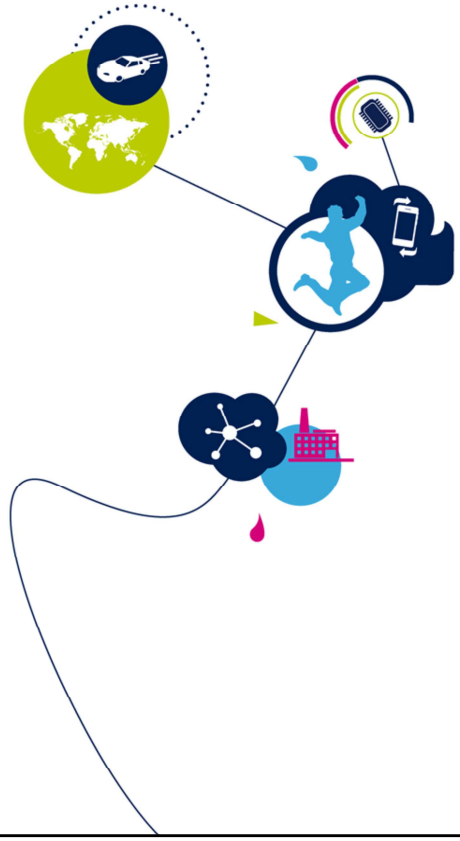
STM32MP1 - ETZPC

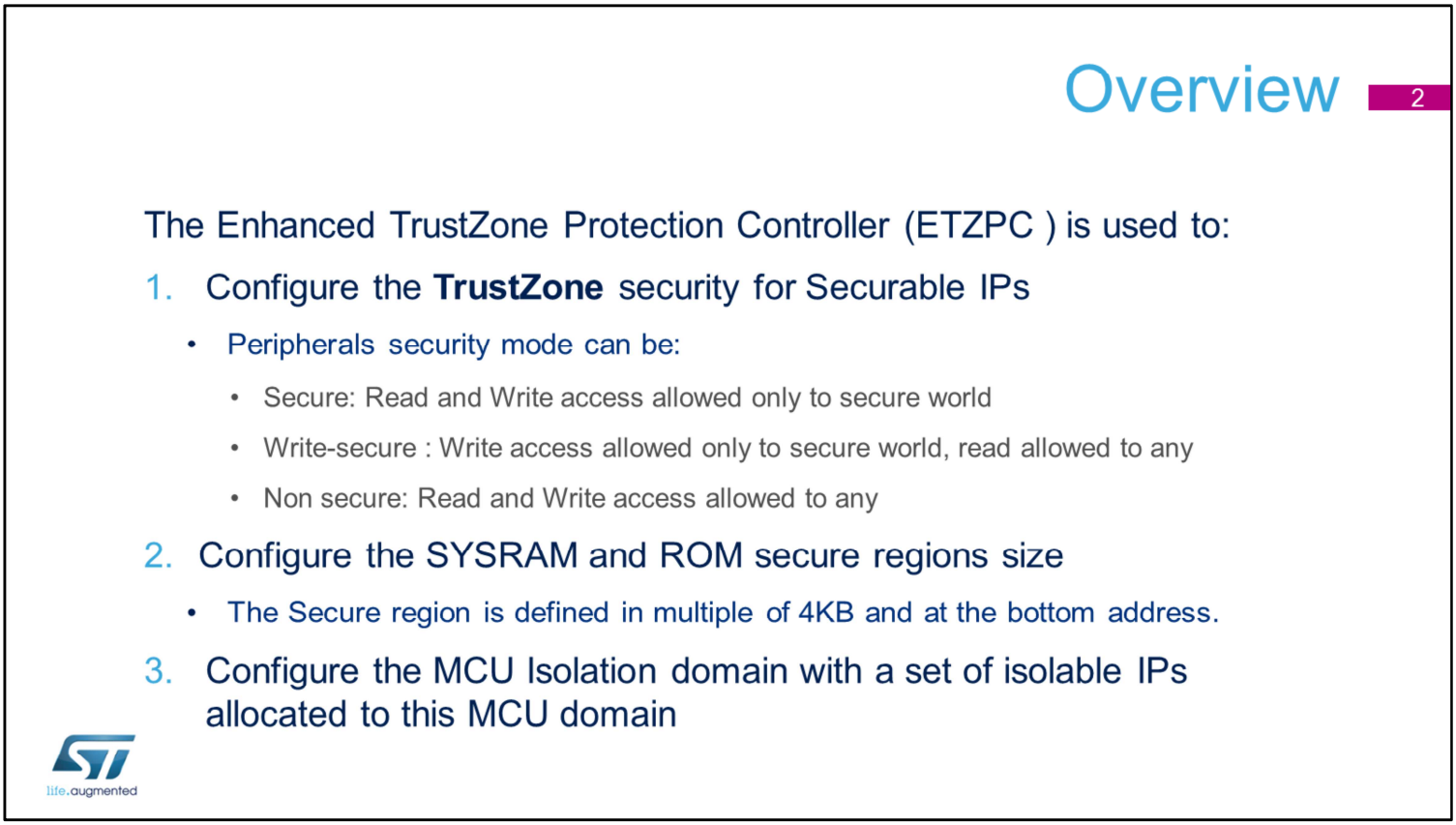
TrustZone Address Space Controller

Revision 1.0



life.augmented

Hello, and welcome to this presentation of the STM32MP1 TrustZone Address Space Controller.



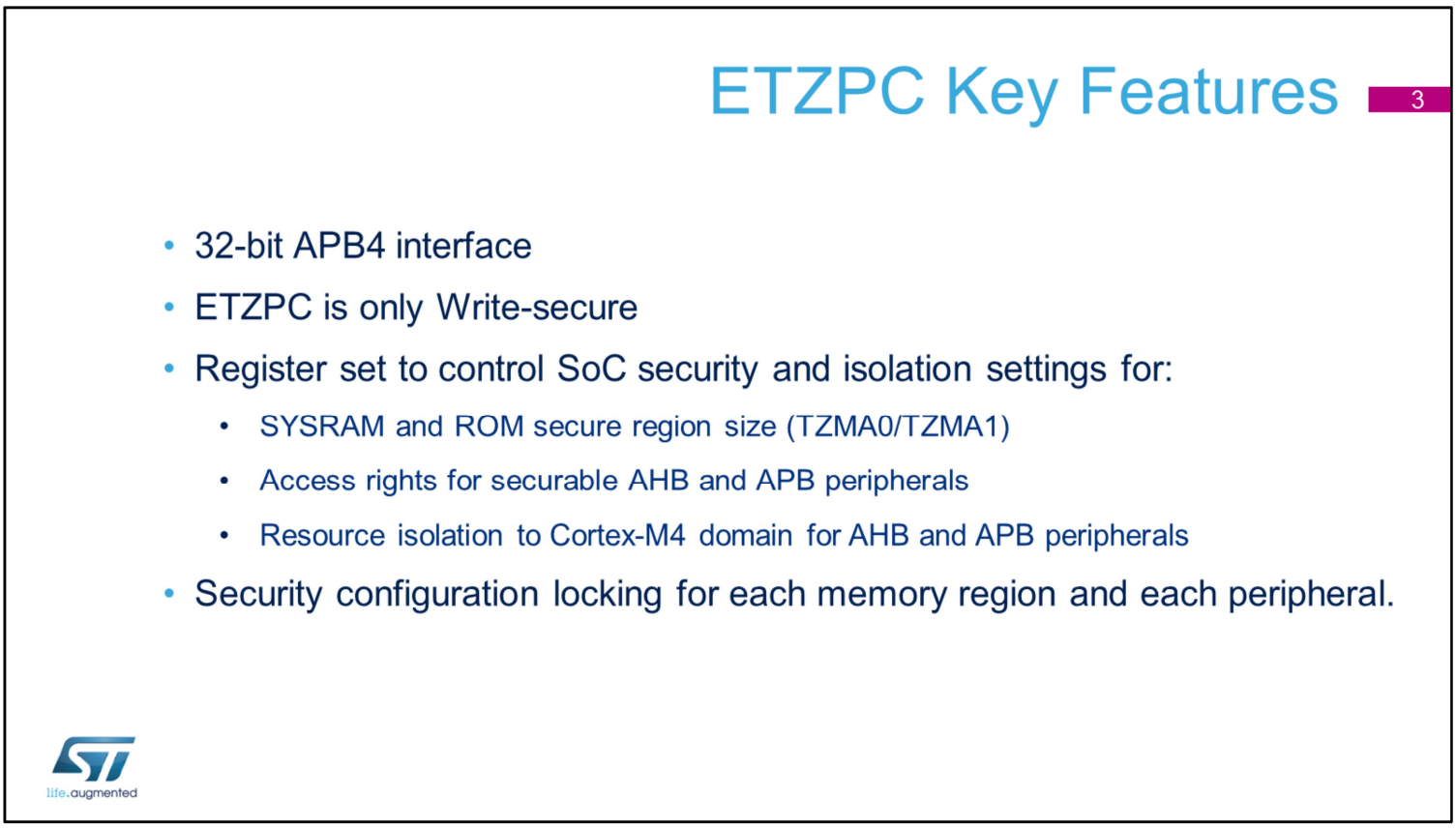
The Enhanced TrustZone Protection Controller (ETZPC) is used to:

1) Configure TrustZone the security for Securable IPs. Peripherals security mode can be:

- Secure: Read and Write access allowed only to secure world
- Write-secure : Write access allowed only to secure world, read allowed to any
- Non secure: Read and Write access allowed to any

2) Configure the SYSRAM and ROM secure regions size. The Secure region is defined in multiple of 4KB and at the bottom address.

3) Configure the MCU Isolation domain with a set of isolable IPs allocated to this MCU domain



The Key features of the TrustZone Address Space Controller are:

- 32-bit APB4 interface
- ETZPC is only Write-secure
- Register set to control SoC security and isolation settings for:
  - SYSRAM and ROM secure region size (TZMA0/TZMA1)
  - Access rights for securable AHB and APB peripherals
  - Resource isolation to Cortex-M4 domain for AHB and APB peripherals
- Security configuration locking for each memory region

and each peripheral.

Peripherals security

4

- Secure resources:
  - No control from ETZPC
  - ETZPC : write secure only
  - TZC : always secure
  - AXIM/GPC: always secure
- Non secure resources:
  - Many peripherals are not concerned by security, they are not controlled by ETPZ from security view point
  - MCU isolation applicable to non secure resources and controlled from ETZPC.
- Securable resources:
  - Peripherals security can be either secure, write secure or non secure according to DECPROT bits
  - SYSRAM and BootROM memories have programmable secure region size according to TZMA0/1 settings

life.augmented

Note: SRAM1/2/3/4 and RETRAM can not be made secure or write secure according to DECPROT bits

Secure resources:

- No control from ETZPC
- ETZPC : write secure only
- TZC : always secure
- AXIM/GPC: always secure

Non secure resources:

- Many peripherals are not concerned by security, they are not controlled by ETPZ from security view point
- MCU isolation applicable to non secure resources and controlled from ETZPC.

