



HSEM internal peripheral



Contents

1. HSEM internal peripheral	3
2. STM32MP15 resources	6
3. ETZPC internal peripheral	6
4. Hardware spinlock overview	6
5. STM32CubeMP1 architecture	6
6. STM32CubeMX	6
7. STM32MPU Embedded Software architecture overview	7
8. How to assign an internal peripheral to a runtime context	7



HSEM internal peripheral

Stable: 04.02.2020 - 15:58 / Revision: 04.02.2020 - 15:47

Contents

1 Article purpose	3
2 Peripheral overview	3
2.1 Features	3
2.2 Security support	3
3 Peripheral usage and associated software	4
3.1 Boot time	4
3.2 Runtime	4
3.2.1 Overview	4
3.2.2 Software frameworks	4
3.2.3 Peripheral configuration	4
3.2.4 Peripheral assignment	5

1 Article purpose

The purpose of this article is to briefly introduce the hardware semaphore peripheral (HSEM) and its main features.

2 Peripheral overview

The peripheral hardware spinlock is used to provide synchronization and mutual exclusion between heterogeneous processors.

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.

- 32 hardware semaphores are available on the platform.
- semaphores could be accessed by the Arm[®] Cortex[®]-A7 core and the Arm[®] Cortex[®]-M4

2.2 Security support

The hardware semaphores is a **non-secure** peripheral (under ETZPC control).



3 Peripheral usage and associated software

3.1 Boot time

The hardware semaphore is used at boot time for GPIO access protection between the Arm® Cortex®-A7 and Cortex®-M4 cores.

3.2 Runtime

3.2.1 Overview

The hardware spinlock can be used by:

- the Arm Cortex-A7 non-secure core to be controlled in Linux® by the [hardware spinlock framework](#)
- the Arm Cortex-M4 to be controlled in STM32Cube MPU Package by [HSEM HAL driver](#)

Notice that the Arm Cortex-A7 secure could also use the spinlock, but there is no such using yet in OpenSTLinux distribution.

3.2.2 Software frameworks

Do	Peri	Software frameworks		Comment
mai Cor tex -A7 sec ure (O P- TE E)	Cor tex -A7 no n- sec ure (Li nux)	Cortex-M4 (STM32Cube)		
Do m ain		Linux hardware spinlock framework	HSEM HAL driver	

3.2.3 Peripheral configuration

The configuration is applied by the firmware running in the context to which the peripheral is assigned. The configuration can be done alone via the [STM32CubeMX](#) tool for all internal peripherals, and then manually completed (particularly for external peripherals), according to the information given in the corresponding software framework article or, for Linux in the [Hardware spinlock overview](#) article.

The HSEM peripheral is shared between the Cortex-A and Cortex-M contexts, so a particular attention must be paid to have a complementary configuration on both contexts.

3.2.4 Peripheral assignment

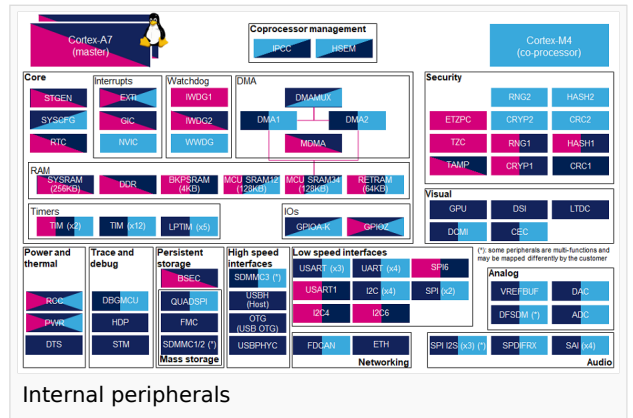
It does not make sense to allocate HSEM to a single runtime execution context, that is why it is enabled by default for both cores in the STM32CubeMX.

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 possibilities might be described in STM32MP15 reference manuals.



		Runtime allocation				Comment
Do ma in in st a nc e	Per in C or te x- A 7 se cu re (O P T E E)	Cortex-A7 non-secure (Linux)	Cortex-M4 (STM32Cube)			
	C o p r o c e s s o r	H S E M	HSEM			



Hardware Semaphore

General-Purpose Input/Output (A realization of open ended transmission between devices on an embedded level. These pins available on a processor can be programmed to be used to either accept input or provide output to external devices depending on user desires and applications requirements.)

Microprocessor Unit

Open Portable Trusted Execution Environment

Permission error

Stable: 24.06.2020 - 17:52 / Revision: 24.06.2020 - 12:32

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 31.07.2020 - 14:57 / Revision: 31.07.2020 - 14:56

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 16.01.2020 - 15:11 / Revision: 16.01.2020 - 15:07

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 21.02.2020 - 08:39 / Revision: 04.02.2020 - 15:22

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 31.01.2020 - 13:04 / Revision: 31.01.2020 - 13:02

You do not have permission to read this page, for the following reason:



The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 15.10.2019 - 11:55 / Revision: 15.10.2019 - 11:55

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer

Permission error

Stable: 22.06.2020 - 09:50 / Revision: 22.06.2020 - 09:49

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer