



RNG internal peripheral



Contents

1. RNG internal peripheral	3
2. ETZPC internal peripheral	9
3. Hardware random overview	15
4. How to assign an internal peripheral to a runtime context	26
5. OP-TEE overview	33
6. STM32CubeMP1 architecture	41
7. STM32CubeMX	55
8. STM32MP15 resources	58
9. STM32MPU Embedded Software architecture overview	62



A quality version of this page, approved on *12 February 2020*, was based off this revision.

Contents

1 Article purpose	4
2 Peripheral overview	5
2.1 Features	5
2.2 Security support	5
3 Peripheral usage and associated software	6
3.1 Boot time	6
3.2 Runtime	6
3.2.1 Overview	6
3.2.2 Software frameworks	6
3.2.3 Peripheral configuration	6
3.2.4 Peripheral assignment	6
4 How to go further	8
5 References	9



1 Article purpose

The purpose of this article is to:

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



2 Peripheral overview

The **RNG** peripheral is used to provide 32-bit random numbers.

2.1 Features

Refer to [STM32MP15 reference manuals](#) for the complete list of features, and to the software components, introduced below, to know which features are really implemented.

2.2 Security support

RNG1 is a **secure** peripheral (under ETZPC control).

RNG2 is a **non-secure** peripheral.



3 Peripheral usage and associated software

3.1 Boot time

RNG instances are not used as boot devices.

3.2 Runtime

3.2.1 Overview

RNG instances can be allocated to:

- the Arm[®]Cortex[®]-A7 secure core to be controlled in OP-TEE with OP-TEE RNG driver
- or
- the Arm[®]Cortex[®]-A7 non-secure core to be controlled in Linux[®] by the Linux hardware random framework
- or
- the Arm[®]Cortex[®]-M4 to be controlled in STM32Cube MPU Package by STM32Cube RNG driver

Chapter #Peripheral assignment exposes which instance can be assigned to which context.

3.2.2 Software frameworks

Domain	Peripheral	Software frameworks			Comment
Cortex-A7 secure (OP-TEE)	Cortex-A7 non-secure (Linux)	Cortex-M4 (STM32Cube)			
Security	RNG	OP-TEE RNG driver	Linux hardware random framework	STM32Cube RNG 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.

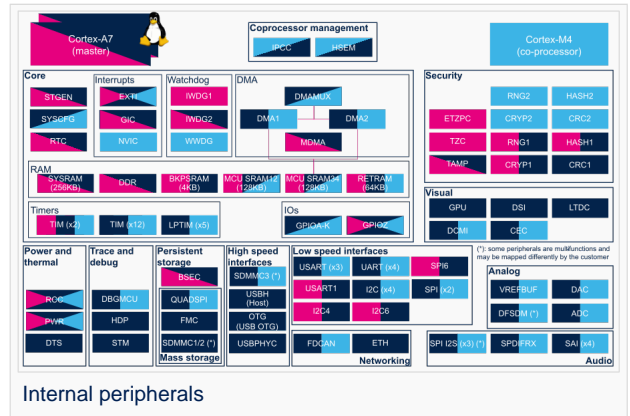
3.2.4 Peripheral assignment

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 possibilities might be described in *STM32MP15* reference manuals.



Domain	Periphera	Runtime allocation		Comment
Instance	Cortex-A7 secure (OP-TEE)	Cortex-A7 non-secure (Linux)	Cortex-M4 (STM32Cube)	
Security	RNG	RNG1		Assignment (single choice)
		RNG2		



4 How to go further

Not applicable.



5 References

Random Number Generator

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.

Microprocessor Unit

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

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

Contents

1 Article purpose	10
2 Peripheral overview	11
2.1 Features	11
2.2 Security support	11
3 Peripheral usage and associated software	12
3.1 Boot time	12
3.2 Runtime	12
3.2.1 Overview	12
3.2.2 Software frameworks	12
3.2.3 Peripheral configuration	12
3.2.4 Peripheral assignment	12
4 How to go further	14
5 References	15



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

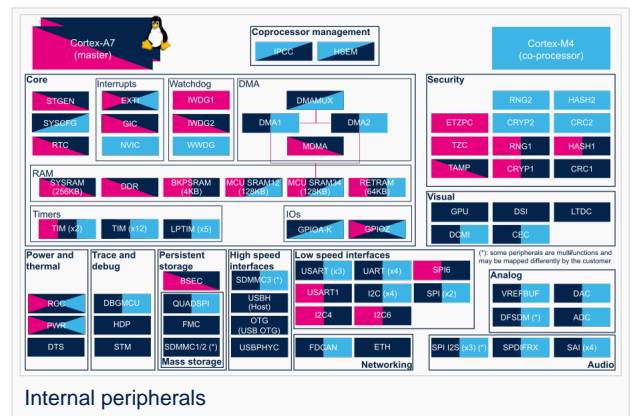
The configuration is applied by the firmware running in a secure context.

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.





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.

Domain	Periphera	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 had serial 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-access semiconductor 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.

Stable: 17.02.2021 - 19:52 / Revision: 17.02.2021 - 19:51

A quality version of this page, approved on 17 February 2021, was based off this revision.

This article gives information about the Linux® hardware random framework.

Contents

1 Article Purpose	17
2 Framework purpose	18
3 System overview	19
3.1 Component description	19
3.2 API description	20
4 Configuration	21
4.1 Kernel configuration	21
4.2 Device tree configuration	21
5 How to use the framework	22
5.1 How to use from char device	22
5.2 How to use from sysfs	22
6 How to trace and debug the framework	23
7 Source code location	24
8 To go further	25



9 References	26
--------------------	----



1 Article Purpose

This article gives information about the hardware random (HWRNG) framework.



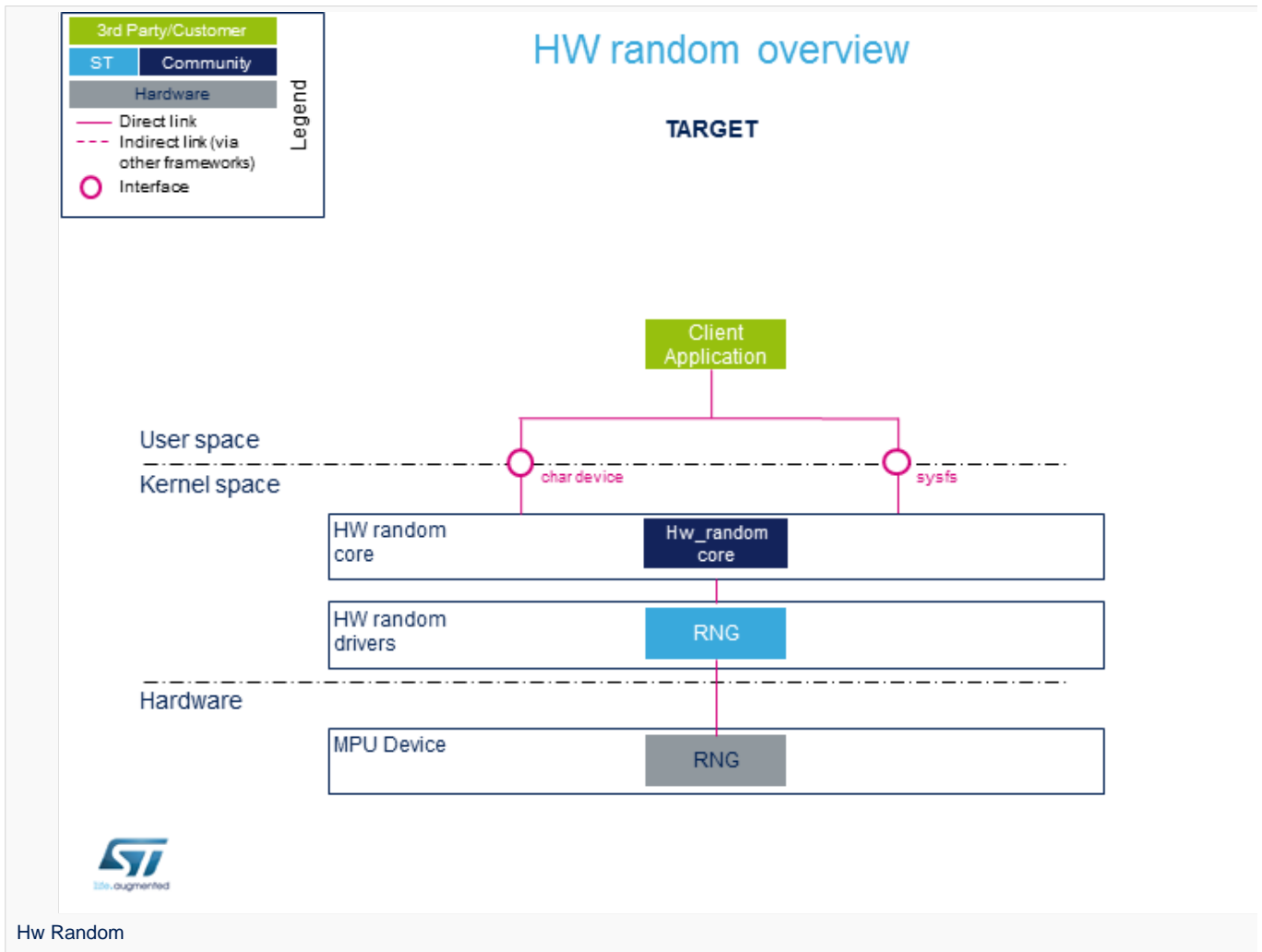
2 Framework purpose

The Hardware random framework is integrated in the kernel. It provides access to RNG peripherals and focuses on supporting the hardware number generator.



3 System overview

The HW random framework allows retrieving random numbers in userland.



3.1 Component description

- **HW random core** (Kernel space)

Generic interface in kernel space. This layer is in charge of creating the character device (char device) and sysfs to access hw_random.

- **RNG** (Kernel space)

Hardware random Linux[®] drivers handling the HW blocks.

- **RNG** (Hardware)

HW blocks handling the RNG peripheral.



3.2 API description

The Hardware random framework uses char device API^[1] ioctl operations. For additional information, refer to:

- sysfs interface.
- Kernel Documentation directory^[2]



4 Configuration

4.1 Kernel configuration

The Hardware random support is activated by default in ST deliveries. No specific configuration is required apart from enabling or disabling peripheral support using Linux® Menuconfig tool. Refer to [Menuconfig](#) or [how to configure kernel](#) and select:

```
[*] Device Drivers --->
  [*] Character devices --->
    [*] Hardware Random Number Generator Core support --->
      [*] STMicroelectronics STM32 random number generator
```

4.2 Device tree configuration

DT configuration can be done thanks to the [STM32CubeMX](#).

A detailed device tree configuration is described in [RNG device tree configuration](#).



5 How to use the framework

The framework provides external interfaces from userland : [How to control RNG](#).

5.1 How to use from char device

The community tool for using Hardware random framework is `rng_tools`^[3] which provides a complete set of utilities related to random number generators:

- **rngd**: runs a background daemon that opens `/dev/hwrng` file (default) to connect and retrieve random numbers.
- **rngtest**: runs different tests that check the entropy and verify the compliance regarding FIPS 140-2 standard.

5.2 How to use from sysfs

Available devices compatible with Hardware framework can be listed using sysfs commands:

```
Board $> cat /sys/class/misc/hw_random/rng_available  
stm32-rng
```

The selected device is shown here:

```
Board $> cat /sys/class/misc/hw_random/rng_current  
stm32-rng
```

To select a different device:

```
Board $> echo "stm32-rng"> /sys/class/misc/hw_random/rng_current
```



6 How to trace and debug the framework

Light information on the framework can be accessed by using `sysfs`.

By default, the framework does not provide any specific debug output or dynamic debugging tool.



7 Source code location

Hardware random drivers and framework are available here^[4].



8 To go further

Code examples are directly available from [rng-tools^{\[3\]}](#) github.



9 References

- <https://bootlin.com/doc/legacy/accessing-hardware/accessing-hardware.pdf>
- Documentation/admin-guide/hw_random.rst
- 3.03.1 Rng_tools source code
- drivers/char/hw_random , Hw_random sources

Linux® is a registered trademark of Linus Torvalds.

Random Number Generator

System File System (See <https://en.wikipedia.org/wiki/Sysfs> for more details)

Application programming interface

Device Tree

Stable: 16.02.2021 - 17:29 / Revision: 16.02.2021 - 17:11

A quality version of this page, approved on *16 February 2021*, was based off this revision.

Contents

1 Article purpose	27
2 Introduction	28
3 STM32CubeMX generated assignment	29
4 Manual assignment	31
4.1 TF-A	31
4.2 U-boot	31
4.3 Linux kernel	32
4.4 STM32Cube	32
4.5 OP-TEE	33



1 Article purpose

This article explains how to configure the software that assigns a peripheral to a runtime context.



2 Introduction

A peripheral can be **assigned** to a [runtime context](#) via the configuration defined in the [device tree](#). The device tree can be either generated by the [STM32CubeMX](#) tool or edited manually.

On STM32MP15 line devices, the assignment can be strengthened by a hardware mechanism: the [ETZPC internal peripheral](#), which is configured by the TF-A boot loader. The [ETZPC internal peripheral](#) isolates the peripherals for the [Cortex-A7 secure](#) or the [Cortex-M4](#) context. The peripherals assigned to the [Cortex-A7 non-secure](#) context are visible from any context, without any isolation.

The components running on the platform after TF-A execution (such as [U-Boot](#), [Linux](#), [STM32Cube](#) and [OP-TEE](#)) must have a **configuration** that is consistent with the assignment and the isolation configurations.

The following sections describe how to configure TF-A, U-Boot, Linux and STM32Cube accordingly.

