TZC internal peripheral

Contents

Stable: 04.02.2020 - 15:43 / Revision: 04.02.2020 - 15:56

A quality version of this page, approved on *4 February 2020*, was based off this revision.

Contents

1 Article purpose

The purpose of this article is to:

- briefly introduce the TZC peripheral and its main features
- indicate the level of security supported by this hardware block
- explain how it can be allocated to the three runtime contexts and linked to the corresponding software components
- explain, when necessary, how to configure the TZC peripheral.

2 Peripheral overview

The TZC peripheral is used to filter read/write accesses to the DDR controller according to TrustZone access rights, and according to Non-Secure master Address ID (NSAID) on up to 9 programmable regions.

2.1 Features

Refer to the STM32MP15 reference manuals for the complete list of features, and to the software components, introduced below, to see which features are implemented.

2.2 Security support

The TZC is a **secure** peripheral.

3 Peripheral usage and associated software

3.1 Boot time

The TZC is configured at boot time to setup DDR accesses.

3.2 Runtime

3.2.1 Overview

The TZC is a system peripheral and is controlled by the Arm®Cortex®-A7 secure.

3.2.2 Software frameworks

Domain	Peripheral	Software frameworks			Comment
Cortex-A7 secure (OP-TEE)	Cortex-A7 non-secure (Linux)	Cortex-M4 (STM32Cube)			
Security	TZC	OP-TEE TZC driver			

3.2.3 Peripheral configuration

The configuration is applied by the firmware running in the secure context.

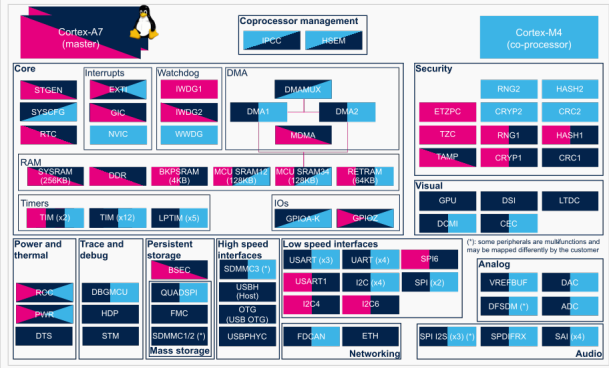
This configuration is done in TF-A or in OP-TEE.

3.2.4 Peripheral assignment

Check boxes illustrate the possible peripheral allocations supported by STM32 MPU Embedded Software:

- means that the peripheral can be assigned () to the given runtime context.
- is used for system peripherals that cannot be unchecked because they are statically connected in the device.

Refer to How to assign an internal peripheral to a runtime context for more information on how to assign peripherals manually or via STM32CubeMX.
The present chapter describes STMicroelectronics recommendations or choice of implementation. Additional possiblities might be described in STM32MP15 reference manuals
.



Internal peripherals

Domain	Peripheral	Runtime allocation		Comment
	Cortex-A7	Cortex-A7	Cortex-M4	

Domain	Peripheral	Runtime allocation				Comment
Instance	secure (OP-TEE)	non-secure (Linux)	(STM32Cube)			
Security	TZC	TZC				

4 How to go further

The TZC is an Arm® peripheral: TZC-400 TrustZone Address Space Controller[1]

5 References

- http://infocenter.arm.com/help/topic/com.arm.doc.ddi0504c/DDI0504C_tzc400_r0p1_trm.pdf

TrustZone® address space Controller for DDR

Arm® and TrustZone® are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Doubledata rate (memory domain)

TrustZone®

Arm® and TrustZone® are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Arm® is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Cortex®

Open Portable Trusted Execution Environment

Linux® is a registered trademark of Linus Torvalds.