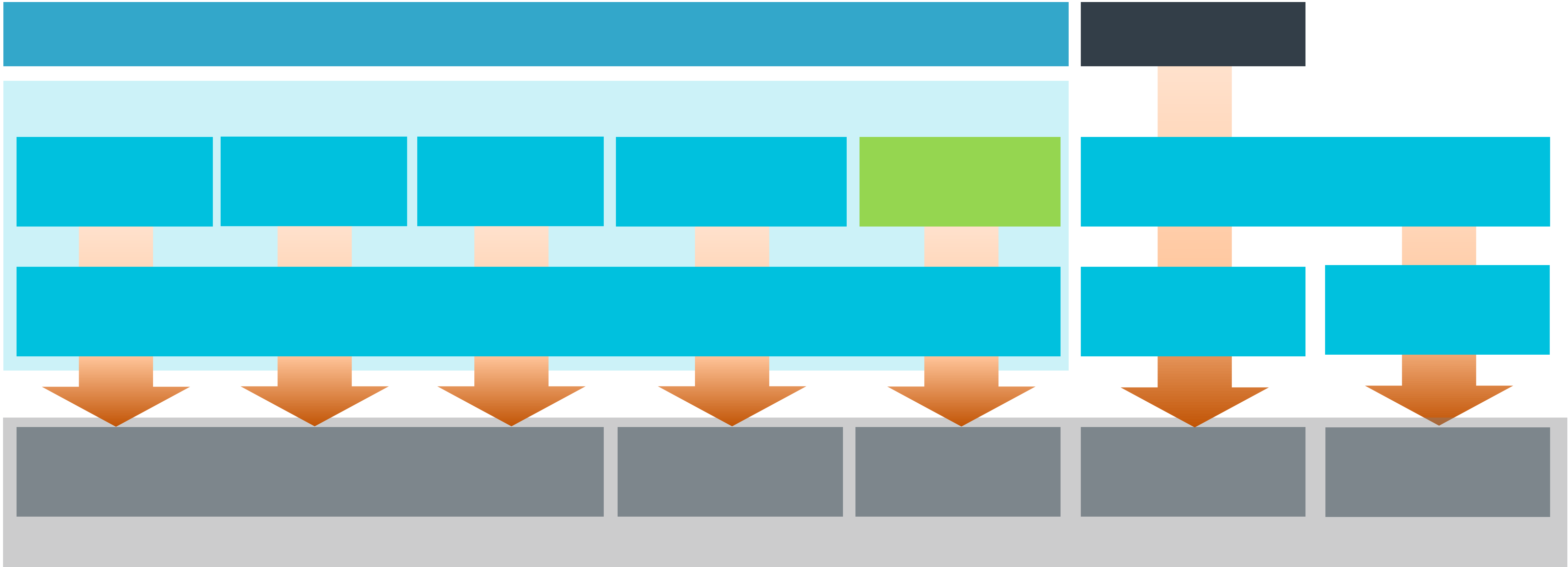
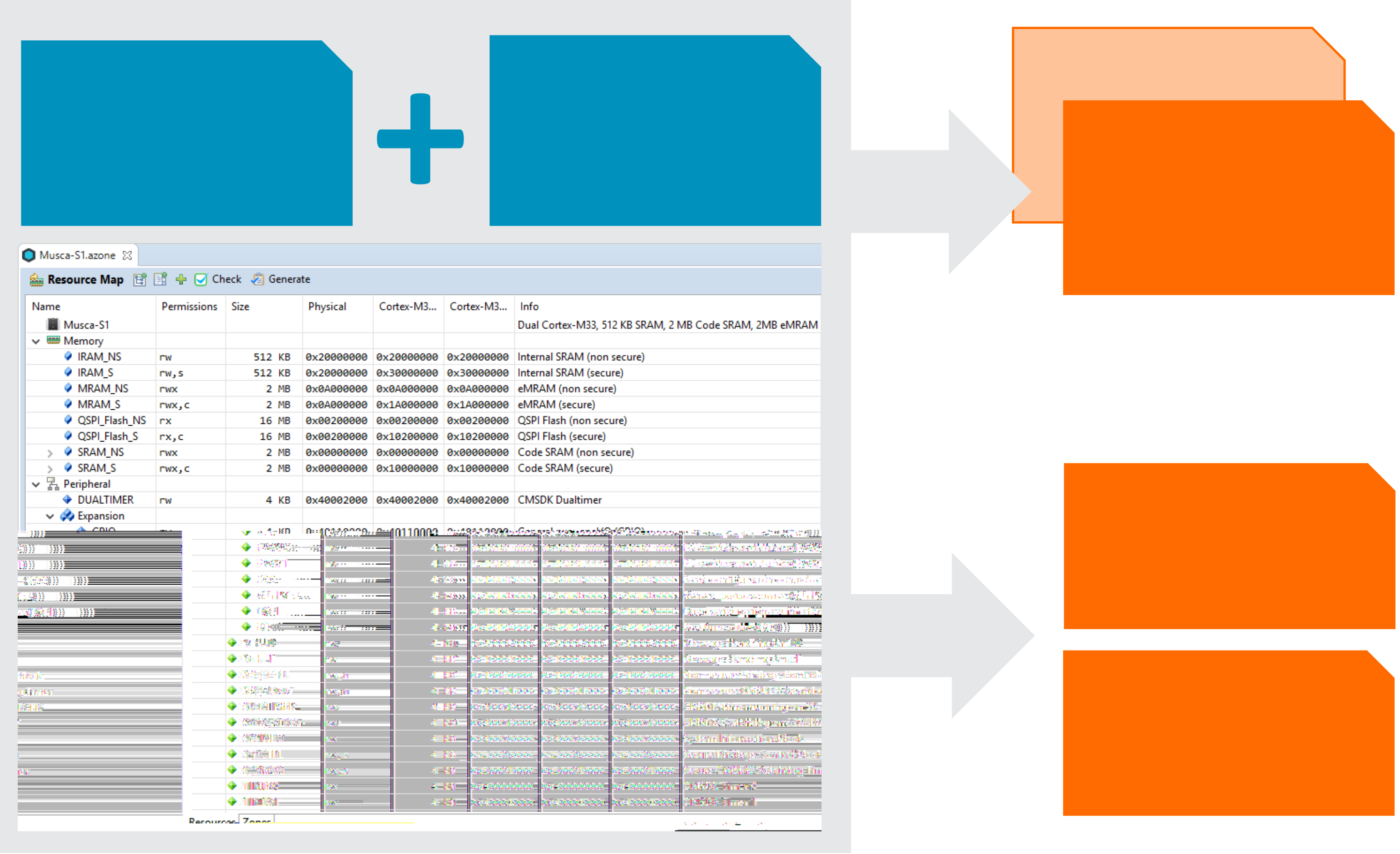
arm