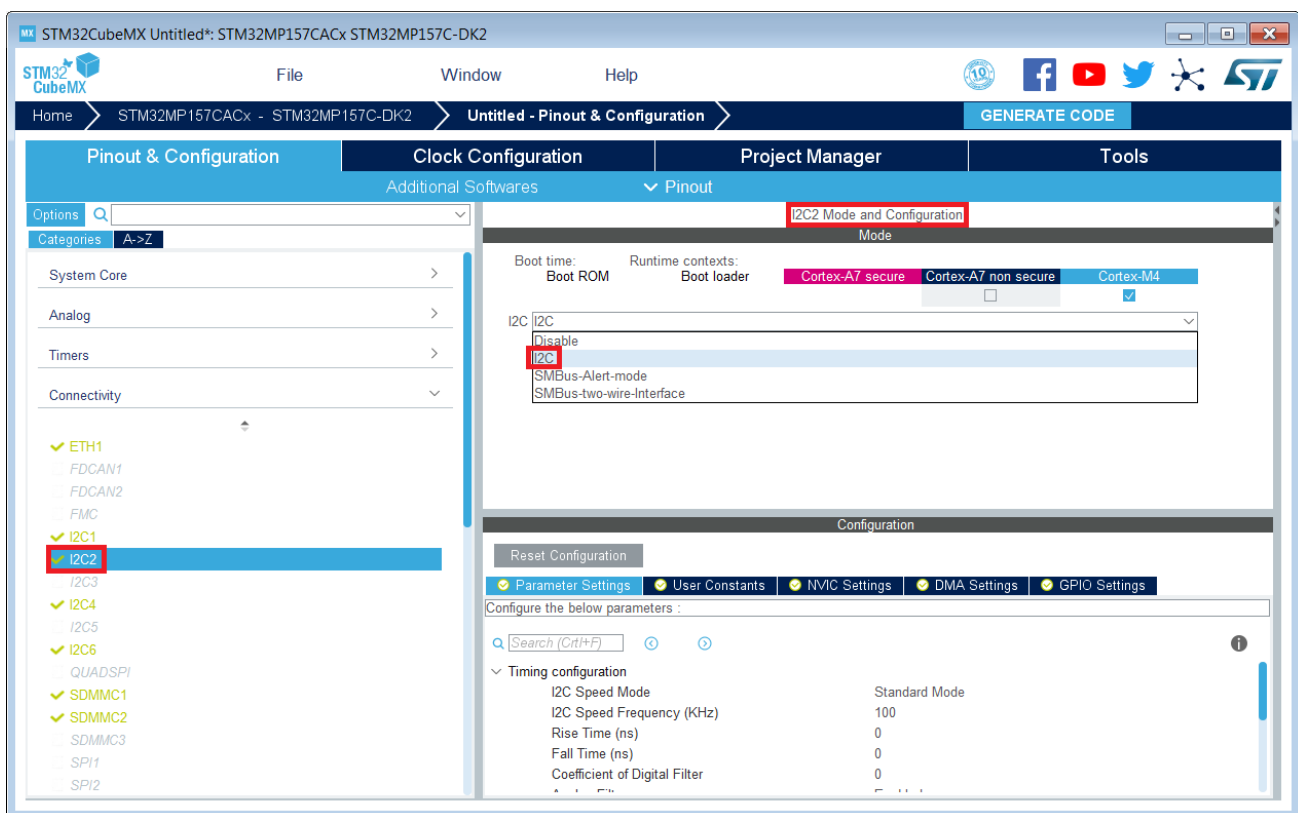
Information

Beyond the peripherals assignment, explained in this article, it is also important to understand [How to configure system resources](#) (i.e clocks, regulator, gpio,...), shared between the Cortex-A7 and Cortex-M4 contexts

3 STM32CubeMX generated assignment

The screenshot below shows the STM32CubeMX user interface:

- I2C2 peripheral is selected, on the left
- I2C2 Mode and Configuration panel, on the right, shows that this I2C instance can be assigned to the Cortex-A7 non-secure or the Cortex-M4 (that is selected) runtime context
- I2C mode is enabled in the drop down menu



Information

The context assignment table is displayed inside each peripheral **Mode and Configuration** panel but it is possible to display it for all the peripherals in the **Options** menu via the **Show contexts** option

The **GENERATE CODE** button, on the top right, produces the following:

- The **TF-A device tree** with the ETZPC configuration that isolates the I2C2 instance (in the example) for the Cortex-M4 context. This same device tree can be used by **OP-TEE**, when enabled
- The **U-Boot device tree** widely inherited from the Linux one, just below
- The **Linux kernel device tree** with the I2C node disabled for Linux and enabled for the coprocessor
- The **STM32Cube project** with I2C2 HAL initialization code

The Manual assignment section, just below, illustrates what STM32CubeMX is generating as it follows the same example.

Information



In addition of this generation, the user may have to manually complete the system resources configuration in the user sections embedded in the STM32CubeMX generated device tree. Refer to [How to configure system resources](#) for details.



4 Manual assignment

This section gives step by step instructions, per software components, to manually perform the peripherals assignments. It takes the same I2C2 example as the previous section, that showed how to use STM32CubeMX, in order to make the move from one approach to the other easier.

Information

The assignments combinations described in the [STM32MP15 peripherals overview](#) article are naturally supported by [STM32MPU Embedded Software distribution](#). Note that the [STM32MP15 reference manual](#) may describe more options that would require embedded software adaptations

4.1 TF-A

The assignment follows the ETZPC device tree configuration, with below possible values:

- **DECPROT_S_RW** for the **Cortex-A7 secure** (Secure OS like OP-TEE)
- **DECPROT_NS_RW** for the **Cortex-A7 non-secure** (Linux)
 - As stated earlier in this article, there is no hardware isolation for the Cortex-A7 non-secure so this value allows accesses from any context
- **DECPROT_MCU_ISOLATION** for the **Cortex-M4** (STM32Cube)

Example:

```
@etzpc: etzpc@5C007000 {
    st,decprot = <
        DECPROT(STM32MP1_ETZPC_I2C2_ID, DECPROT_MCU_ISOLATION, DECPROT_UNLOCK)
    >;
};
```

Information

The value **DECPROT_NS_RW** can be used with **DECPROT_LOCK** as last parameter. In Cortex-M4 context, this specific configuration allows the generation of an error in the [resource manager utility](#) while trying to use on Cortex-M4 side a peripheral that is assigned to the Cortex-A7 non-secure context. If **DECPROT_UNLOCK** is used, then the utility allows the Cortex-M4 to use a peripheral that is assigned to the Cortex-A7 non-secure context.

4.2 U-boot

No specific configuration is needed in U-Boot to configure the access to the peripheral.

Information

U-Boot does not perform any check with regards to ETZPC configuration before accessing to a peripheral. In case of inconsistency an illegal access is generated.



Information

U-Boot checks the consistency between ETZPC isolation configuration and Linux kernel device tree configuration to guarantee that Linux kernel do not access an unauthorized device. In order to avoid the access to an unauthorized device, the U-boot fixes up the Linux kernel [device tree](#) to disable the peripheral nodes which are not assigned to the Cortex-A7 non-secure context.

4.3 Linux kernel

Each assignable peripheral is declared twice in the Linux kernel device tree:

- Once in the **soc** node from `arch/arm/boot/dts/stm32mp151.dtsi` , corresponding to Linux assigned peripherals
 - Example: `i2c2`
- Once in the **m4_rproc** node from `arch/arm/boot/dts/stm32mp157-m4-srm.dtsi` , corresponding to the Cortex-M4 context.

Those nodes are disabled, by default.

- Example: `m4_i2c2`

In the board device tree file (*.dts), each assignable peripheral has to be enabled only for the context to which it is assigned, in line with TF-A configuration.

As a consequence, a peripheral assigned to the Cortex-A7 secure has both nodes disabled in the Linux device tree.

Example:

```
&i2c2 {
    status = "disabled";
};
...
&m4_i2c2 {
    status = "okay";
};
```

Information

In addition of this assignment, the user may have to complete the system resources configuration in the device tree nodes. Refer to [How to configure system resources](#) for details.

4.4 STM32Cube

There is no configuration to do on STM32Cube side regarding the assignment and isolation. Nevertheless, the [resource manager utility](#), relying on ETZPC configuration, can be used to check that the corresponding peripheral is well assigned to the Cortex-M4 before using it.

Example:

```
int main(void)
{
    ...
    /* Initialize I2C2----- */
    /* Ask the resource manager for the I2C2 resource */
    ResMgr_Init(NULL, NULL);
    if (ResMgr_Request(RESMGR_ID_I2C2, RESMGR_FLAGS_ACCESS_NORMAL | \
```




```

RESMGR_FLAGS_CPU1, 0, NULL) != RESMGR_OK)
{
    Error_Handler();
}
...
if (HAL_I2C_Init(&I2C2) != HAL_OK)
{
    Error_Handler();
}
}

```

4.5 OP-TEE

The OP-TEE OS may use STM32MP1 resources. OP-TEE STM32MP1 drivers register the device driver they intend to use in a secure context. This information is used to consolidate system configuration including secure hardening of configurable peripherals.

In most cases, the OP-TEE driver probe relies on OP-TEE device tree property *secure-status = "okay"*.

Cortex[®]

Trusted Firmware for Arm Cortex-A

Das U-Boot -- the Universal Boot Loader (see [U-Boot overview](#))

Linux[®] is a registered trademark of Linus Torvalds.

Inter-Integrated Circuit (Bi-directional 2-wire bus standard for efficient inter-IC control.)

Open Portable Trusted Execution Environment

Hardware Abstraction Layer

Operating System

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.)

Extended TrustZone Protection Controller

Stable: 13.05.2020 - 08:56 / Revision: 13.05.2020 - 08:54

A quality version of this page, approved on 13 May 2020, was based off this revision.

Contents

1 Overview of the OP-TEE open source project	35
2 Architecture	36
2.1 OP-TEE core	36
2.2 OP-TEE trusted libraries	36
2.3 TEE Linux driver	37
2.4 TEE Client API	37
2.5 TEE supplicant	37
2.6 Host tools	37
3 Booting with OP-TEE	38
4 Invoking the OP-TEE services from Linux based OS	39
5 Experiencing OP-TEE on a target	40



6 References	41
--------------------	----

1 Overview of the OP-TEE open source project

OP-TEE allows the development and integration of secure services and applications under trusted execution environments, that is execution environments isolated from the Linux[®]-based OS

Description extracted from the OP-TEE site^[1]:

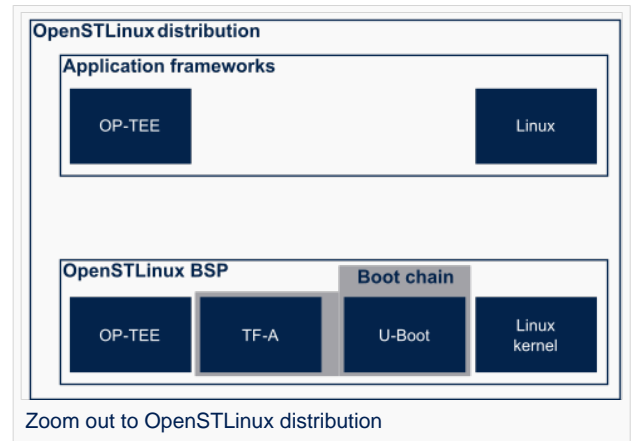
"OP-TEE is an open source project, which contains a full implementation to make up a complete Trusted Execution Environment using the ARM[®]TrustZone[®]. technology. OP-TEE meets the GlobalPlatform TEE System Architecture specification. It also provides the TEE Internal core API v1.1 as defined by the GlobalPlatform TEE Standard for the development of Trusted Applications. OP-TEE Trusted OS is accessible from the Linux based OS using the GlobalPlatform TEE Client API Specification v1.0, which also is used to trigger secure execution of applications within the TEE."

OP-TEE is delivered under a BSD style license and can run secure (trusted) applications without restriction on their licensing model.

The OP-TEE project is maintained by the Linaro Security Working Group.

- OP-TEE official site^[1]
- OP-TEE source repositories ^{[2][3][4]}
- OP-TEE documentation^[5]

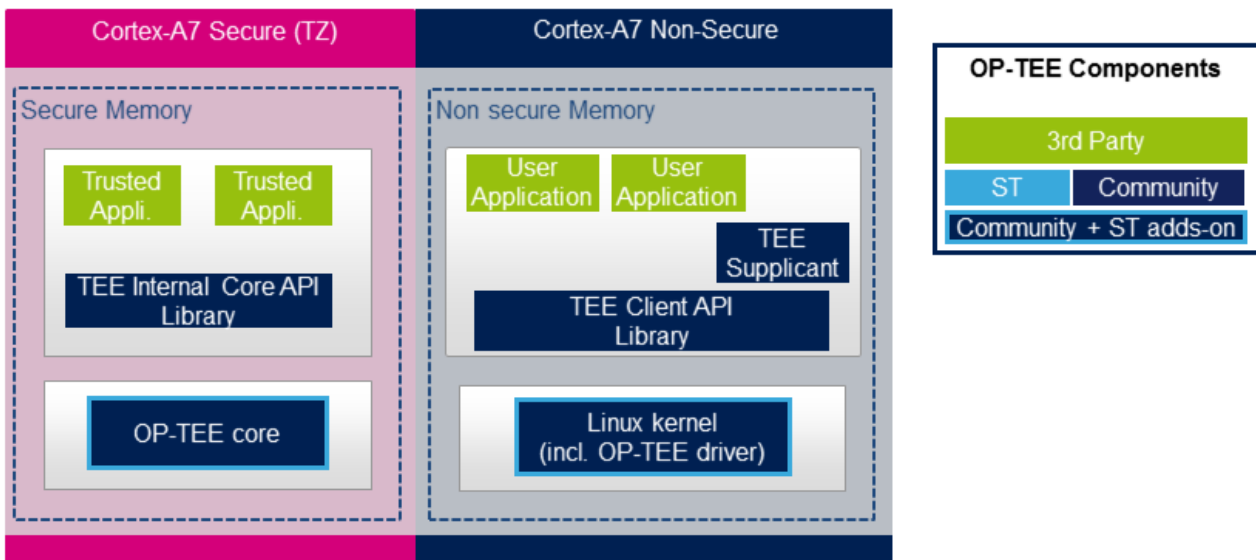
GlobalPlatform Device TEE specifications (TEE Client API, TEE Internal Core API and few more) is available from the GlobalPlatform site^[6].



2 Architecture

The OP-TEE project includes several secure and non-secure embedded components, as well as some tools for development and debugging purposes.

