Open-CMSIS-Pack

Technical Project Meeting 2021-07-27

This meeting is recorded !

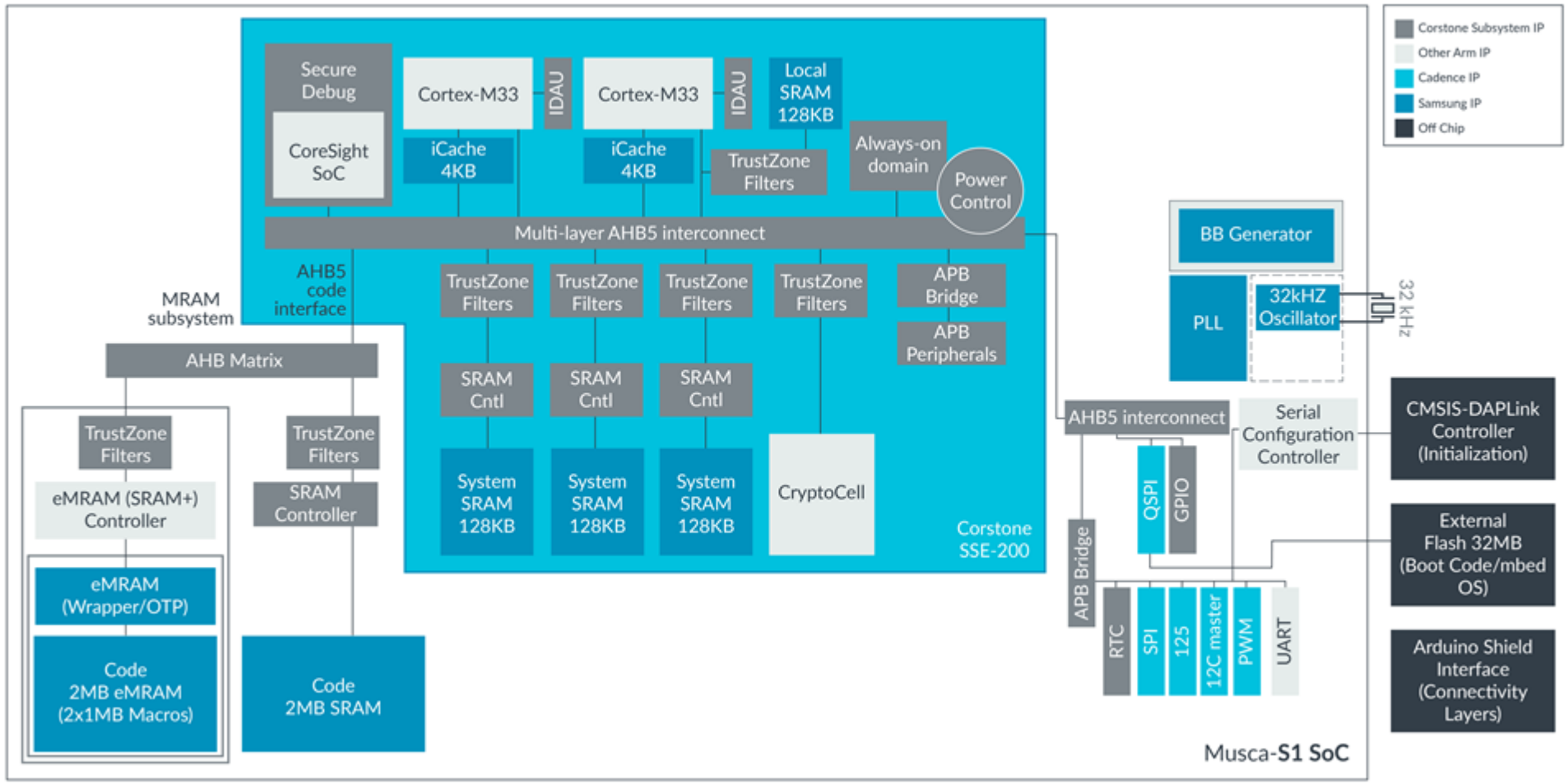
Agenda

- Welcome and review of the agenda
- Actions from last week
- CMSIS-Zone flow – example – dual Cortex-M33 TZ-enabled
  - 4 zones
- Common Description of HW
- Wrap Up

Actions from last week

- feedback for “Include Paths” Estimation
- feedback common framework
- feedback pack generator

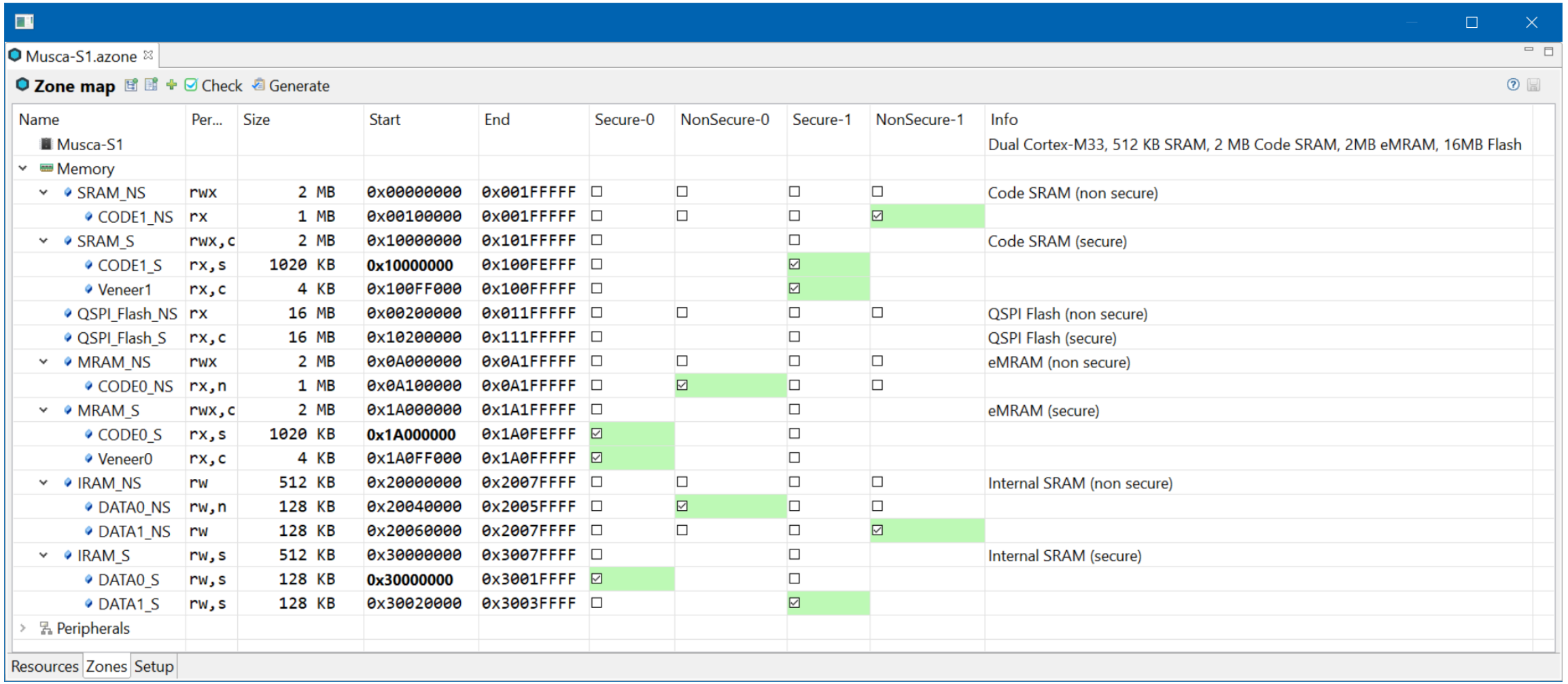
CMSIS-Zone flow



CMSIS-Zone flow

Non-secure		Secure		Description		
From	To	From	To	Size	Non-secure	Secure
0x0000_0000	0x001F_FFFF	0x1000_0000	0x101F_FFFF	2MB	Code SRAM	Code SRAM
0x0020_0000	0x021F_FFFF	0x1020_0000	0x121F_FFFF	32MB	External QSPI Flash	External QSPI Flash
0x0A00_0000	0x0A1F_FFFF	0x1A00_0000	0x1A1F_FFFF	2MB	eMRAM	eMRAM
0x2000_0000	0x2001_FFFF	0x3000_0000	0x3001_FFFF	128KB	Internal SRAM bank 0	Internal SRAM bank 0
0x2002_0000	0x2003_FFFF	0x3002_0000	0x3003_FFFF	128KB	Internal SRAM bank 1	Internal SRAM bank 1
0x2004_0000	0x2005_FFFF	0x3004_0000	0x3005_FFFF	128KB	Internal SRAM bank 2	Internal SRAM bank 2
0x2006_0000	0x2007_FFFF	0x3006_0000	0x3007_FFFF	128KB	Internal SRAM bank 3	Internal SRAM bank 3