CMSIS

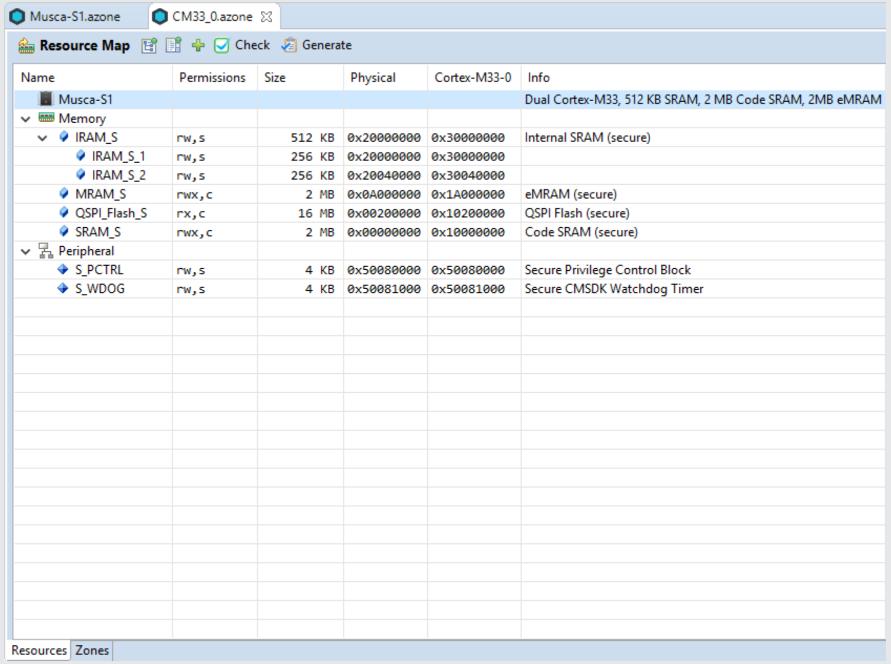
Review meeting at embedded world 2020



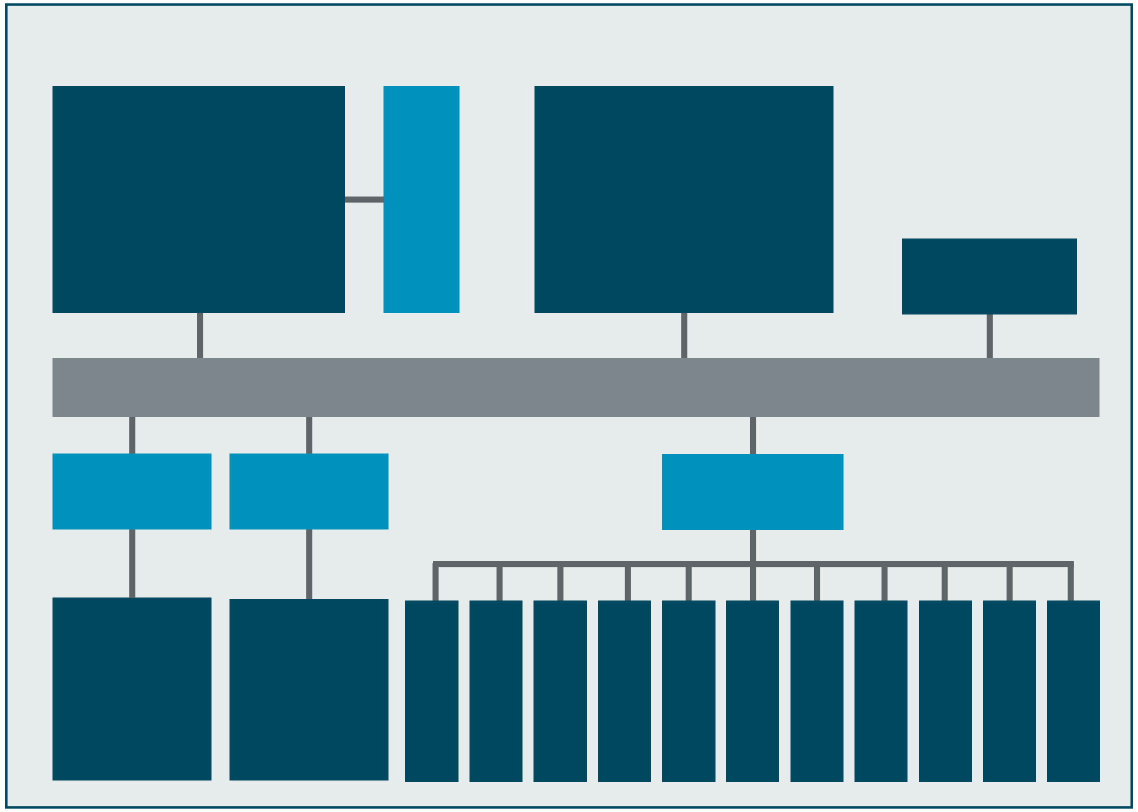
Configure multi-core, TrustZone and MPU

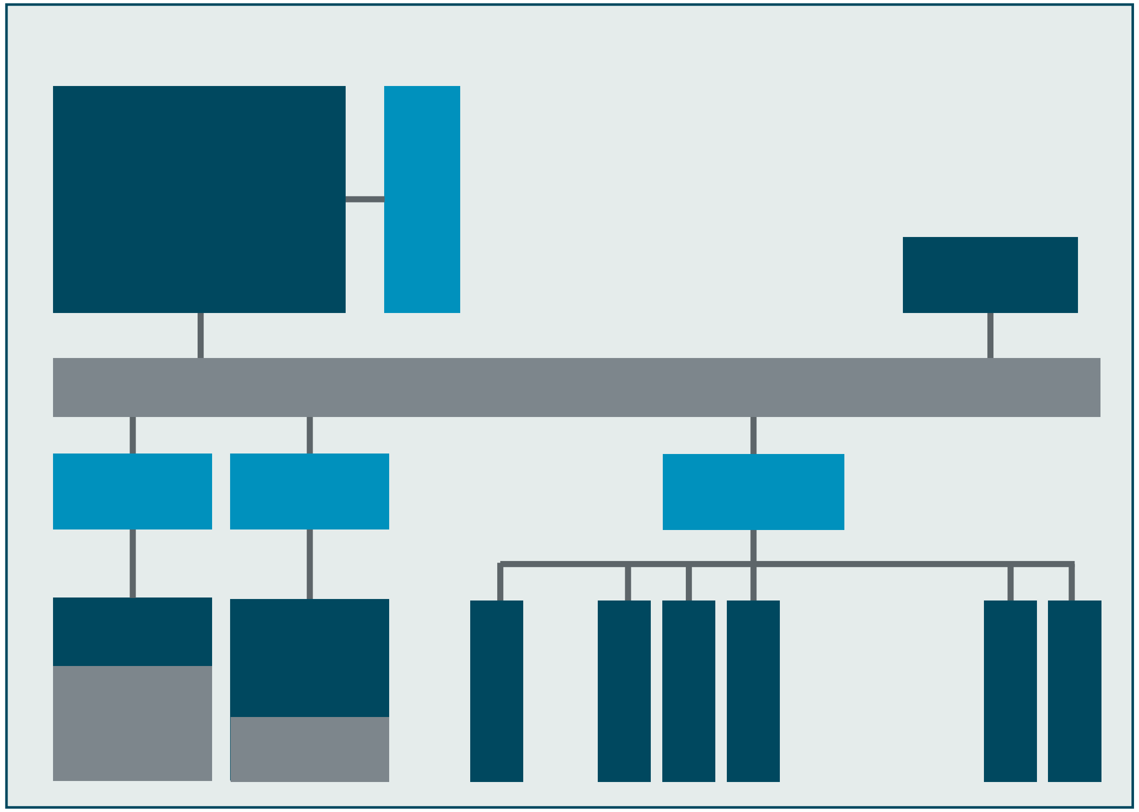


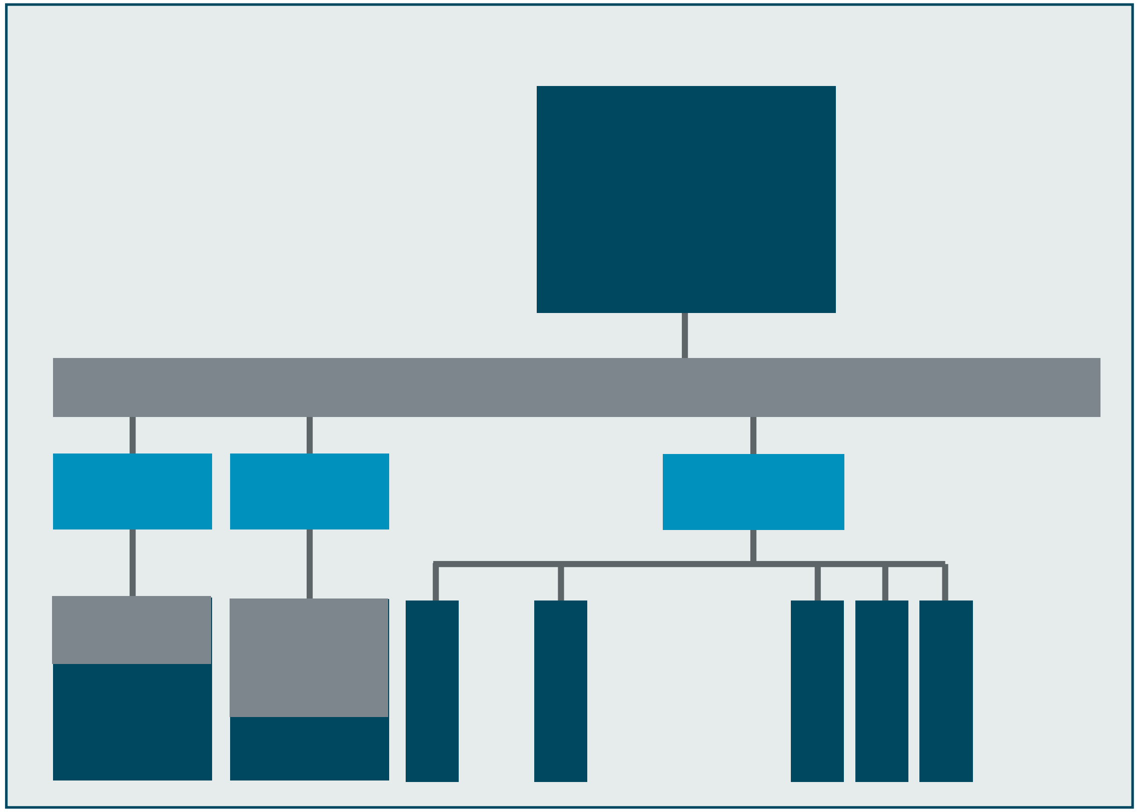
Name	Permissions	Size	Physical	Cortex-M3...	Cortex-M3...	Info
Musca-S1						Dual Cortex-M33, 512 KB SRAM, 2 MB Code SRAM, 2MB eMRAM
Memory						
IRAM_NS	rw	512 KB	0x20000000	0x20000000	0x20000000	Internal SRAM (non secure)
IRAM_S	rw,s	512 KB	0x20000000	0x30000000	0x30000000	Internal SRAM (secure)
MRAM_NS	rwx	2 MB	0x0A000000	0x0A000000	0x0A000000	eMRAM (non secure)
MRAM_S	rwx,c	2 MB	0x0A000000	0x1A000000	0x1A000000	eMRAM (secure)
QSPI_Flash_NS	rx	16 MB	0x00200000	0x00200000	0x00200000	QSPI Flash (non secure)
QSPI_Flash_S	rx,c	16 MB	0x00200000	0x10200000	0x10200000	QSPI Flash (secure)
SRAM_NS	rwx	2 MB	0x00000000	0x00000000	0x00000000	Code SRAM (non secure)
SRAM_S	rwx,c	2 MB	0x00000000	0x10000000	0x10000000	Code SRAM (secure)
Peripheral						
DUALTIMER	rw	4 KB	0x40002000	0x40002000	0x40002000	CMSDK Dualtimer
Expansion						