The figure below shows the main OP-TEE embedded components, namely the OP-TEE core and trusted application standard libraries on the secure side, and the Client API library, the OP-TEE supplicant daemon and the OP-TEE Linux kernel driver on the non-secure side.



2.1 OP-TEE core

The main OP-TEE component is the OP-TEE core. The OP-TEE core execution is done in Arm[®]Cortex[®]-A secure state while the non-secure world (likely a Linux based OS) is done in the non-secure state of the processor. The OP-TEE core executes in secure privileged (kernel) mode, while trusted applications are executed in secure user mode.

OP-TEE can load signed trusted applications stored in the Linux OS file system or embedded in the OP-TEE core boot image.

On devices with secure external memory, the OP-TEE core runs as a monolithic image in the secure memory. On devices with a small secure memory, the OP-TEE core can run in paging-on-demand configuration: a small resident agent is loaded in the small secure memory and can securely page-in/page-out data from/to the non-secure (or less secure) external memory.

OP-TEE core source files can be found from `optee_os` repository ^[2].

2.2 OP-TEE trusted libraries

OP-TEE embeds utility libraries for trusted application development including the GlobalPlatform Device TEE Internal Core API Library, which provides the standard services a trusted application can expect from the TEE. OP-TEE supports the loading of static and dynamic libraries in the TEE.

The OP-TEE standard trusted application libraries source files can be found in the `optee_os` repository ^[2].



2.3 TEE Linux driver

The OP-TEE Linux driver is part of the Linux kernel since release 4.12.

The OP-TEE Linux driver is enabled via the CONFIG_OPTEE configuration directive through the usual Linux kernel configuration means. The driver can be probed thanks to a device tree node.

2.4 TEE Client API

The OP-TEE project embeds an implementation of the GlobalPlatform Device TEE Client API specification for Linux based OS. This TEE Client API specification is partly implemented as a userland library and partly as a Linux kernel OP-TEE driver. The API allows userland clients to invoke trusted applications and the OP-TEE core services exported to non-secure world with a standard API.

The OP-TEE Client API library source files can be found in the optee_client repository^[3].

2.5 TEE supplicant

The OP-TEE core can rely on non-secure remote services. OP-TEE embeds an implementation of a non-secure userland supplicant, that can be invoked by the OP-TEE core through the OP-TEE Linux kernel driver. An example of such service is the access to a non-volatile media device that is controlled in the non-secure world.

The OP-TEE supplicant source files can be found in the optee_client repository^[3].

2.6 Host tools

The OP-TEE optee_os component, once built, generates a so-called Trusted Application Development Kit to ease the development and integration of trusted applications on a target system. The Trusted Application Development Kit includes the libraries, with their header files and makefile scripts, that allow the generation of signed trusted applications from their respective source files.

Optee_os package also provides a tool to analyse call stack backtraces in case of trusted application and/or OP-TEE core crash. Refer to script **symbolize.py** in optee_os source tree^[2].



3 Booting with OP-TEE

The OP-TEE core is a secure firmware. It must be booted prior to the non-secure world on Arm Cortex-A core(s). The secure bootloader must therefore load the OP-TEE core images in memory and run its initialization prior to executing the first booted non-secure image.

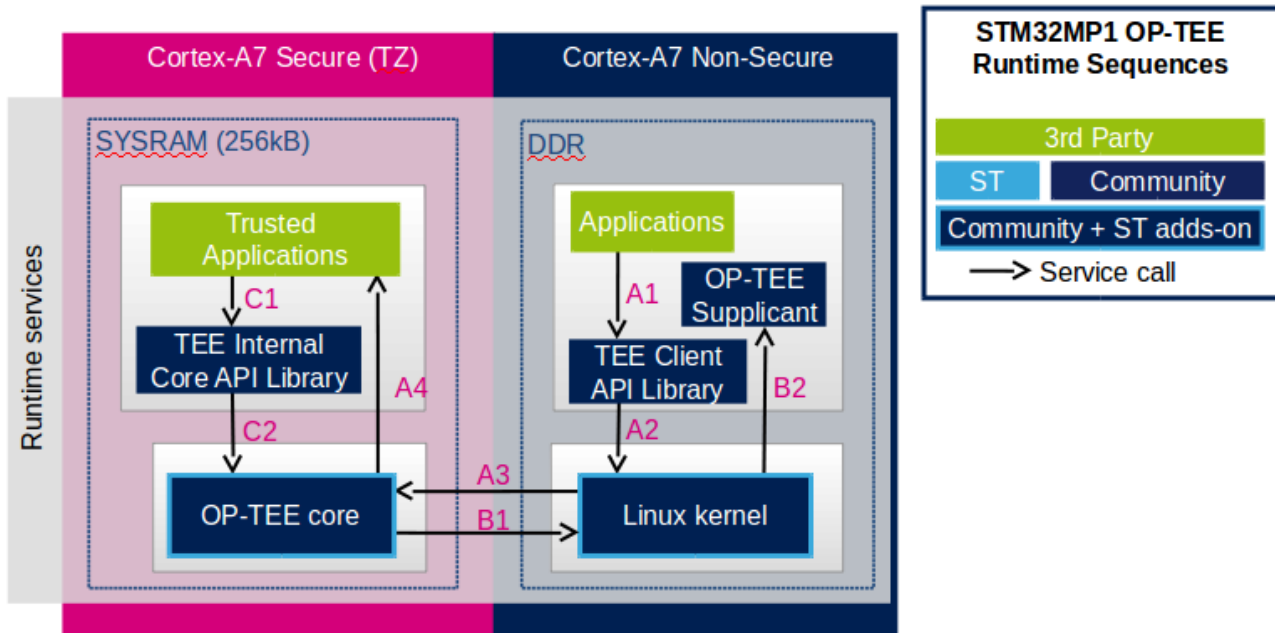
Refer to the target system boot sequences for more details.



4 Invoking the OP-TEE services from Linux based OS

Once the Linux kernel is booted, the OP-TEE core is already initialized and ready to serve.

The figure below shows the main run time sequences in which the OP-TEE can be involved.



Sequence A: an non-secure application invokes a service from a trusted application.

The non-secure application calls the TEE Client API library (**A1**), which in turns invokes (**A2**) the Linux kernel OP-TEE driver. The OP-TEE driver invokes the secure world (**A3**) and reaches the OP-TEE core. The last OP-TEE core transfers the request (**A4**) to the target trusted application. Once the trusted application has completed the request, the system branches back to the calling application with the request status.

If an invoked trusted application is not yet loaded into the TEE, the OP-TEE core loads it by calling remote services through the non-secure TEE supplicant as described in **sequence B** below.

In addition, any invocation of the TEE from the non-secure world must go through the Linux kernel OP-TEE driver.

Sequence B: the OP-TEE core must invoke a non-secure remote service.

The OP-TEE core invokes (**B1**) the Linux kernel OP-TEE driver which in turns notifies the TEE supplicant daemon (**B2**) for a request. Once the supplicant has completed the request, the system branches back to the OP-TEE core with the request status.

Sequence C: a trusted application invokes an OP-TEE core service.

Most of the services defined by the GlobaPlatform Device TEE Internal Core API must be executed in OP-TEE core privileged mode. The trusted application calls the corresponding service from the TEE Internal Core API library (**C1**), which issues a system call (**C2**) to the OP-TEE core. Once the core has completed the request, the system branches back to the calling trusted application with the request status.



