure IoT Application Fundamentals**
- **Day 3 Summary**



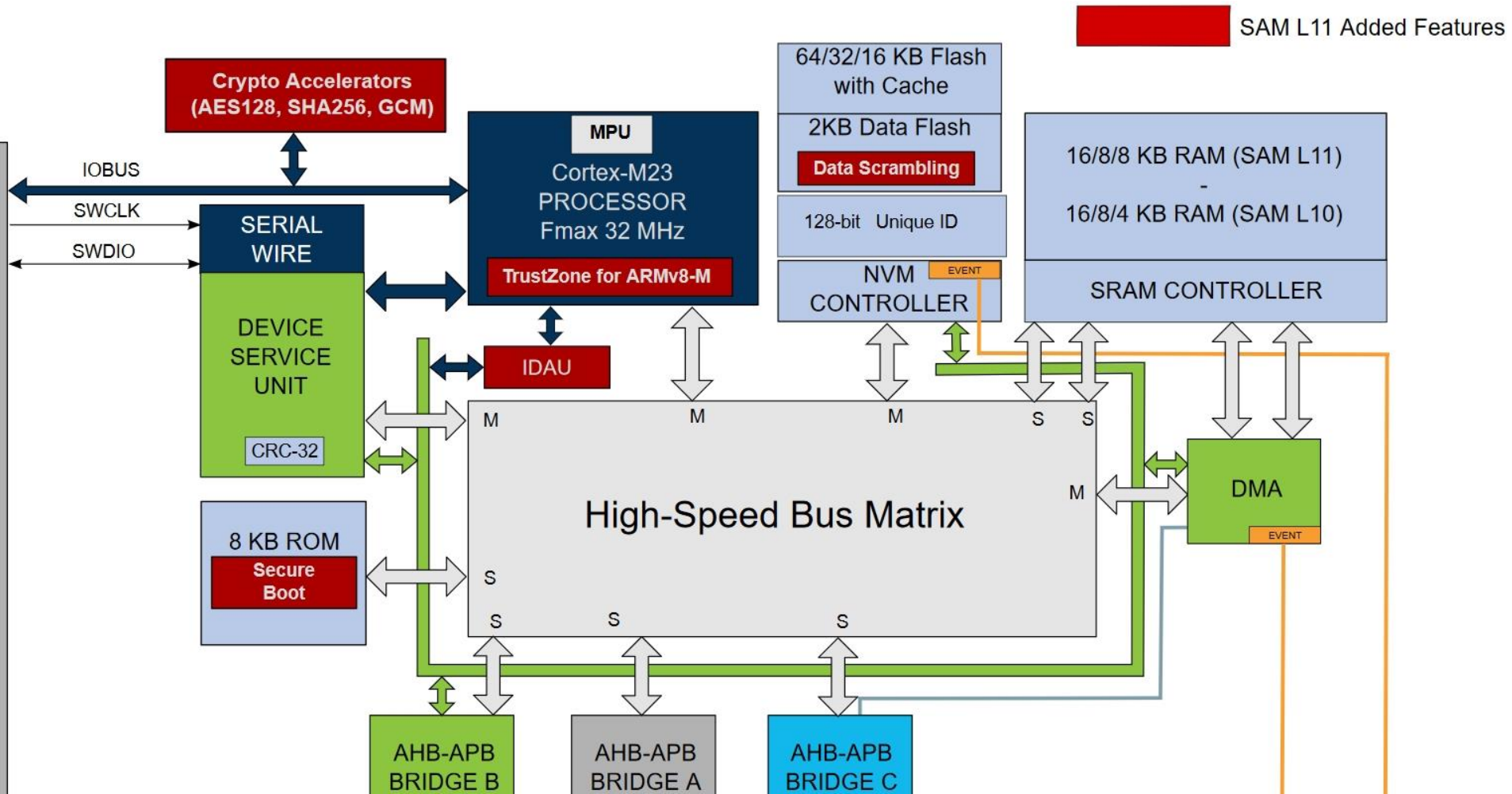
# ARM Your Sensors

## SAM L11



# ARM Your Sensors