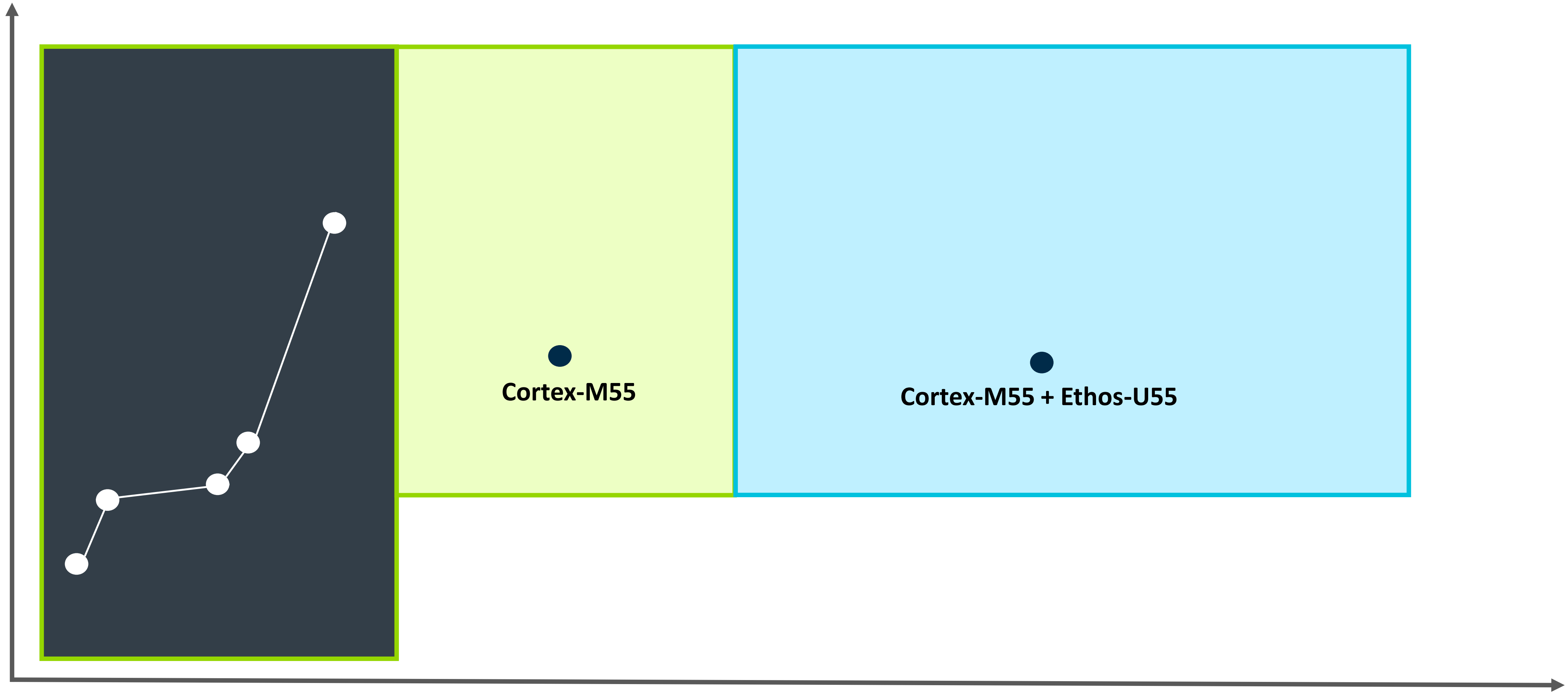
Name	Permissions	Size	Physical	Cortex-M33-0	Info
Musca-S1					Dual Cortex-M33, 512 KB SRAM, 2 MB Code SRAM, 2MB eMRAM
Memory					
IRAM_S	rw,s	512 KB	0x20000000	0x30000000	Internal SRAM (secure)
IRAM_S_1	rw,s	256 KB	0x20000000	0x30000000	
IRAM_S_2	rw,s	256 KB	0x20040000	0x30040000	
MRAM_S	rwx,c	2 MB	0x0A000000	0x1A000000	eMRAM (secure)
QSPI_Flash_S	rx,c	16 MB	0x00200000	0x10200000	QSPI Flash (secure)
SRAM_S	rwx,c	2 MB	0x00000000	0x10000000	Code SRAM (secure)
Peripheral					
S_PCTRL	rw,s	4 KB	0x50080000	0x50080000	Secure Privilege Control Block
S_WDOG	rw,s	4 KB	0x50081000	0x50081000	Secure CMSDK Watchdog Timer