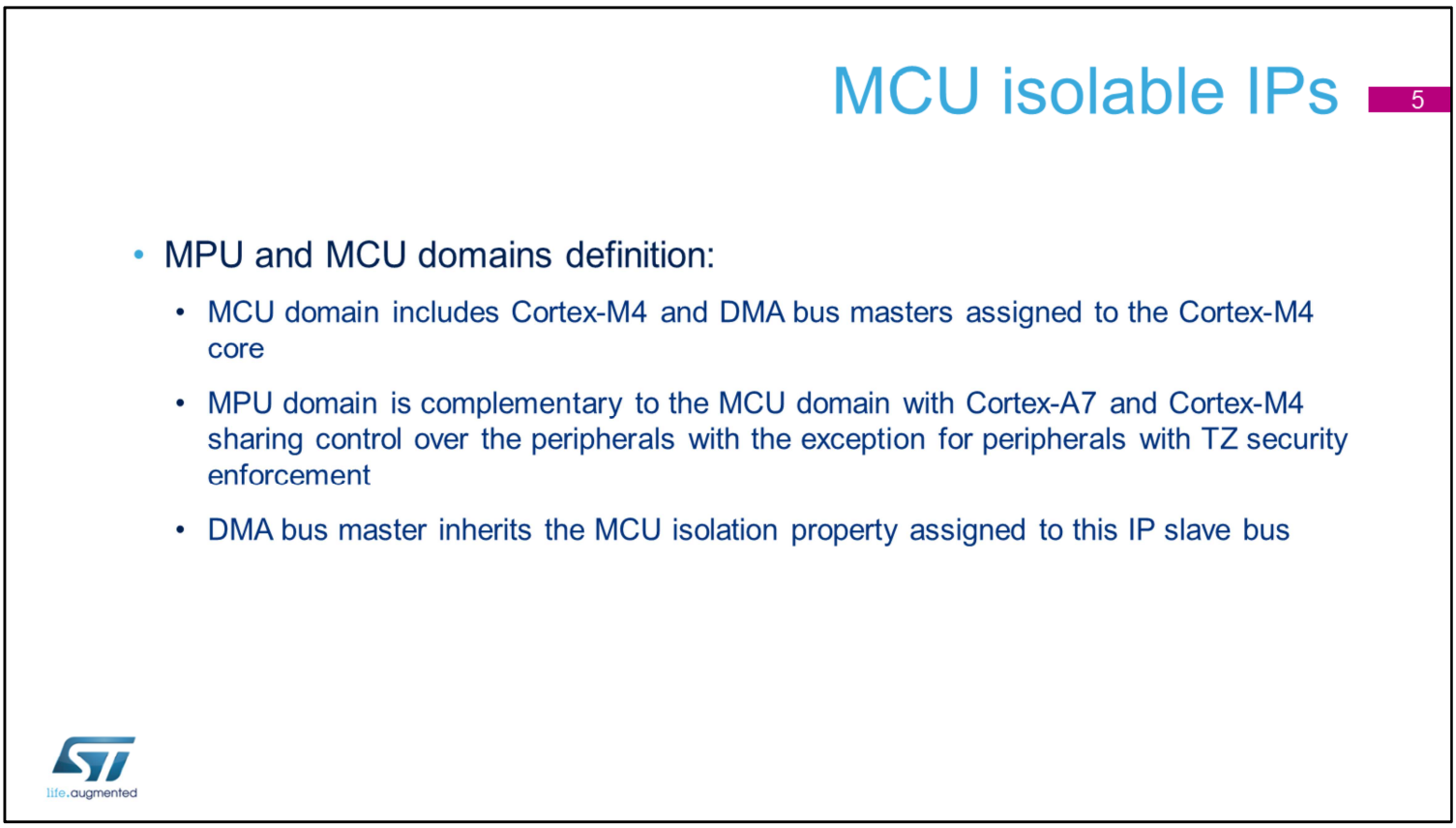
Securable resources:

Peripherals security can be either secure, write secure or

non secure according to DECPROT bits

SYSRAM and BootROM memories have programmable secure region size according to TZMA0/1 settings

Note: SRAM1/2/3/4 and RETRAM can not be made secure or write secure according to DECPROT bits



MPU and MCU domains definition:

- MCU domain includes Cortex-M4 and DMA bus masters assigned to the Cortex-M4 core
- MPU domain is complementary to the MCU domain with Cortex-A7 and Cortex-M4 shared control with the exception for peripherals with TZ security enforcement
- DMA bus master inherits the MCU isolation property assigned to this IP slave bus

Peripherals type and access

- Peripherals can be one of 3 types:
  - Type1: Securable
  - Type2: Non-secure and MCU isolable
  - Type3: Securable and MCU isolable
- ETZPC controls MPU/MCU domain access according to DECPROT[1:0] bits.

DECPROT[1:0]	MPU access				MCU access		Allowed DECPROT bits vs Peripheral Type			Peripheral mode
	secure		non-secure		non-secure					
	read	write	read	write	read	write	Type1	Type2	Type3	
0b00	y	y	n	n	n	n	Yes/default	reserved	Yes	Secure peripheral
0b01	y	y	y	n	y	n	Yes	reserved	Yes	write-secure peripheral
0b10	n	n	n	n	y	y	reserved	Yes	Yes	non-secure peripheral MCU isolated
0b11	y	y	y	y	y	y	Yes	Yes/default	Yes/default	non-secure shared

life.augmented

Peripherals can be one of 3 types:

- Type1: Securable
- Type2: Non-secure and MCU isolable
- Type3: Securable and MCU isolable

ETZPC controls MPU/MCU domain access according to DECPROT[1:0] bits as shown in this table.

- Type1 can be secure, write secure or non secure shared, but never be MCU isolated
- Type2 can be shared or MCU isolated but never be secure or write-secure
- Type3 can be secure, write-secure or non-secure MCU isolated or non-secure shared

Type 1: Securable IPs

- Located on AHB5/APB5 bus
- They are secured by default after reset
- Security property can be changed to Write-secure or non secure by ETZPC
- They can not be made MCU isolable
- Peripheral List:
  - STGENC, BKPSRAM, IWDG1, USART1, SPI6, I2C4, I2C6, CRYP1, HASH1, RNG1, DDRCTRL, DDRPHYC

life.augmented

Type 1 securable IPs are located on AHB5/APB5 bus.

They are secured by default after reset .

Security property can be changed to write-secure or non secure by ETZPC.

They can not be made MCU isolable.

Type 2: Non secure MCU Isolable IPs

- Most peripherals are of type 2 Non secure IPs
- They are Shared between the MPU and the MCU by default after reset
- Security property can be changed to MCU Isolable by ETZPC
- They can not be made Secure or write secure
- Peripherals with bus master change their bus master attribute according to the MCU isolation

life.augmented

Most peripherals are of type 2 Non secure IPs.

They are shared between the MPU and the MCU by default after reset.

The security property can be changed to MCU Isolable by ETZPC.

They can not be made secure or write secure.

Peripherals with a bus master change their bus master attribute according to the MCU isolation.

Type 3: Securable and MCU Isolable IPs

- Only Internal RAMs: SRAM1/2/3/4 and RETRAM memories
- They are non secure shared between MPU and MCU by default after reset
- Security property can be changed by ETZPC to :
  - Secure
  - Write Secure
  - Non secure and MCU isolable

life.augmented

Type 3 Securable IPs are only internal RAMs: SRAM1/2/3/4 and RETRAM memories.

They are non secure shared between the MPU and the MCU by default after reset .

The security property can be changed by ETZPC to :

- Secure
- Write Secure
- Non secure and MCU isolable

DMA master IPs

10

- DMA master IPs, which may be allocated to MCU domain, are:
  - DMA1/DMA2
  - ETH
  - SDMMC3
  - OTG
- a DMA master is set to the MCU when its slave interface is allocated to the MCU by DECPROT bits.
- A DMA master allocated to the MCU ignores all R/W access by the MPU (secure or non-secure)

life.augmented

DMA master IPs, which may be allocated to MCU domain, are:

- DMA1/DMA2
- ETH
- SDMMC3
- OTG

a DMA master is set to the MCU when its slave interface is allocated to the MCU by DECPROT bits.

A DMA master allocated to the MCU ignores all R/W access by the MPU (secure or non-secure).