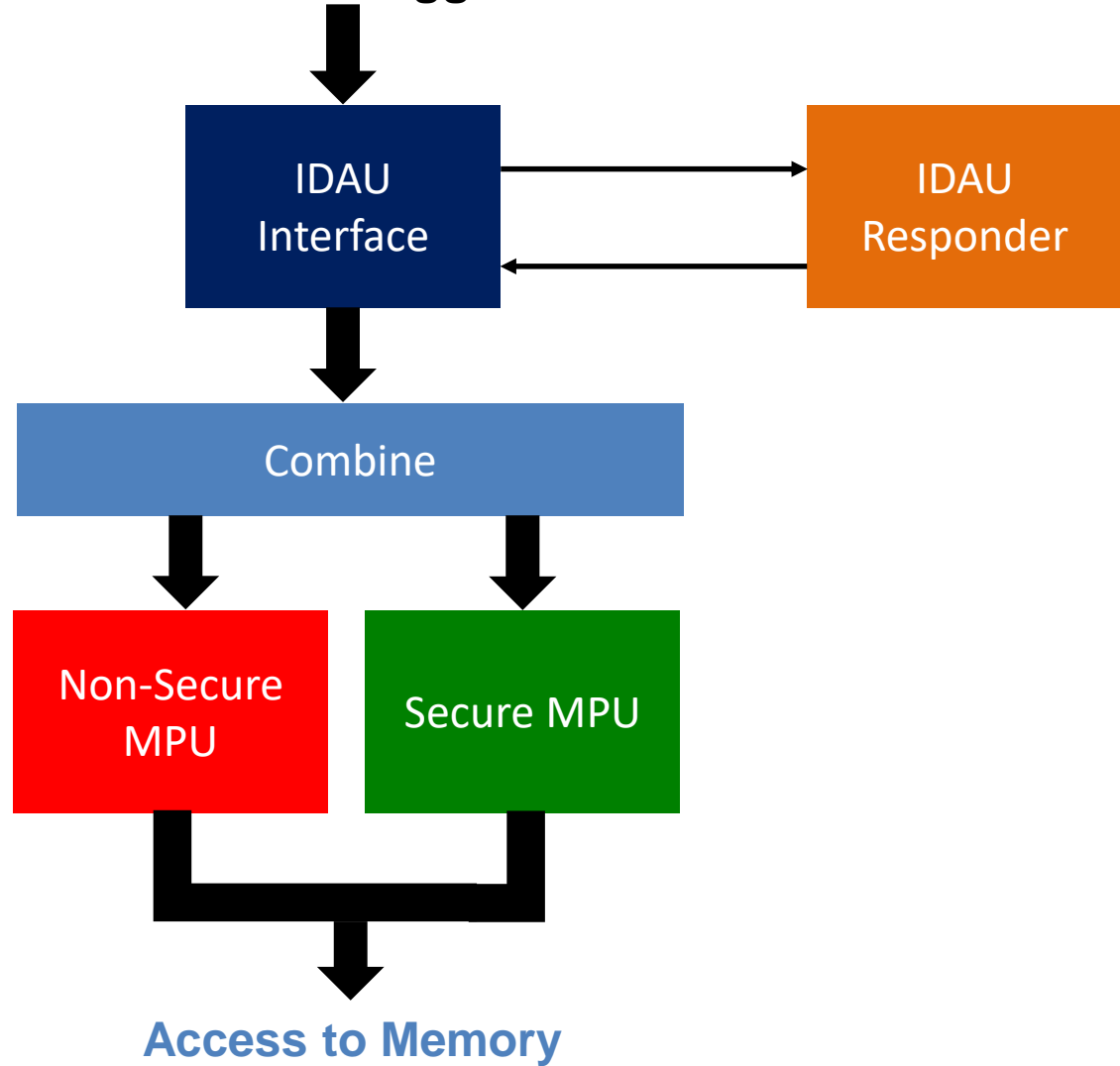
## SAM L11



# ARM Your Sensors

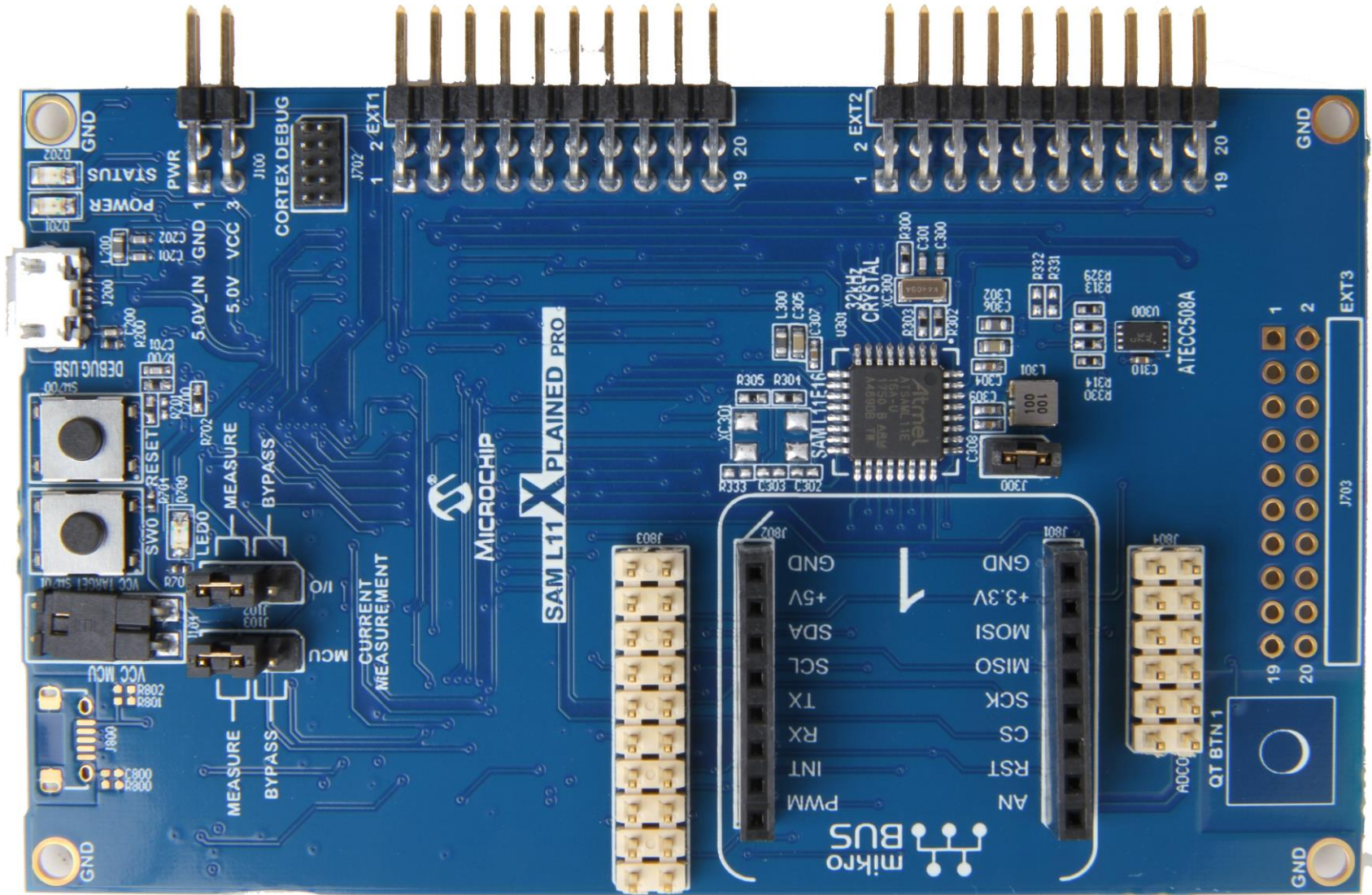
## SAM L11

Core/Debugger



# ARM Your Sensors

## SAM L11

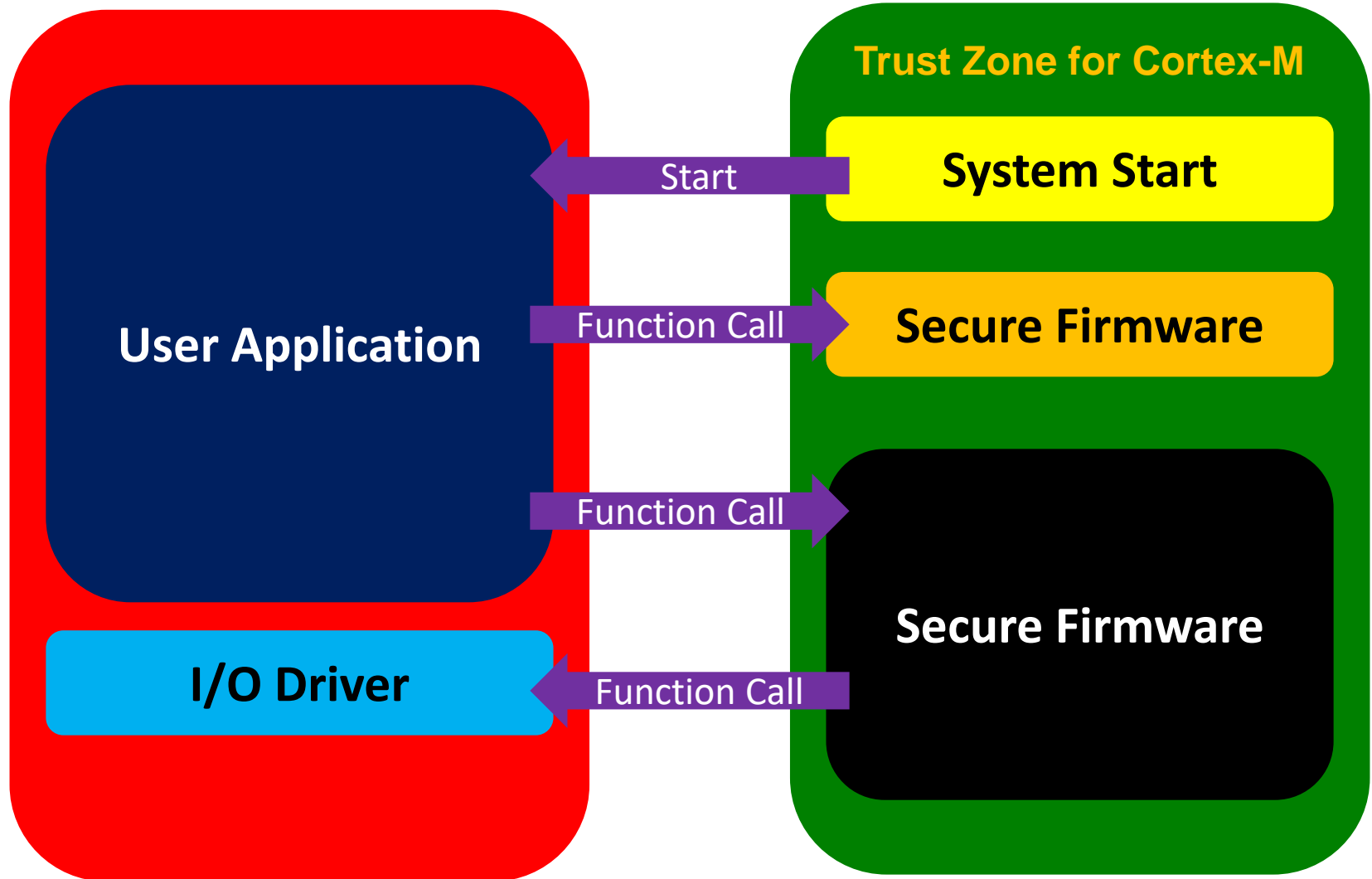


# ARM Your Sensors

## Secure IoT Application Fundamentals – TrustZone Implementation