Software Support for latest Arm IP


Cortex-M55
Cortex-M55 + Ethos-U55

Key Algorithms for Signal Processing and ML

Complex dot-product

Fast Fourier Transform

Neural-Networks

Biquad filter

Armv8.1-M architecture performance boost

Plans

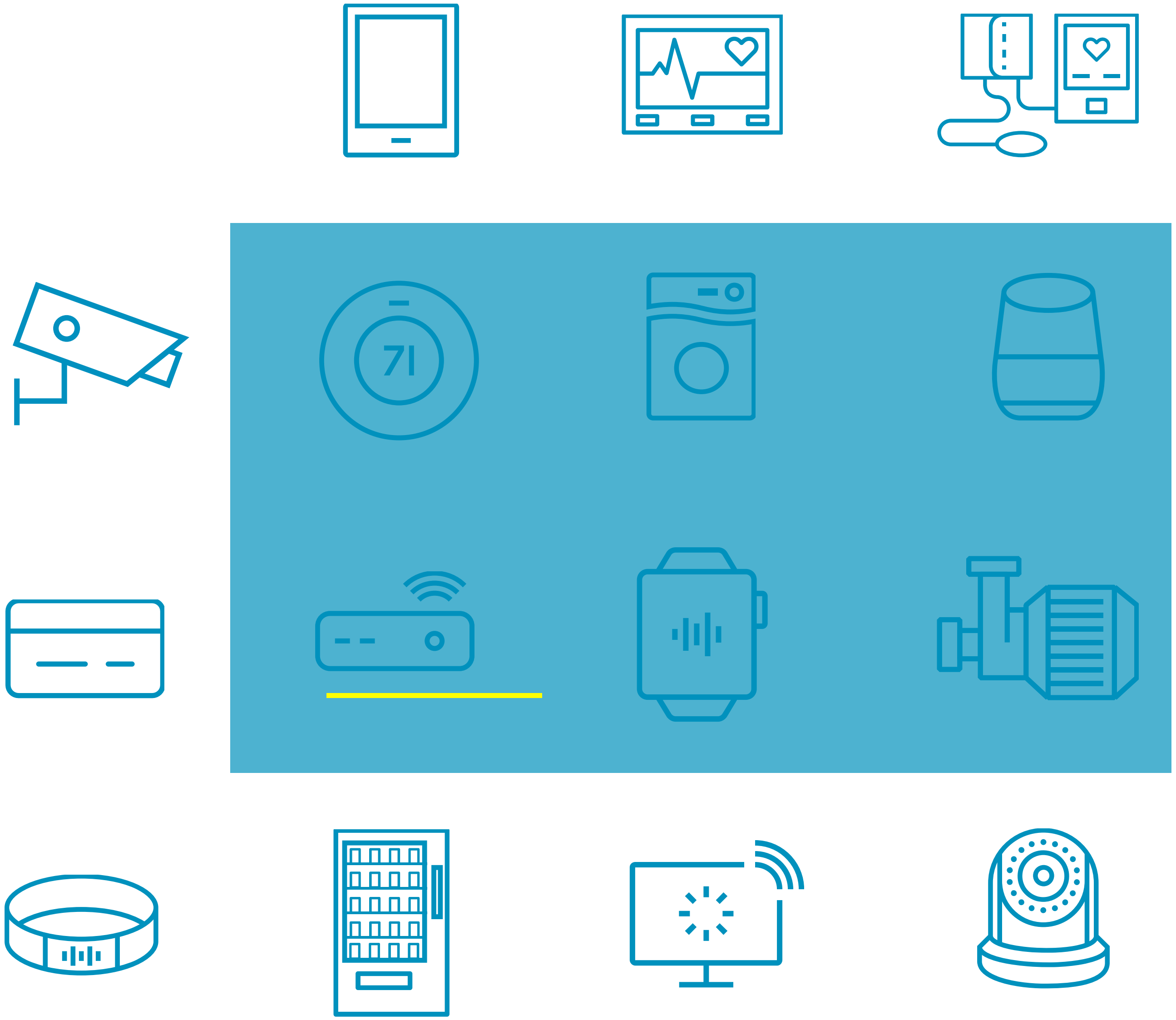
CMSIS DSP/ML kernels :

software portability

data-flow framework

Classical-ML kernels

Create IoT Applications with ready-to-use software components

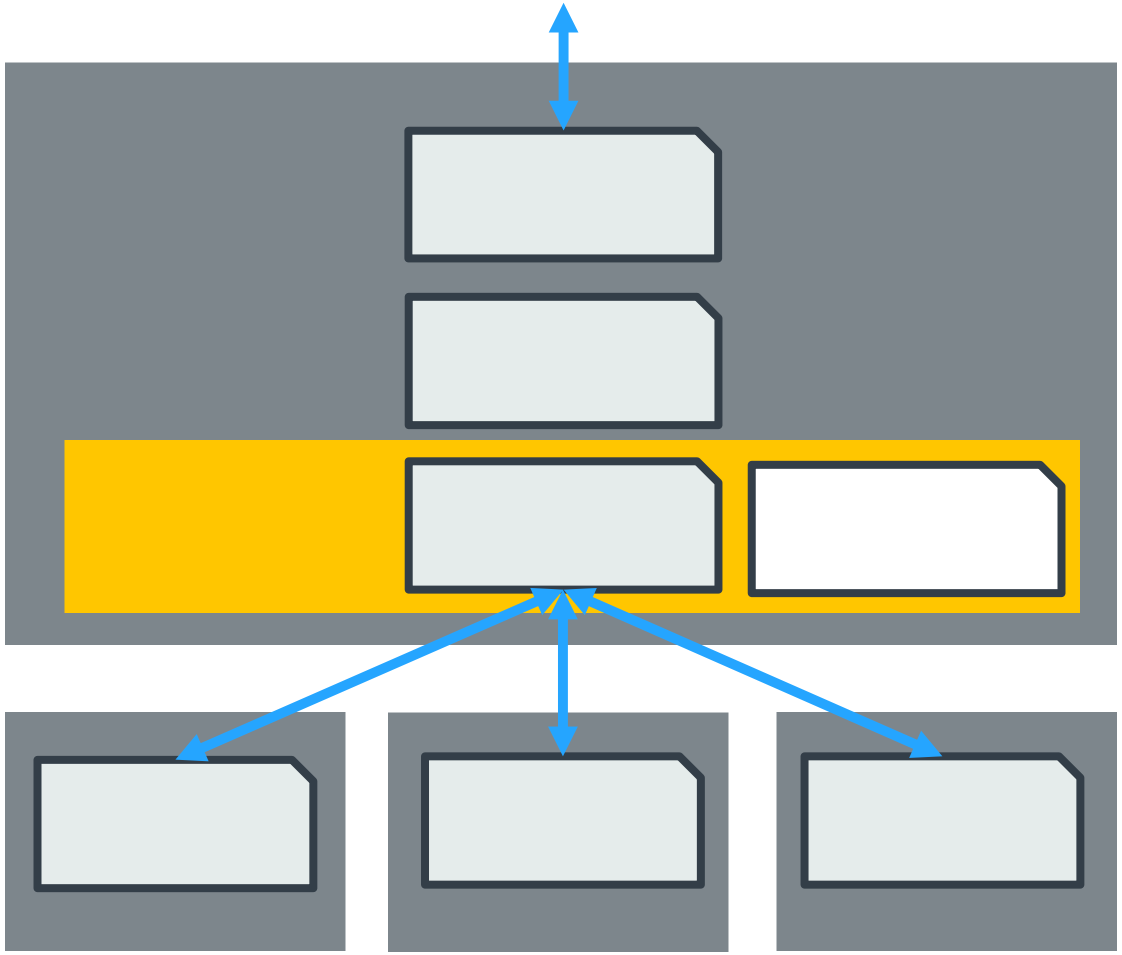

71

- Device / Board HAL:
- RTOS
- Secure Network Interface
- Cloud Connector:
- User Application:

Security

Software components

CMSIS



Azure

IBM

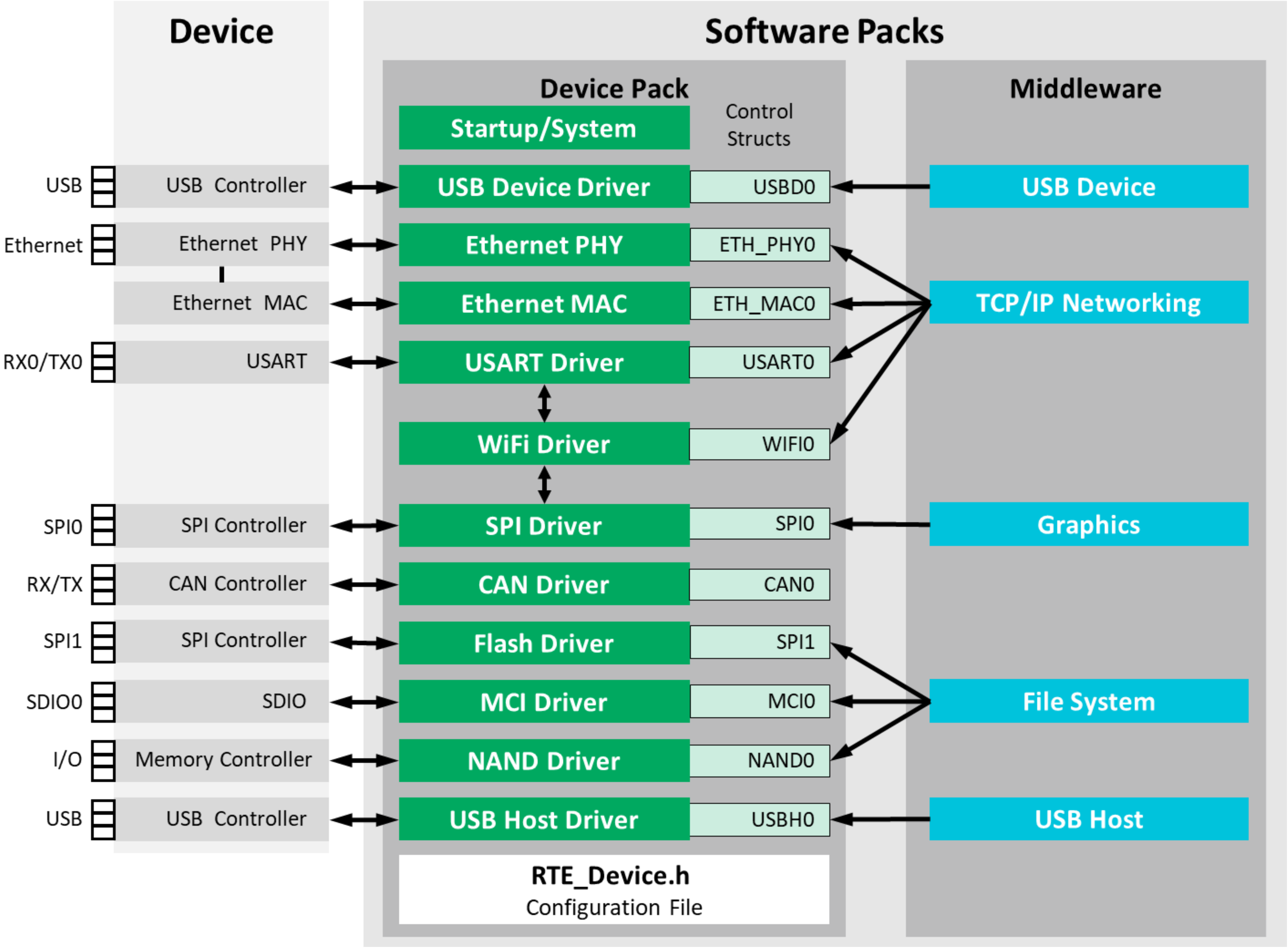
Google Cloud Platform

aws

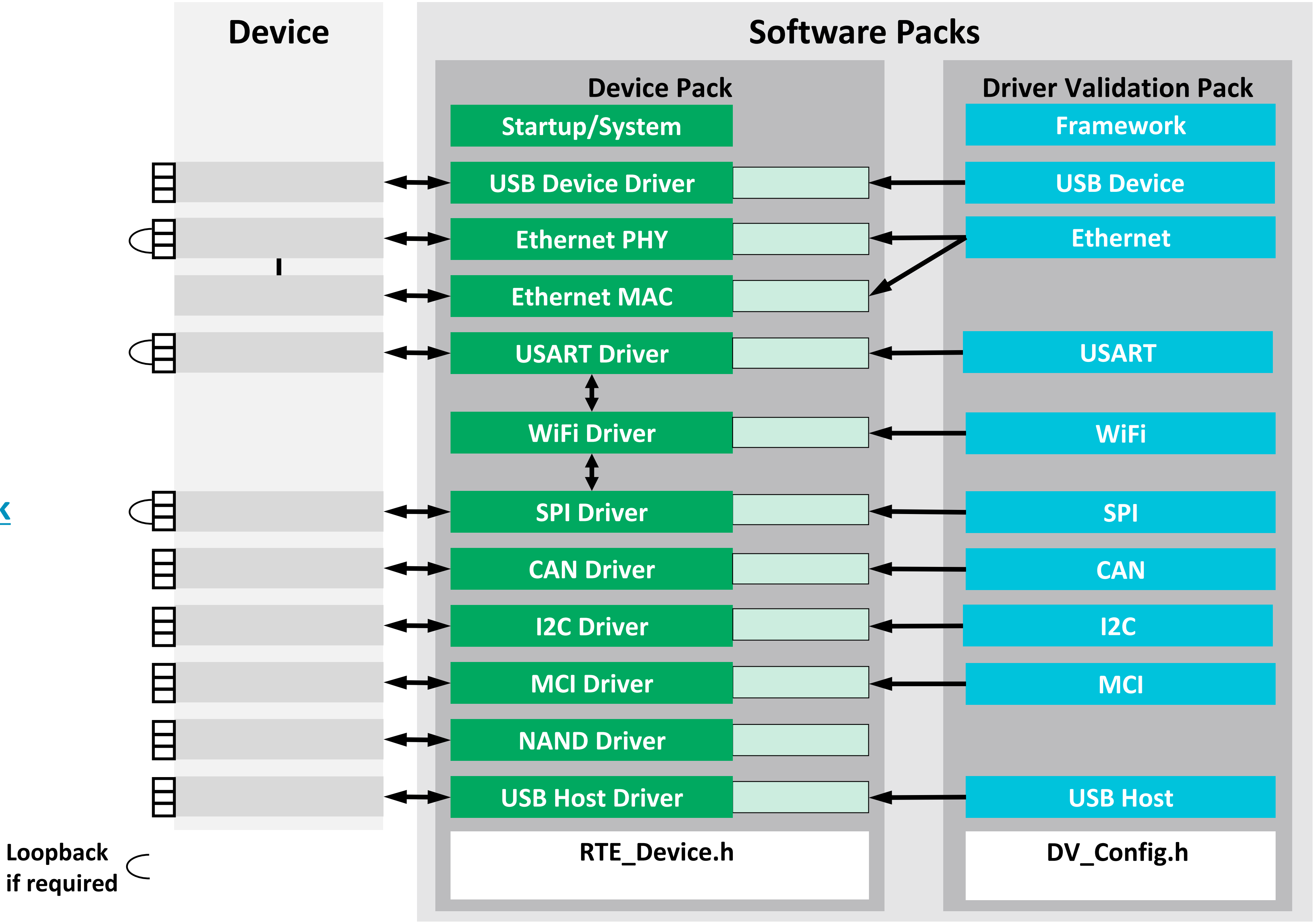
arm PELION

Mbed Crypto

Generic Peripheral Interfaces


Device
Software Packs
Device Pack
Middleware
Startup/System
Control Structs
USB
USB Controller
USB Device Driver
USBD0
USB Device
Ethernet
Ethernet PHY
Ethernet PHY
ETH_PHY0
Ethernet MAC
Ethernet MAC
ETH_MAC0
TCP/IP Networking
RX0/TX0
USART
USART Driver
USART0
WiFi Driver
WIFI0
SPI0
SPI Controller
SPI Driver
SPI0
Graphics
RX/TX
CAN Controller
CAN Driver
CAN0
SPI1
SPI Controller
Flash Driver
SPI1
SDIO0
SDIO
MCI Driver
MCI0
File System
I/O
Memory Controller
NAND Driver
NAND0
USB
USB Controller
USB Host Driver
USBH0
USB Host
RTE_Device.h
Configuration File