CMSIS-Zone flow



Name	Per...	Size	Start	End	Secure-0	NonSecure-0	Secure-1	NonSecure-1	Info
Musca-S1									Dual Cortex-M33, 512 KB SRAM, 2 MB Code SRAM, 2MB eMRAM, 16MB Flash
Memory									
SRAM_NS	rwx	2 MB	0x00000000	0x001FFFFF	☐	☐	☐	☐	Code SRAM (non secure)
CODE1_NS	rx	1 MB	0x00100000	0x001FFFFF	☐	☐	☐	☑	
SRAM_S	rwx,c	2 MB	0x10000000	0x101FFFFF	☐		☐		Code SRAM (secure)
CODE1_S	rx,s	1020 KB	**0x10000000**	0x100FEFFF	☐		☑		
Veneer1	rx,c	4 KB	0x100FF000	0x100FFFFF	☐		☑		
QSPI_Flash_NS	rx	16 MB	0x00200000	0x011FFFFF	☐	☐	☐	☐	QSPI Flash (non secure)
QSPI_Flash_S	rx,c	16 MB	0x10200000	0x111FFFFF	☐		☐		QSPI Flash (secure)
MRAM_NS	rwx	2 MB	0x0A000000	0x0A1FFFFF	☐	☐	☐	☐	eMRAM (non secure)
CODE0_NS	rx,n	1 MB	0x0A100000	0x0A1FFFFF	☐	☑	☐	☐	
MRAM_S	rwx,c	2 MB	0x1A000000	0x1A1FFFFF	☐		☐		eMRAM (secure)
CODE0_S	rx,s	1020 KB	**0x1A000000**	0x1A0FEFFF	☑		☐		
Veneer0	rx,c	4 KB	0x1A0FF000	0x1A0FFFFF	☑		☐		
IRAM_NS	rw	512 KB	0x20000000	0x2007FFFF	☐	☐	☐	☐	Internal SRAM (non secure)
DATA0_NS	rw,n	128 KB	0x20040000	0x2005FFFF	☐	☑	☐	☐	
DATA1_NS	rw	128 KB	0x20060000	0x2007FFFF	☐	☐	☐	☑	
IRAM_S	rw,s	512 KB	0x30000000	0x3007FFFF	☐		☐		Internal SRAM (secure)
DATA0_S	rw,s	128 KB	**0x30000000**	0x3001FFFF	☑		☐		
DATA1_S	rw,s	128 KB	0x30020000	0x3003FFFF	☐		☑		
Peripherals									

Common Hardware Description(s)

- CMSIS-Pack specifies
  - Devices
  - Boards

  No Modules
- CMSIS-SVD specifies access/debug of
  - Device Peripherals

  No Board Peripherals
- CMSIS-Zone rzone specifies device resources
  - Memory + memory protection controller
  - Peripherals + security/privilege setup
  - Security Attribution Unit

  Need gap analysis

Common Hardware Description(s) - (cont'd)

- What data is already being used today?
- What data is / will be required?
- What data is already available to and can be shared by Silicon Vendors?
- What data formats exist?

- What shall be the strategy under Open-CMSIS-Pack?
  - From experience we know that establishing descriptions takes some time
    - Agree format and scope
    - Conversion, Generation, Validation
    - Availability of data at scale

Wrap Up

Issue Overview

Next week: TBD

August:

- How to cover a "corner case": expressing dependencies on features #5
  - When Maxime is back from vacation
- Protecting CMSIS-Pack from malicious tempering (TBD)
- Kick-off development for project creation and maintenance MVP CMSIS-12

Next Meeting: Tuesday Aug. 3rd 2021, 15:00 – 16:00 (UK)

Thank you