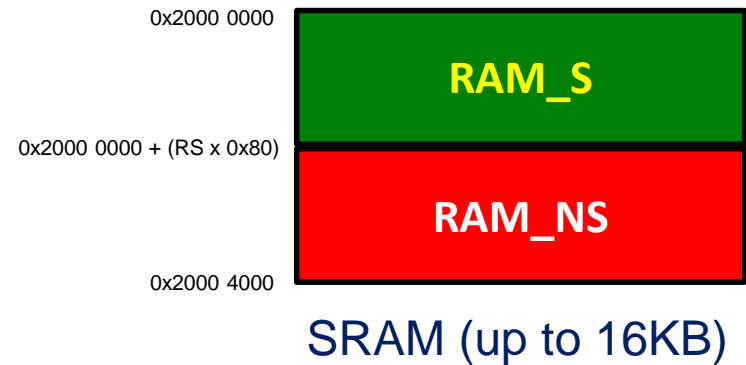
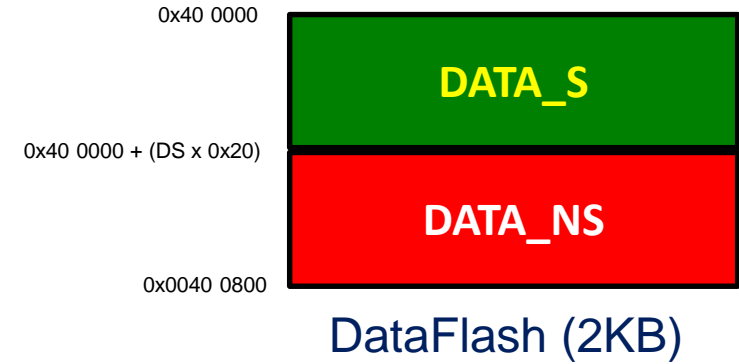
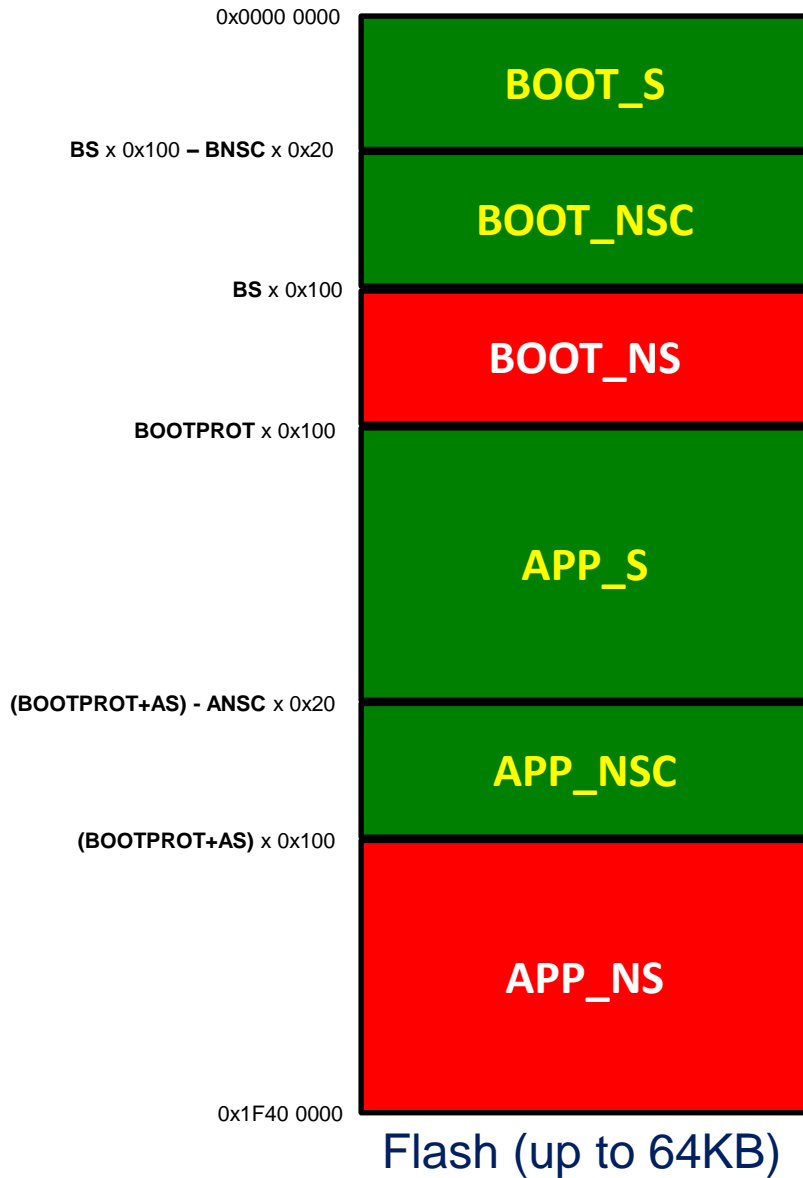
**Non-Secure State**

**Secure State**



# ARM Your Sensors

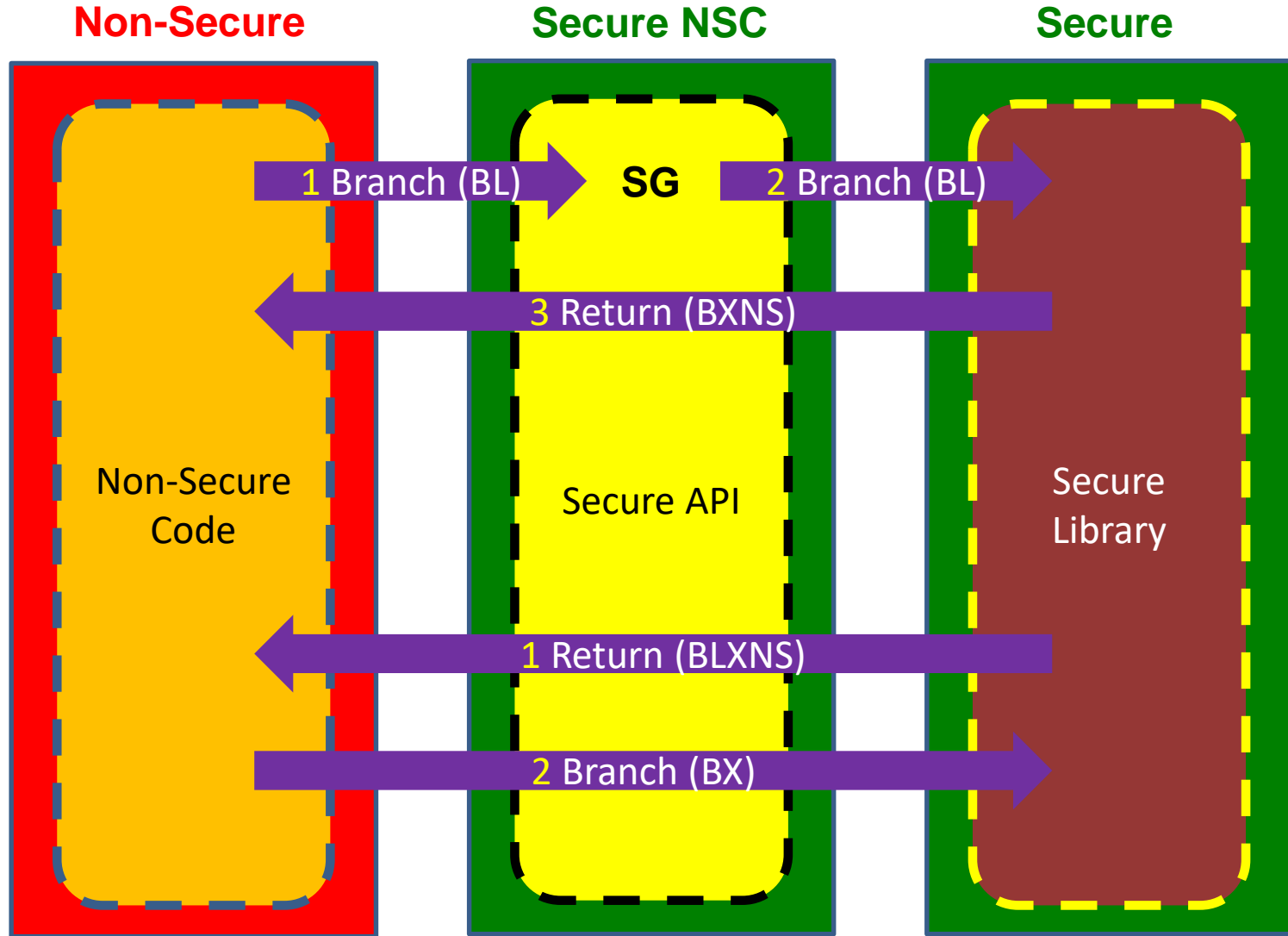
## Secure IoT Application Fundamentals – Memory Partitioning