Driver Validation Pack



Security Foundation for Cortex-M TrustZone

Platform Security Architecture

Analyze

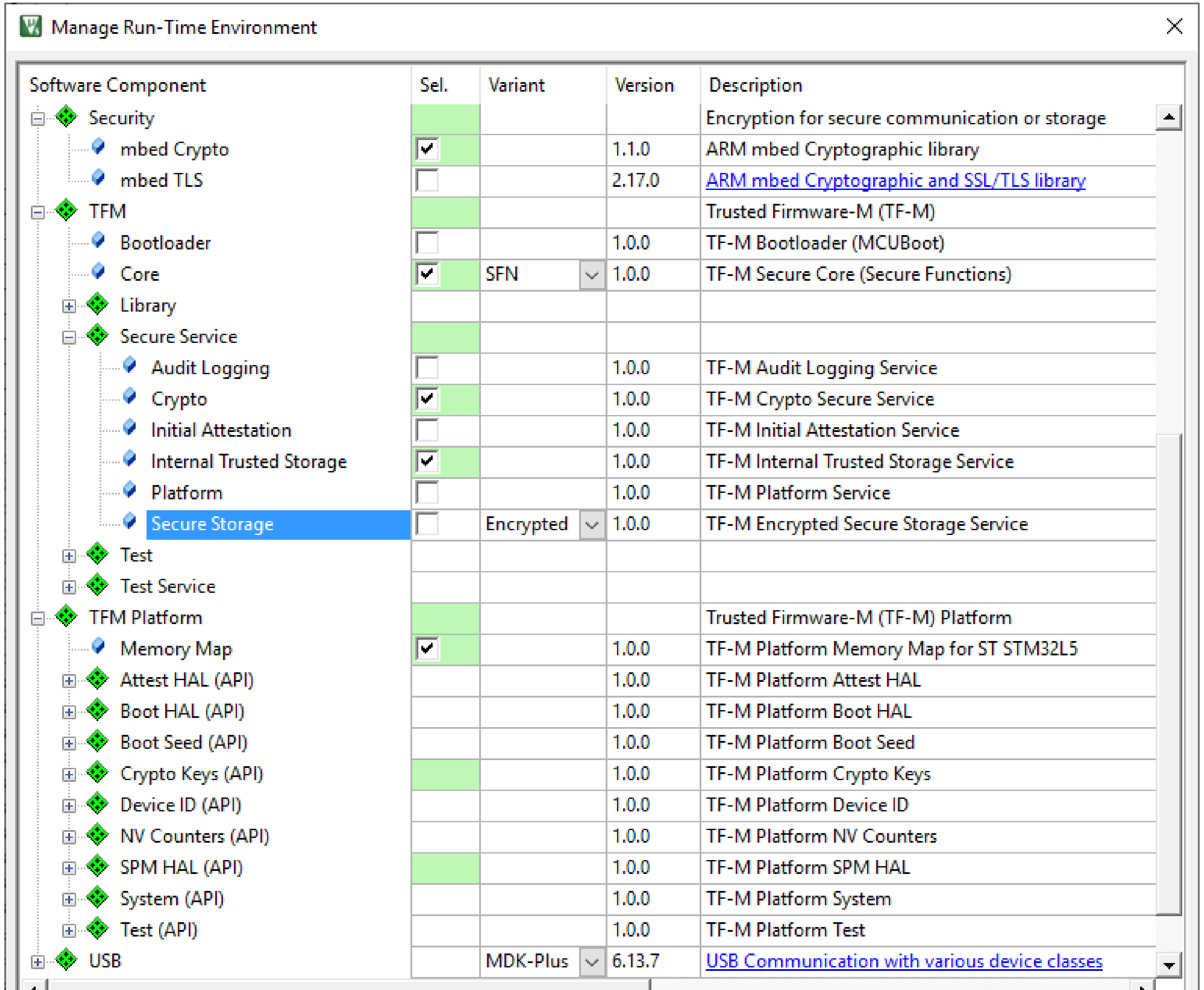
Architect

Implement

Certify

psacertified™

psacertified™



Manage Run-Time Environment

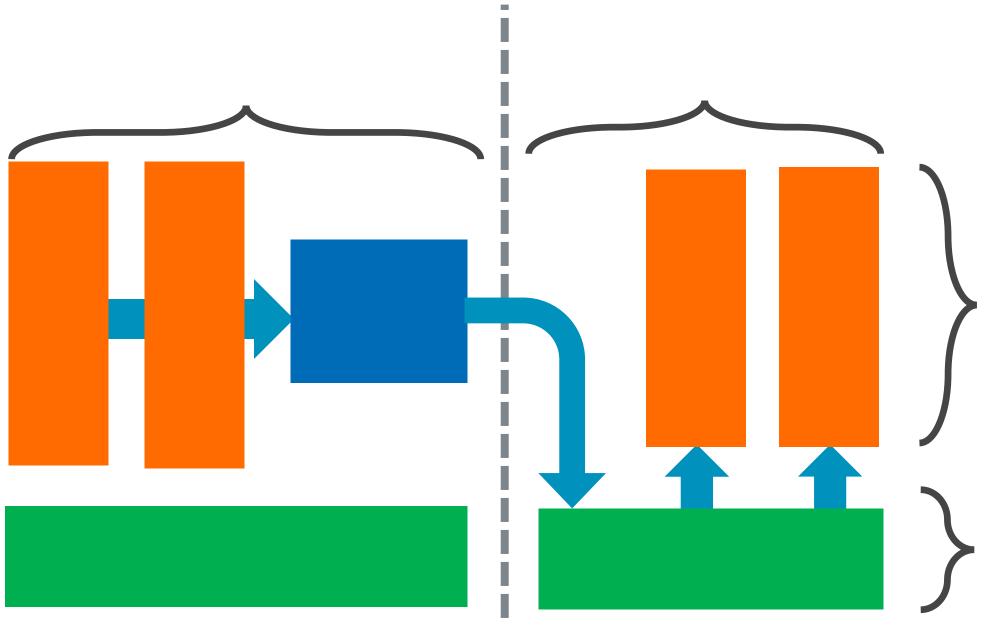
Software Component	Sel.	Variant	Version	Description
Security				Encryption for secure communication or storage
mbed Crypto	☑		1.1.0	ARM mbed Cryptographic library
mbed TLS	☐		2.17.0	ARM mbed Cryptographic and SSL/TLS library
TFM				Trusted Firmware-M (TF-M)
Bootloader	☐		1.0.0	TF-M Bootloader (MCUBoot)
Core	☑	SFN	1.0.0	TF-M Secure Core (Secure Functions)
Library				
Secure Service				
Audit Logging	☐		1.0.0	TF-M Audit Logging Service
Crypto	☑		1.0.0	TF-M Crypto Secure Service
Initial Attestation	☐		1.0.0	TF-M Initial Attestation Service
Internal Trusted Storage	☑		1.0.0	TF-M Internal Trusted Storage Service
Platform	☐		1.0.0	TF-M Platform Service
Secure Storage	☐	Encrypted	1.0.0	TF-M Encrypted Secure Storage Service
Test				
Test Service				
TFM Platform				Trusted Firmware-M (TF-M) Platform
Memory Map	☑		1.0.0	TF-M Platform Memory Map for ST STM32L5
Attest HAL (API)			1.0.0	TF-M Platform Attest HAL
Boot HAL (API)			1.0.0	TF-M Platform Boot HAL
Boot Seed (API)			1.0.0	TF-M Platform Boot Seed
Crypto Keys (API)			1.0.0	TF-M Platform Crypto Keys
Device ID (API)			1.0.0	TF-M Platform Device ID
NV Counters (API)			1.0.0	TF-M Platform NV Counters
SPM HAL (API)			1.0.0	TF-M Platform SPM HAL
System (API)			1.0.0	TF-M Platform System
Test (API)			1.0.0	TF-M Platform Test
USB		MDK-Plus	6.13.7	USB Communication with various device classes

