ETZPC internal peripheral

Contents

Stable: 31.07.2020 - 14:07 | Revision: 31.07.2020 - 14:00

A quality version of this page, approved on *31 July 2020*, was based off this revision.

Contents

1 Article purpose

The purpose of this article is to:

- briefly introduce the ETZPC 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 ETZPC peripheral.

2 Peripheral overview

The ETZPC peripheral is used to configure TrustZone security in a SoC having bus masters and slaves with programmable-security attributes (securable resources) such as:

- on-chip RAM/ROM with programmable secure region size
- AHB and APB peripherals to be made secure
- AHB masters to be granted secure rights

The ETZPC peripheral also allows peripheral isolation. With MCU isolation, some peripherals can be assigned to Cortex-M4 context execution only. Those peripherals will not be accessible for Cortex-A7 contexts (secure and non-secure).

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 ETZPC is a **secure** peripheral.

3 Peripheral usage and associated software

3.1 Boot time

The ETZPC is configured at boot time to setup the platform security.

3.2 Runtime

3.2.1 Overview

The ETZPC 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	ETZPC	TF-A(BL32) or OP-TEE ETZPC driver Read/Write access	U-Boot Read only access	Resource Manager Utility Read only access	Configuration made by A7 secure. U-Boot updates the L inux device tree.

3.2.3 Peripheral configuration

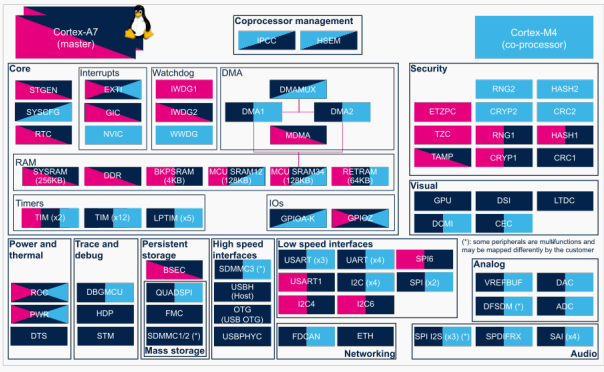
The configuration is applied by the firmware running in a secure context.

This configuration is done in TF-A(BL32) or OP-TEE, through device tree (see ETZPC device tree configuration).

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.



Internal peripherals

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.

Domain	Peripheral	Runtime allocation				Comment
Instance	Cortex-A7 secure (OP-TEE)	Cortex-A7 non-secure (Linux)	Cortex-M4 (STM32Cube)			
Security	ETZPC	ETZPC				

4 How to go further

The ETZPC is an STMicroelectronics extension of the Arm® peripheral: TrustZone Protection Controller[1]

5 References

- http://infocenter.arm.com/help/topic/com.arm.doc.dto0015a/DTO0015_primecell_infrastructure_amba3_tzpc_bp147_to.pdf

Extended TrustZone Protection Controller

TrustZone®

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

Random Access Memory (Early computer memories generally hadserial access. Memories where any given address can be accessed when desired were then called "random access" to distinguish them from the memories where contents can only be accessed in a fixed order. The term is used today for volatile random-acces ssemiconductor memories.)

Read Only Memory

Advanced High-performance Bus

Advanced Peripheral Bus

Microcontroller Unit (MCUs have internal flash memory and are intended to operate with a minimum amount of external support ICs. They commonly are a self-contained, system-on-chip (SoC) designs.)

Cortex®

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

Open Portable Trusted Execution Environment

Linux® is a registered trademark of Linus Torvalds.