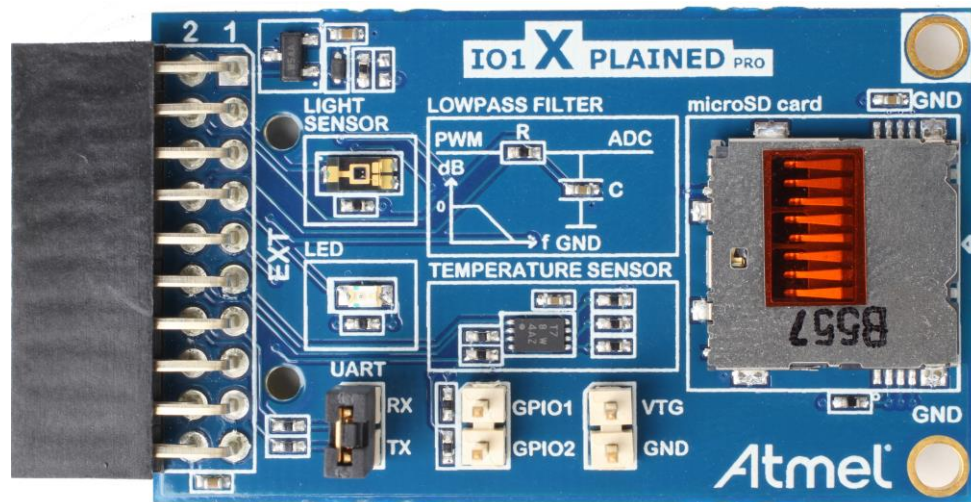
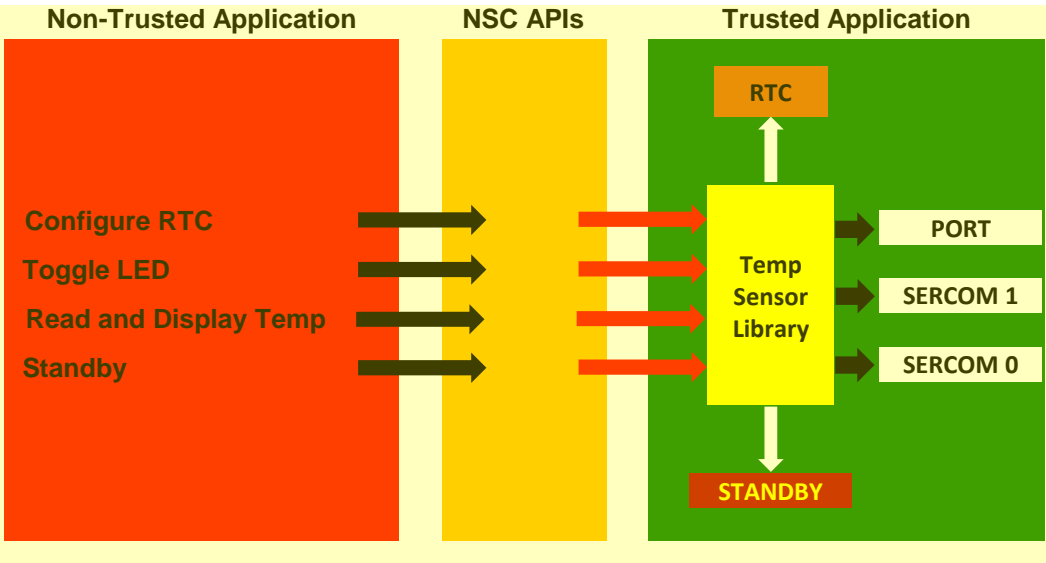
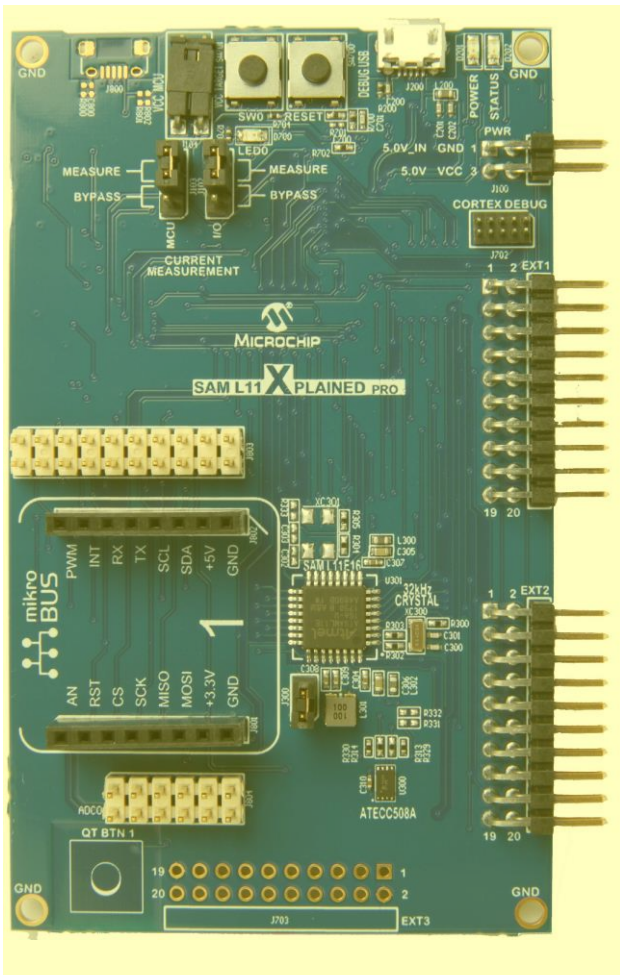
# ARM Your Sensors

## Secure IoT Application Fundamentals – Secure/Non-Secure Function Calls



# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation



# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation

```
VT COM4 - Tera Term VT
File Edit Setup Control Window Help

-----
Customer A - Trusted application
-----

      @@@@@@ @@@@@@ @ @ @ @@@@@@ @@@@@@ @@@@@@ @@@@@@
      @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
      @ @@@@@@ @ @ @ @@@@@ @ @ @@@@@ @ @ @
      @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @
      @ @ @ @ @ @@@@@ @@@@@ @ @@@@@ @@@@@

                @@@@@
                @@@@@@@@@@@@@@
                @@@@ @@@@@
                @@@ @@@@@
                @@@ @@@@@
                @@@ @@@@@
                @@@@@@@@@@@@@@
                @@@@@@@@@@@@@@
                @@@@@@@@@@@@@@
                @@@@@@@@@@@@@@.@@@@@
                @@@@@@@@@@@@@@.@@@@@
                @@@@@@.@@@.@@@@@
                @@@@@@@@..@@@@@
                @@@@@@@@@@@@@@
                @@@@@@@@@@@@@@

----- Trusted application options -----
0 - Print this menu
1 - Print resources secure allocation
2 - Fill TRAM with secrets
3 - Print TRAM content
4 - Fill DataFlash TEROW with secrets
5 - Print DataFlash TEROW content

----- Start Non-Trusted Application -----
S - Start Standard Customer B application
M - Start Malware Customer B application

-----
Choice :
```



# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation

```
VT COM4 - Tera Term VT
File Edit Setup Control Window Help
1 - Print resources secure allocation
2 - Fill TRAM with secrets
3 - Print TRAM content
4 - Fill DataFlash TEROW with secrets
5 - Print DataFlash TEROW content

----- Start Non-Trusted Application -----
S - Start Standard Customer B application
M - Start Malware Customer B application

-----
Choice :
Fill TRAM with secret (0xCAFECAFE) :

0x42003500 : cafecafe cafecafe
0x42003508 : cafecafe cafecafe
0x42003510 : cafecafe cafecafe
0x42003518 : cafecafe cafecafe
0x42003520 : cafecafe cafecafe
0x42003528 : cafecafe cafecafe
0x42003530 : cafecafe cafecafe
0x42003538 : cafecafe cafecafe
0x42003540 : cafecafe cafecafe
0x42003548 : cafecafe cafecafe
0x42003550 : cafecafe cafecafe
0x42003558 : cafecafe cafecafe
0x42003560 : cafecafe cafecafe
0x42003568 : cafecafe cafecafe
0x42003570 : cafecafe cafecafe
0x42003578 : cafecafe cafecafe
0x42003580 : cafecafe cafecafe
0x42003588 : cafecafe cafecafe
0x42003590 : cafecafe cafecafe
0x42003598 : cafecafe cafecafe
0x420035a0 : cafecafe cafecafe
0x420035a8 : cafecafe cafecafe
0x420035b0 : cafecafe cafecafe
0x420035b8 : cafecafe cafecafe
0x420035c0 : cafecafe cafecafe
0x420035c8 : cafecafe cafecafe
0x420035d0 : cafecafe cafecafe
0x420035d8 : cafecafe cafecafe
0x420035e0 : cafecafe cafecafe
0x420035e8 : cafecafe cafecafe
0x420035f0 : cafecafe cafecafe
0x420035f8 : cafecafe cafecafe
```

Presented by:



# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation

```
COM4 - Tera Term VT
File Edit Setup Control Window Help
- Switch-off secure LED
->nsc_set_secure_led_off(); ->secure_led_off()
- Enter Standby mode
->nsc_secure_enter_sleep_mode(); ->secure_enter_sleep_mode()

- RTC Wake-up
- Switch-on secure LED
->nsc_set_secure_led_on(); ->secure_led_on()
- Read secure temperature sensor
->nsc_temperature_sensor_read(); ->temperature_sensor_read(AT30TSE75X)-> 24 Deg C
- Switch-off secure LED
->nsc_set_secure_led_off(); ->secure_led_off()
- Enter Standby mode
->nsc_secure_enter_sleep_mode(); ->secure_enter_sleep_mode()

- RTC Wake-up
- Switch-on secure LED
->nsc_set_secure_led_on(); ->secure_led_on()
- Read secure temperature sensor
->nsc_temperature_sensor_read(); ->temperature_sensor_read(AT30TSE75X)-> 24 Deg C
- Switch-off secure LED
->nsc_set_secure_led_off(); ->secure_led_off()
- Enter Standby mode
->nsc_secure_enter_sleep_mode(); ->secure_enter_sleep_mode()

- RTC Wake-up
- Switch-on secure LED
->nsc_set_secure_led_on(); ->secure_led_on()
- Read secure temperature sensor
->nsc_temperature_sensor_read(); ->temperature_sensor_read(AT30TSE75X)-> 24 Deg C
- Switch-off secure LED
->nsc_set_secure_led_off(); ->secure_led_off()
- Enter Standby mode
->nsc_secure_enter_sleep_mode(); ->secure_enter_sleep_mode()

- RTC Wake-up
- Switch-on secure LED
->nsc_set_secure_led_on(); ->secure_led_on()
- Read secure temperature sensor
->nsc_temperature_sensor_read(); ->temperature_sensor_read(AT30TSE75X)-> 24 Deg C
- Switch-off secure LED
->nsc_set_secure_led_off(); ->secure_led_off()
- Enter Standby mode
->nsc_secure_enter_sleep_mode(); ->secure_enter_sleep_mode()
```



# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation

```
COM4 - Tera Term VT
File Edit Setup Control Window Help

Customer B - Non-Trusted application - Malware

# : Secure code execution (Trusted)
# : Non-Secure-Callable code execution
# : Non-Secure code execution (Non-Trusted)

Malware Application options

0 - Print this menu
1 - Malicious - Jump to Secure Function
2 - Malicious - Dump secure Flash area
3 - Malicious - Dump secure DataFlash area
4 - Malicious - Dump secure RAM area
5 - Malicious - Dump TrustRAM Memory
6 - Malicious - Disable RTC/TAMPER
7 - Malicious - Drive secure LED
8 - Malicious - Drive secure SERCOM1

Choice :
```