TFM

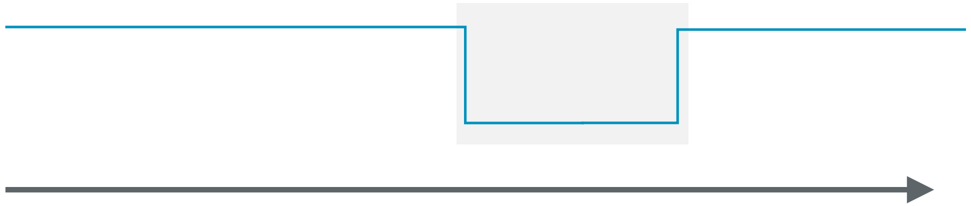
TFM-Platform

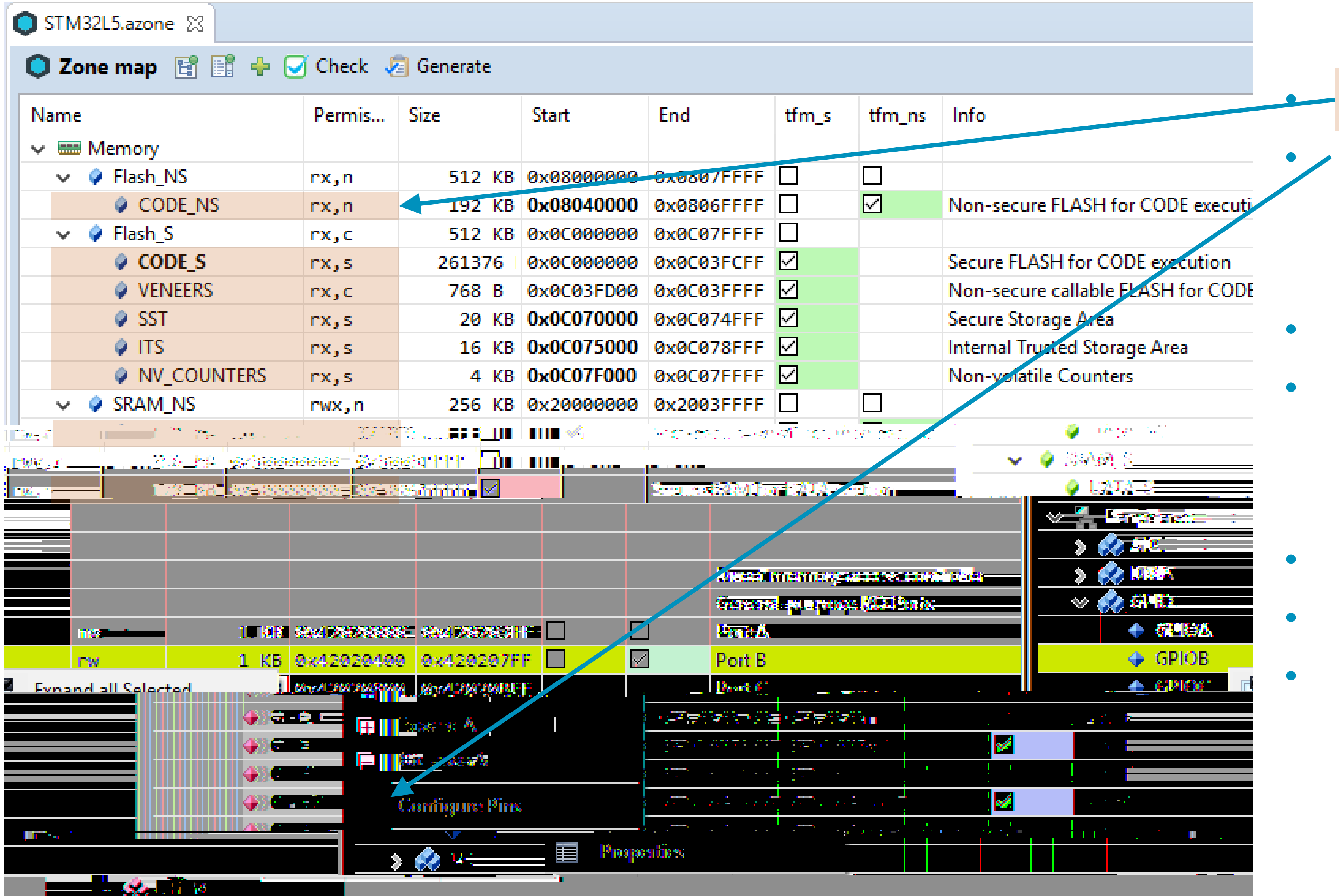
TFM Pack

trustedfirmware.org



- ☑
- ☑
- ☑





STM32L5.azone

Zone map Check Generate

Name	Permis...	Size	Start	End	tfm_s	tfm_ns	Info
Memory							
Flash_NS	rx,n	512 KB	0x08000000	0x0807FFFF	□	□	
CODE_NS	rx,n	192 KB	**0x08040000**	0x0806FFFF	□	☑	Non-secure FLASH for CODE executi
Flash_S	rx,c	512 KB	0x0C000000	0x0C07FFFF	□		
CODE_S	rx,s	261376	0x0C000000	0x0C03FCFF	☑		Secure FLASH for CODE execution
VENEERS	rx,c	768 B	0x0C03FD00	0x0C03FFFF	☑		Non-secure callable FLASH for CODE
SST	rx,s	20 KB	**0x0C070000**	0x0C074FFF	☑		Secure Storage Area
ITS	rx,s	16 KB	**0x0C075000**	0x0C078FFF	☑		Internal Trusted Storage Area
NV_COUNTERS	rx,s	4 KB	**0x0C07F000**	0x0C07FFFF	☑		Non-volatile Counters
SRAM_NS	rwx,n	256 KB	0x20000000	0x2003FFFF	□	□	

rw	1 KB	0x42020400	0x420207FF	□	☑	Port B

www.arm.com/psa

www.keil.com/iot

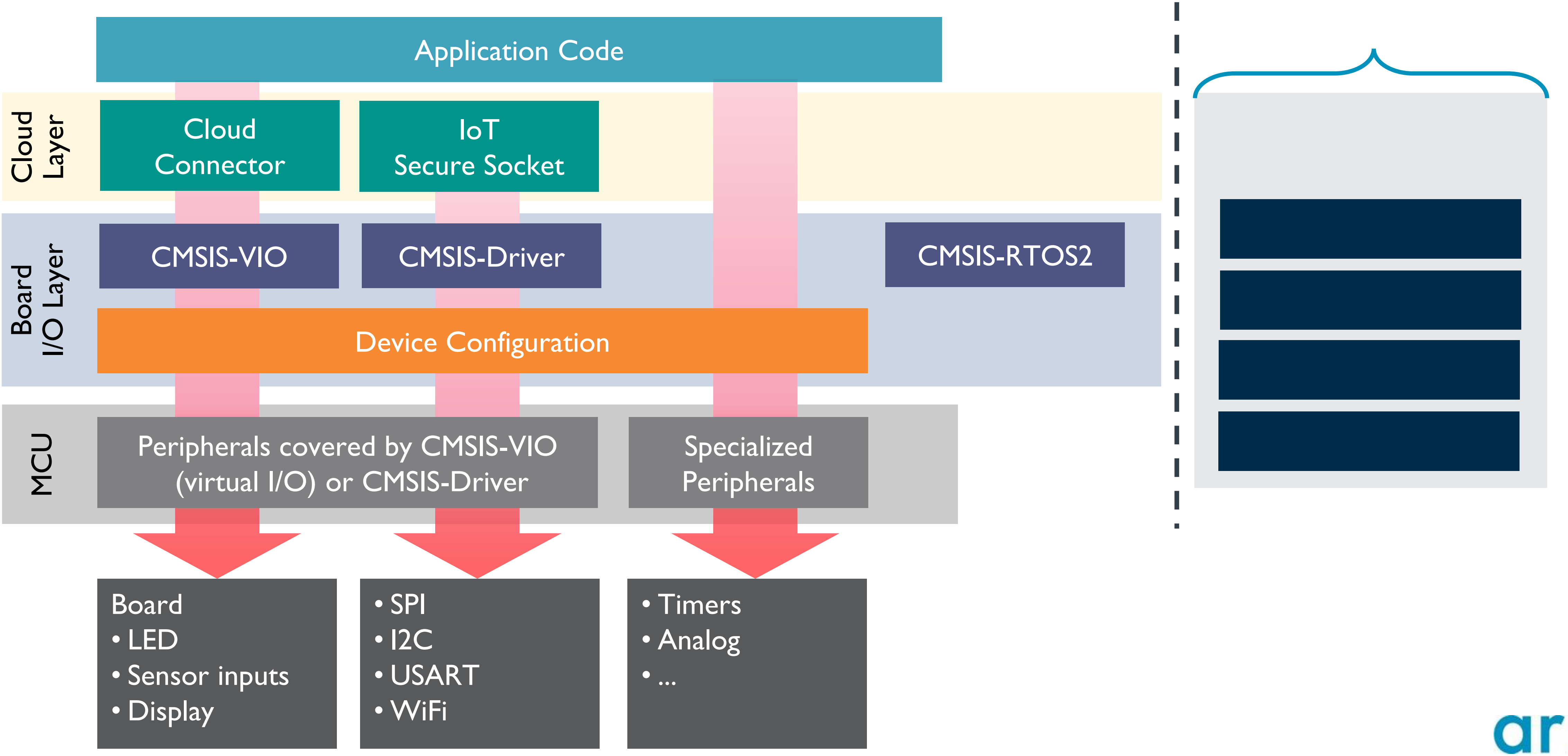
Live demos

hitex

EMBEDDED TOOLS & SOLUTIONS

IoT Security with TrustZone and TF-M on STM32L5

Productivity for complex software templates:

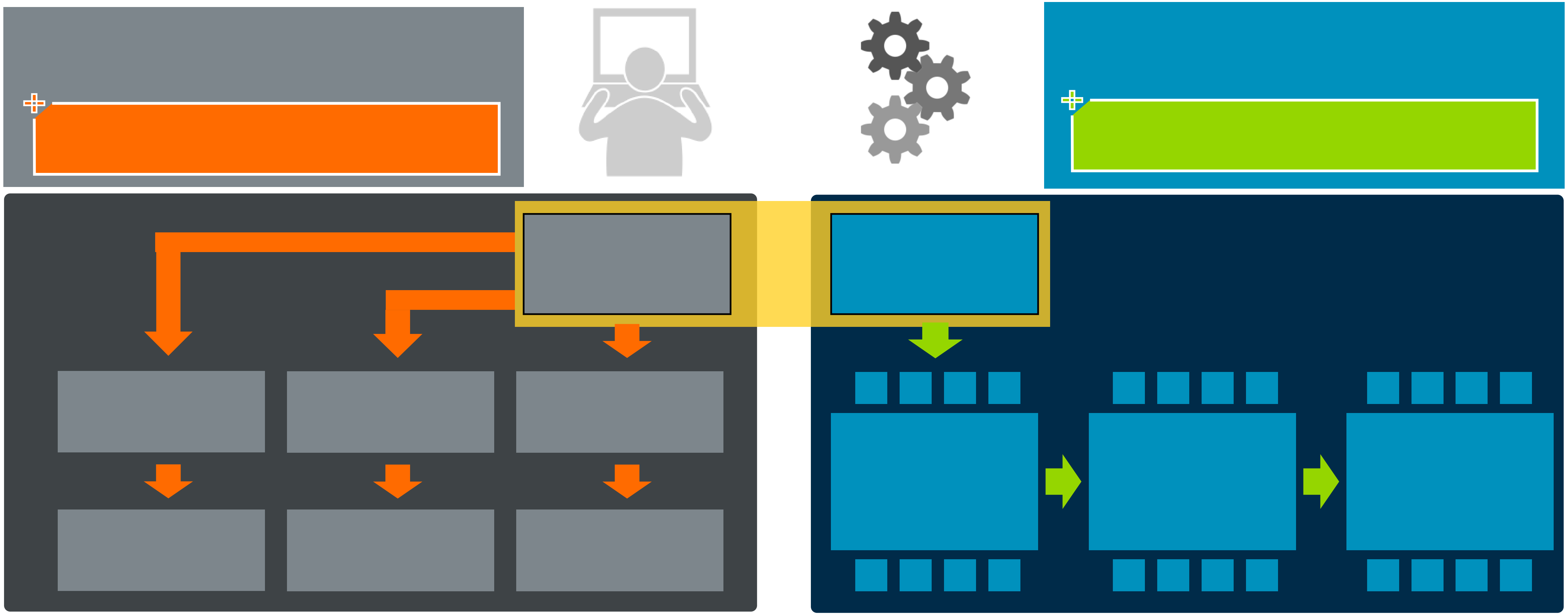


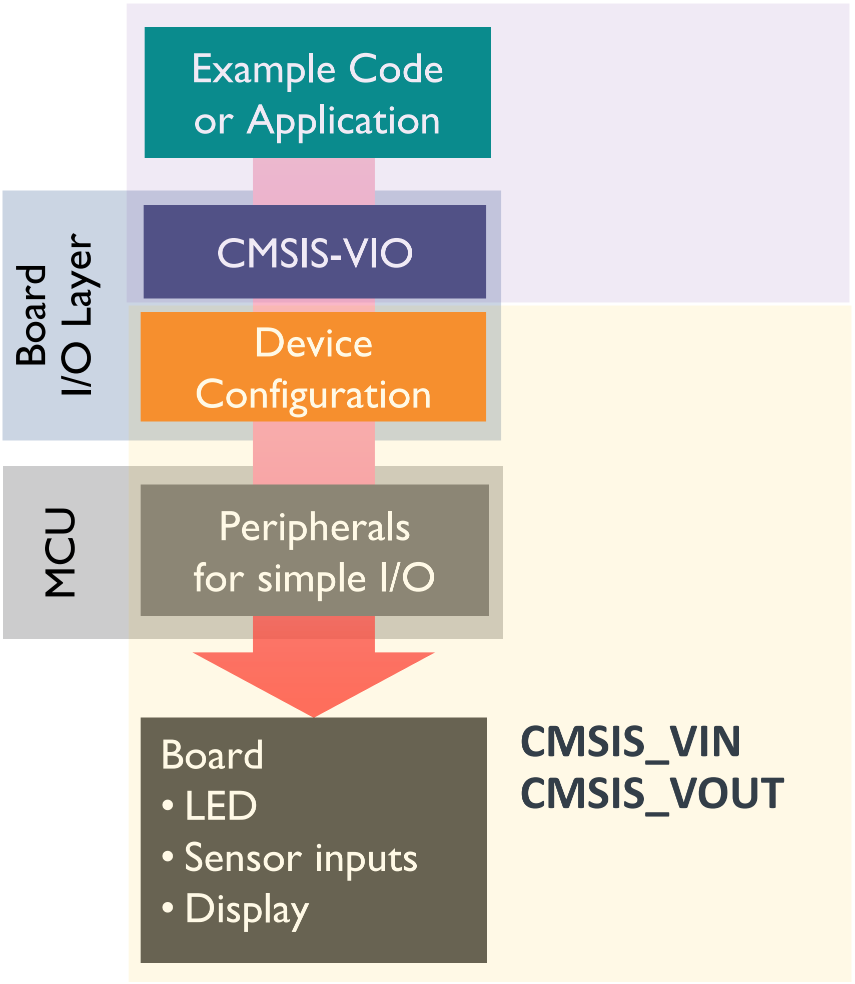
Application Code
Cloud Layer
Cloud Connector
IoT Secure Socket
Board I/O Layer
CMSIS-VIO
CMSIS-Driver
CMSIS-RTOS2
Device Configuration
MCU
Peripherals covered by CMSIS-VIO (virtual I/O) or CMSIS-Driver
Specialized Peripherals
Board
• LED
• Sensor inputs
• Display
• SPI
• I2C
• USART
• WiFi
• Timers
• Analog
• ...

Describes everything required for project build

Command-line tools

- ccmerge: Config File Updater
- cbuildgen: Build Process Manager





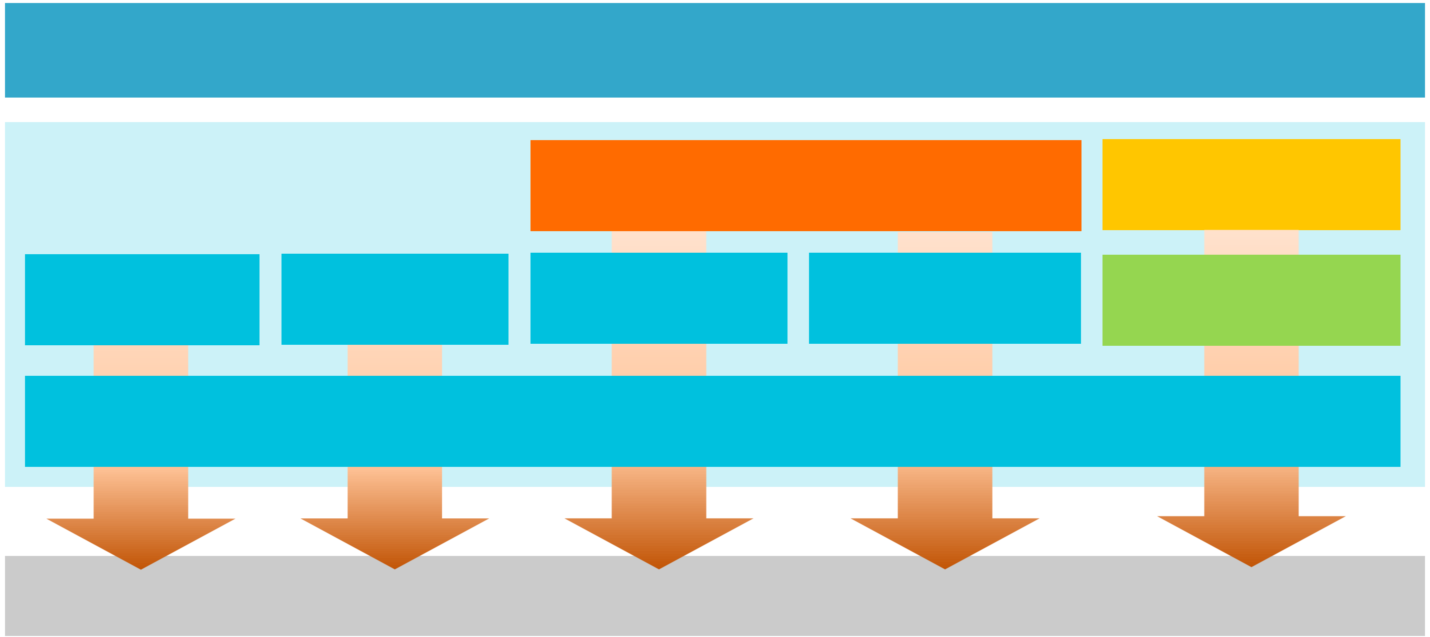
CMSIS-VIO solves that problem with:

CMSIS-VIO solves that problem with:

CMSIS-VIO solves that problem with:

Collaborate with us

CMSIS timeline	Description	How you can contribute
	CMSIS v5.7.0	**Issues**
	CMSIS-Zone	
	Tutorials	



Benefits for the software developer

Easy evaluation

Fast development

Reliable systems

谢谢
ありがとう

감사합니다
धन्यवाद
شكرًا
תודה