5 Experiencing OP-TEE on a target

First make sure your setup includes OP-TEE in the boot sequence. If the OP-TEE core console traces are enabled, you should see the OP-TEE banner after secure bootloader traces and before non-secure bootloader traces. The OP-TEE core banner looks like this:

```
I/TC: OP-TEE version: <some-reference-version-info> #1 Mon Jun 25 08:59:21 UTC 2018 arm
I/TC: Initialized
```

The Linux kernel boot traces also show the successful probing of the OP-TEE Linux kernel driver:

```
optee: probing for conduit method from DT.
optee: initialized driver
```

The OP-TEE non-secure components are stored in the file system:

- By default the TEE supplicant is installed at `/usr/bin/tee-supPLICANT`.
- By default, the TEE Client API library is installed at `/usr/lib/teec.so`.
- By default the TEE regression test tool is installed at `/usr/bin/xtest`.

In the default OP-TEE configuration, trusted applications are stored in the non-secure filesystem at `/lib/optee_armtz/*.ta`.

OP-TEE provides means to protect the trusted application binary images from corruption as image signature or installation in the OP-TEE secure storage. In any case, it is likely that the P-TEE core needs to invoke a non-secure service to retrieve the trusted application(s) from some non-secure filesystem data in order to load trusted application(s) in the TEE. This service requires the availability of the OP-TEE supplicant.

Therefore, once the non-secure OS has booted, it must launch the OP-TEE supplicant as a background daemon. Use the following shell command to start the OP-TEE supplicant from a booted Linux system, :

```
sh> tee-supPLICANT &
```

The OP-TEE package comes with some examples and regression tests. Use the following embedded shell command to run the regression tests:

```
sh> xtest
```

or to run only selective tests:

```
sh> xtest 1002    # Invokes some OP-TEE internal core services
sh> xtest 1004    # Invokes a trusted application loaded from the non-secure filesystem
```




6 References

- 1.01.1 <https://op-tee.org>
- 2.02.12.22.3 https://github.com/OP-TEE/optee_os
- 3.03.13.2 https://github.com/OP-TEE/optee_client
- https://github.com/OP-TEE/optee_test
- <https://optee.readthedocs.io/>
- <https://globalplatform.org/>

Open Portable Trusted Execution Environment

Linux[®] is a registered trademark of Linus Torvalds.

Operating System

TrustZone[®]

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

Trusted Execution Environment

Application programming interface

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



Cortex[®]

Device Tree

Stable: 17.11.2020 - 15:37 / Revision: 03.11.2020 - 13:18

A quality version of this page, approved on 17 November 2020, was based off this revision.

Contents

1 Introduction	43
2 STM32Cube MP1 Package architecture	44
2.1 Level 0 (Drivers)	45
2.1.1 HAL drivers	45
2.1.1.1 HAL drivers overview	45
2.1.1.2 List of HAL drivers	45
2.1.2 LL drivers	46
2.1.2.1 Low Layer drivers overview	46
2.1.2.2 List of LL drivers	47
2.1.3 BSP drivers	47
2.1.3.1 BSP drivers overview	47
2.1.3.2 List of BSP drivers	47
2.2 Level 1 (Middlewares)	48
2.2.1 OpenAMP	48
2.2.2 FreeRTOS	48
2.3 Level 2 (Boards demonstrations)	49
2.4 Utilities	49
2.5 CMSIS	50



3 STM32Cube MP1 Package versus legacy STM32Cube MCU Package	53
4 References	54



1 Introduction

This article introduces **STM32Cube MP1 Package** architecture based on the Arm[®]Cortex[®]-M processor (e.g. Arm Cortex-M4)

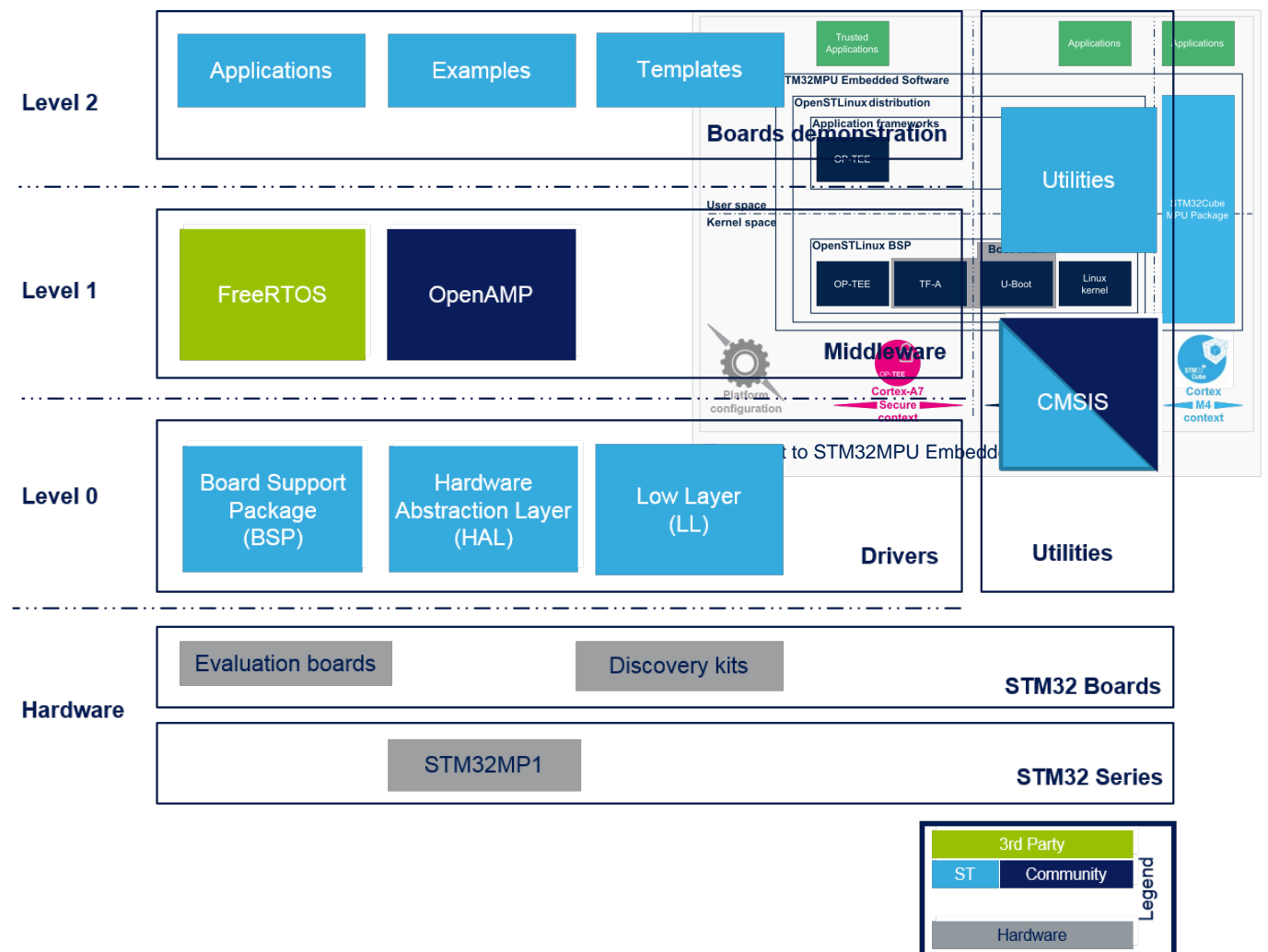
- Please refer to [STM32Cube MP1 Package](#) article to get started.