# ARM Your Sensors

## Secure IoT Application Fundamentals – A Simple Implementation

```
COM4 - Tera Term VT
File Edit Setup Control Window Help

    000      000
    000      000
    000000000000000000000000
    000000000000000000000000
    000000000000000000000000
    000000000000..0000
    000000..000..00000000
    0000000..000000000
    000000000000000000000000
    000000000000000000000000

----- Trusted application options -----
0 - Print this menu
1 - Print resources secure allocation
2 - Fill TRAM with secrets
3 - Print TRAM content
4 - Fill DataFlash TEROW with secrets
5 - Print DataFlash TEROW content

----- Start Non-Trusted Application -----
S - Start Standard Customer B application
M - Start Malware Customer B application

-----
Choice :
Current TRAM content :

0x42003500 : 00000000 00000000
0x42003508 : 00000000 00000000
0x42003510 : 00000000 00000000
0x42003518 : 00000000 00000000
0x42003520 : 00000000 00000000
0x42003528 : 00000000 00000000
0x42003530 : 00000000 00000000
0x42003538 : 00000000 00000000
0x42003540 : 00000000 00000000
0x42003548 : 00000000 00000000
0x42003550 : 00000000 00000000
0x42003558 : 00000000 00000000
0x42003560 : 00000000 00000000
0x42003568 : 00000000 00000000
0x42003570 : 00000000 00000000
0x42003578 : 00000000 00000000
0x42003580 : 00000000 00000000
0x42003588 : 00000000 00000000
0x42003590 : 00000000 00000000
0x42003598 : 00000000 00000000
0x420035a0 : 00000000 00000000
0x420035a8 : 00000000 00000000
0x420035b0 : 00000000 00000000
0x420035b8 : 00000000 00000000
0x420035c0 : 00000000 00000000
0x420035c8 : 00000000 00000000
0x420035d0 : 00000000 00000000
0x420035d8 : 00000000 00000000
0x420035e0 : 00000000 00000000
0x420035e8 : 00000000 00000000
0x420035f0 : 00000000 00000000
0x420035f8 : 00000000 00000000
```





# ARM Your Sensors

## Day 3 Summary

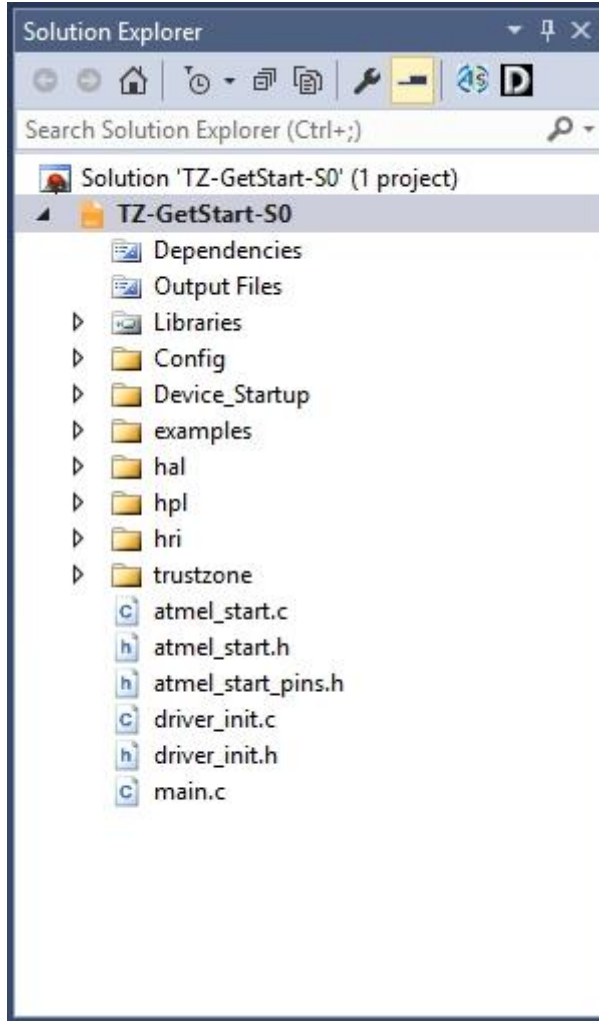
```

COM4 - Tera Term VT
File Edit Setup Control Window Help

Customer B - Trusted application

.....
Trusted application options
.....
0 - Print this menu
1 - Print resources secure allocation
2 - Fill TRAM with secrets
3 - Print TRAM content
4 - Fill DataFlash TRAM with secrets
5 - Print DataFlash TRAM content
.....
Start Non-Trusted Application
.....
0 - Start Standard Customer B application
1 - Start Malware Customer B application

Choice :
    
```



```

COM4 - Tera Term VT
File Edit Setup Control Window Help

Customer B - Non-Trusted application - Malware

.....
Non-Trusted application options
.....
0 - Print this menu
1 - Malicious - Dump to Secure Function
2 - Malicious - Dump secure Flash area
3 - Malicious - Dump secure DataFlash area
4 - Malicious - Dump secure DRAM area
5 - Malicious - Dump TrustZone Memory
6 - Malicious - Disable TRAM
7 - Malicious - Drive secure LED
8 - Malicious - Drive secure SERCOM

Choice :
    
```

