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

Overview

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

1. Configure the **TrustZone** security for Securable IPs
   - Peripheral security state can be:
     - Secure: Only secure Read and Write access is allowed
     - Write-secure : Only secure Write access is allowed. Any read access is allowed.
     - Non secure: Any Read and Write access is allowed
2. Configure the SYSRAM and ROM secure region size
   - The secure region is defined in multiples of 4KB starting at the bottom address.

life.augmented

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

1) Configure TrustZone security for Securable IPs.
Peripheral security state can be:

- Secure: Only secure Read and Write access is allowed
- Write-secure : Only secure Write access is allowed. Any read access is allowed.
- Non secure: Any Read and Write access is allowed

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

ETZPC Key Features

- 32-bit APB4 interface
- ETZPC is Write-secure
- Register set to control:
  - SYSRAM and ROM secure region size (TZMA0/TZMA1)
  - Access rights for securable AHB and APB peripherals
- Security configuration locking for each memory region and each peripheral.

life.augmented

The TrustZone Address Space Controller has a 32-bit APB4 interface which is write-secure.

It contains registers to program SYSRAM and ROM secure region size and access rights for securable AHB and APB peripherals.

The security configuration for each memory region and each peripheral can be locked.

Peripheral security

- Secure resources:
  - Not controlled by ETZPC
  - ETZPC : write secure only
  - TZC, AXIM/GPC, MDMA config, DMA3 config : always secure
- Non secure resources:
  - Several peripherals are not concerned by security, they are not controlled by ETZPC
- Securable resources:
  - Some peripherals 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

4

Secure resources are not controlled from the ETZPC

The ETZPC itself is always write secure.

The TZC, the AXIM/GPC and the MDMA and DMA3 configuration ports are always secure.

Many peripherals are always non-secure, and are not controlled by the ETZPC

Securable peripherals can be either secure, write secure or non secure according to the DECPROT bits in the ETZPC

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

Peripheral access vs DECPROT[1:0]

DECPROT[1:0]	MPU access				Peripheral mode
	secure		non-secure		
	read	write	read	write	
0b00	y	y	n	n	Secure peripheral
0b01	y	y	y	n	Write-secure peripheral
0b10	y	y	y	y	Reserved
0b11	y	y	y	y	Non-secure

life.augmented

ETZPC controls access to securable resources according to the DECPROT bits, as shown in this table.

Securable IPs

- They are secured by default after reset
- Security property can be changed to write-secure or non-secure by ETZPC
- Securable Peripheral List:
  - VREFBUF, LPTIM2, LPTIM3, LTDC, DCMIPP, USBPHYCTRL, DDRCTRLPHY, IWDG1, STGENC, USART1, USART2, SPI4, SPI5, I2C3, I2C4, I2C5, TIM12, TIM13, TIM14, TIM15, TIM16, TIM17, ADC1, ADC2, OTG, TSC, RNG, HASH, CRYP, SAES, PKA, BKPSRAM, ETH1, ETH2, SDMMC1, SDMMC2, DDRMCE, FMC, QSPI, SRAM1, SRAM2, SRAM3

life.augmented

Securable IPs are Secure by default after a reset.

The Security property can be changed to write-secure or non secure in the ETZPC.

Thank you

life.augmented