2 STM32Cube MP1 Package architecture

The **STM32Cube MP1 Package** gathers together, in a single package, all the generic embedded software components required to develop applications on top of Cortex-M microprocessors.

On top of the hardware, the **STM32Cube MP1 Package** solution is built around three levels of software components (Level 0 for Drivers, level 1 for Middlewares, Level 2 for Boards demonstrations), that interact easily with each other. It also includes 2 common components CMSIS and Utilities which interact with all three levels.



Information

Notes:

- **HAL drivers** deal with the STM32 "internal" devices: they are related to the STM32MP15 internal peripherals
- **BSP drivers** deal with the boards configuration and high-level APIs: they are the equivalent of the Linux DT mechanism (Device tree or STM32MP15 device tree) and of the Linux frameworks (Linux application frameworks overview)



2.1 Level 0 (Drivers)

This level is divided into three software components:

- **Hardware Abstraction Layer (HAL)**
- **Low Layer (LL)**
- **Board Support Package (BSP)**

2.1.1 HAL drivers

The **HAL drivers** provide the low level drivers and the hardware interfacing methods to interact with the upper layers (application, libraries and stacks). They provide generic, multi instance and function-oriented APIs which simplify user application implementation by providing ready-to-use processes.

As example, for the communication peripherals (I2C, UART...), they include APIs allowing to initialize and configure the peripheral, to manage data transfer based on polling, interrupt or DMA process, and to handle communication errors that may raise during communication.

Information

Note:

- Please refer to [STM32MP15 reference manuals](#) to get detailed information about all supported IPs of STM32MP15xx family

2.1.1.1 HAL drivers overview

The HAL APIs layer is composed of native and extended APIs set. It is directly built around a generic architecture and allows the build-upon layers, like the middleware layer, to implement its functions without in-depth knowledge about the used STM32 device. This improves the library code reusability and guarantees an easy portability on other devices and STM32 families

Contrary to the low layer drivers (see HAL Low Layer section), the HAL ones are functionality-oriented and not IP-oriented, Example: for the Timer peripheral, the APIs could be split into several categories following the functions offered by the IPs (Basic timer, capture, PWM ...etc.).

The HAL Drivers are a set of common APIs with a high compliancy level with most of the clients available on the market (stacks) called native APIs and embed also some extended functionalities for special services or a combination of several features offered by the STM32 peripherals

The HAL drivers APIs are split in two categories:

- Generic APIs which provide common and generic functions to all the STM32 Series
- Extension APIs which provide specific customized functions for a specific family or a specific part number

2.1.1.2 List of HAL drivers

Please find hereafter the list of HAL drivers available for STM32MP1xx family :

Information

Note:

- Please refer to [List of HAL Drivers](#) to get full list of delivered HAL drivers

Legend:

(HAL drivers added since ecosystem release \geq v2.1.0 )

— stm32mp1xx_hal_adc.c ADC HAL Driver



stm32mplxx_hal_adc_ex.c	ADC Extended HAL Driver
stm32mplxx_hal_cec.c	CEC HAL Driver
stm32mplxx_hal_cortex.c	CORTEX HAL Driver
stm32mplxx_hal_crc.c	CRC HAL Driver
stm32mplxx_hal_crc_ex.c	CRC Extended HAL Driver
stm32mplxx_hal_cryp.c	CRYP HAL Driver
stm32mplxx_hal_cryp_ex.c	CRYP Extended HAL Driver
stm32mplxx_hal_dac.c	DAC HAL Driver
stm32mplxx_hal_dac_ex.c	DAC Extended HAL Driver
stm32mplxx_hal_dcmi.c	DCMI HAL Driver
stm32mplxx_hal_ddsmdm.c	DFSDM HAL Driver
stm32mplxx_hal_ddsmdm_ex.c	DFSDM Extended HAL Driver
stm32mplxx_hal_dma.c	DMA HAL Driver
stm32mplxx_hal_dma_ex.c	DMA Extended HAL Driver
stm32mplxx_hal_exti.c	EXTI HAL Driver
stm32mplxx_hal_fdcan.c	FDCAN HAL Driver
stm32mplxx_hal_gpio.c	GPIO HAL Driver
stm32mplxx_hal_gpio_ex.c	GPIO Extended HAL Driver
stm32mplxx_hal_hash.c	HASH HAL Driver
stm32mplxx_hal_hash_ex.c	HASH Extended HAL Driver
stm32mplxx_hal_hsem.c	HSEM HAL Driver
stm32mplxx_hal_i2c.c	I2C HAL Driver
stm32mplxx_hal_i2c_ex.c	I2C Extended HAL Driver
stm32mplxx_hal_ipcc.c	IPCC HAL Driver
stm32mplxx_hal_lptim.c	LPTIM HAL Driver
stm32mplxx_hal_mdios.c	MDIOS HAL Driver
stm32mplxx_hal_mdma.c	MDMA HAL Driver
stm32mplxx_hal_pwr.c	PWR HAL Driver
stm32mplxx_hal_pwr_ex.c	PWR Extended HAL Driver
stm32mplxx_hal_qspi.c	QSPI HAL Driver
stm32mplxx_hal_rcc.c	RCC HAL Driver
stm32mplxx_hal_rcc_ex.c	RCC Extended HAL Driver
stm32mplxx_hal_rng.c	RNG HAL Driver
stm32mplxx_hal_rtc.c	RTC HAL Driver
stm32mplxx_hal_rtc_ex.c	RTC Extended HAL Driver
stm32mplxx_hal_sai.c	SAI HAL Driver
stm32mplxx_hal_sai_ex.c	SAI Extended HAL Driver
stm32mplxx_hal_sd.c	SD HAL Driver
stm32mplxx_hal_smartcard.c	SMARTCARD HAL Driver
stm32mplxx_hal_smartcard_ex.c	SMARTCARD Extended HAL Driver
stm32mplxx_hal_smbus.c	SMBUS HAL Driver
stm32mplxx_hal_spdifrx.c	SPDIFRX HAL Driver
stm32mplxx_hal_spi.c	SPI HAL Driver
stm32mplxx_hal_spi_ex.c	SPI Extended HAL Driver
stm32mplxx_hal_sram.c	FMC HAL Driver (for PSRAM)
stm32mplxx_hal_tim.c	TIM HAL Driver
stm32mplxx_hal_tim_ex.c	TIM Extended HAL Driver
stm32mplxx_hal_uart.c	UART HAL Driver
stm32mplxx_hal_uart_ex.c	UART Extended HAL Driver
stm32mplxx_hal_usart.c	USART HAL Driver
stm32mplxx_hal_usart_ex.c	USART Extended HAL Driver
stm32mplxx_hal_wwdg.c	WWDG HAL Driver

2.1.2 LL drivers

The **Low Layer (LL) drivers** offer a fast light-weight expert-oriented layer which is closer to the hardware than the HAL. The LL APIs are available only for a set of peripherals

2.1.2.1 Low Layer drivers overview

The Low Layer (LL) drivers are part of the STM32Cube firmware HAL that provides basic set of optimized and one-shot services. The Low layer drivers, contrary to the HAL ones are not Fully Portable across the STM32 families; the availability of some functions depends on the physical availability of the relative features on the product.



The Low Layer (LL) drivers are designed to offer the following features:

- New set of inline functions for direct and atomic register access
- One-shot operations that can be used by the HAL drivers or from application level.
- Fully independent from HAL and can be used in standalone usage (without HAL drivers)
- Full feature coverage of all the supported peripherals

2.1.2.2 List of LL drivers

Please find hereafter the list of LL drivers available for STM32MP1xx family :

Information

Note:

- Please refer to [List of LL Drivers](#) to get full list of delivered LL drivers

stm32mp1xx_ll_adc.h	ADC LL Driver
stm32mp1xx_ll_bus.h	BUS LL Driver
stm32mp1xx_ll_cortex.h	CORTEX LL Driver
stm32mp1xx_ll_dma.h	DMA LL Driver
stm32mp1xx_ll_dmamux.h	DMAMUX LL Driver
stm32mp1xx_ll_exti.h	EXTI LL Driver
stm32mp1xx_ll_gpio.h	GPIO LL Driver
stm32mp1xx_ll_hsem.h	HSEM LL Driver
stm32mp1xx_ll_i2c.h	I2C LL Driver
stm32mp1xx_ll_ipcc.h	IPCC LL Driver
stm32mp1xx_ll_lptim.h	LPTIM LL Driver
stm32mp1xx_ll_pwr.h	PWR LL Driver
stm32mp1xx_ll_rcc.h	RCC LL Driver
stm32mp1xx_ll_rtc.h	RTC LL Driver
stm32mp1xx_ll_spi.h	SPI LL Driver
stm32mp1xx_ll_sram.h	FMC LL Driver (for PSRAM)
stm32mp1xx_ll_system.h	SYSTEM LL Driver (SYSCFG & DBGMCU)
stm32mp1xx_ll_tim.h	TIM LL Driver
stm32mp1xx_ll_usart.h	USART LL Driver
stm32mp1xx_ll_utils.h	UTILITIES LL Driver
stm32mp1xx_ll_wwdg.h	WWDG LL Driver

2.1.3 BSP drivers

The **BSP drivers** are firmware components based on the HAL drivers and provide a set of APIs relative to the hardware components in the evaluation boards coming with the **STM32Cube Package**. All examples and applications given with the **STM32Cube** are based on these BSP drivers.

2.1.3.1 BSP drivers overview

The BSP architecture proposes a new model that prevents some Standard library weaknesses and provides more features:

- Portable external resources code (components): the external components could be used by all STM32 families.
- Multiple use of hardware resources without duplicated initialization: example: I2C Physical Layer could be used for several EVAL Drivers
- Intuitive functionalities based on high level use case
- Portable BSP drivers for different external devices

2.1.3.2 List of BSP drivers

The **BSP drivers** offer a set of APIs relative to the hardware components available in the hardware boards (LEDs, Buttons and COM port).



```

STM32MP15xx_DISCO
├── bumpversion.cfg
├── Release_Notes.html
├── STM32MP15xx_DISCO_BSP_User_Manual.chm
├── stm32mp15xx_disco_bus.c
├── stm32mp15xx_disco_bus.h
├── stm32mp15xx_disco.c
├── stm32mp15xx_disco_conf_template.h
├── stm32mp15xx_disco_errno.h
├── stm32mp15xx_disco.h
├── stm32mp15xx_disco_stpmic1.c
├── stm32mp15xx_disco_stpmic1.h
├── STM32MP15xx_EVAL
│   ├── bumpversion.cfg
│   ├── Release_Notes.html
│   ├── STM32MP15xx_EVAL_BSP_User_Manual.chm
│   ├── stm32mp15xx_eval_bus.c
│   ├── stm32mp15xx_eval_bus.h
│   ├── stm32mp15xx_eval.c
│   ├── stm32mp15xx_eval_conf_template.h
│   ├── stm32mp15xx_eval_errno.h
│   ├── stm32mp15xx_eval.h
│   ├── stm32mp15xx_eval_stpmic1.c
│   └── stm32mp15xx_eval_stpmic1.h

```

2.2 Level 1 (Middlewares)

Middleware components are a set of libraries providing a set of services. **STM32Cube MP1 Package** offers 2 main components : [OpenAMP](#) and [FreeRTOS](#)

Each middleware component is mainly composed of:

- Library core: this is the core of a component; it manages the main library state machine and the data flow between the several modules.
- Interface layer: the interface layer is generally used to link the component core with the lower layers like the HAL and the BSP drivers

2.2.1 OpenAMP

OpenAMP is a library implementing the Remote Processor Service framework (RPMsg) which is a messaging mechanism to communicate with a remote processor.

- Load and control Cortex[®]-M firmware
- Inter processor communication

Information

Note:

- Please refer to [Coprocesor_management_overview](#) to get more information related to coprocessor management

2.2.2 FreeRTOS

FreeRTOS is a Free Real Time Operating System (RTOS). The **FreeRTOS** offers preemptive real-time performance with optimized context switch and interrupt times, enabling fast, highly predictable response times.



It includes the following main features :

- Small memory footprint
- High portability
- Multithread management
- Pre-emptive scheduling
- Fast interrupt response
- Extensive inter-process communication
- Synchronization facilities
- Tickless operation during low-power mode
- Open source standard
- CMSIS compatibility layer

2.3 Level 2 (Boards demonstrations)

The **Boards demonstrations** level is composed of a single layer which provides all Examples and Applications. It includes also all **STM32CubeIDE** projects for each supported board as well as Templates source files.

There are 4 kinds of projects demonstrating different usages of software APIs from level 0 (Drivers) and level 1 (Middleware):

- **Examples projects** showing how to use HAL APIs and Low Layer drivers if any (Level 0) with very basic usage of BSP layer (buttons and LEDs in general)
- **Applications projects** showing how to use the middleware components (Level 1) and how to integrate them with the hardware and BSP/HAL layers (Level 0). These applications could be hybrid and use several other middleware components.
- **Demonstrations projects** showing how to integrate and run a maximum number of peripherals and Middleware stacks to showcase the product features and performance
- **Templates projects** is a really basic user application including IDE projects files, which could be used to start a custom project

Information

Notes:

- Please refer to [STM32Cube MP1 Package Overview](#) to get information on locating Examples, Applications and Demonstrations in **STM32Cube MP1 Package**
- Please refer to [List of projects](#) to get information on the list of available Examples, Applications and Demonstrations in **STM32Cube MP1 Package**

2.4 Utilities

The **Utilities** is a set of common utilities and services offered by **STM32Cube MP1 Package** and is composed of different components :

```

└─ Utilities
  └─ ResourceManager    Services for coprocessing in multi-core devices. Refer to Reso
  urce_manager_for_coprocessing
  
```



2.5 CMSIS

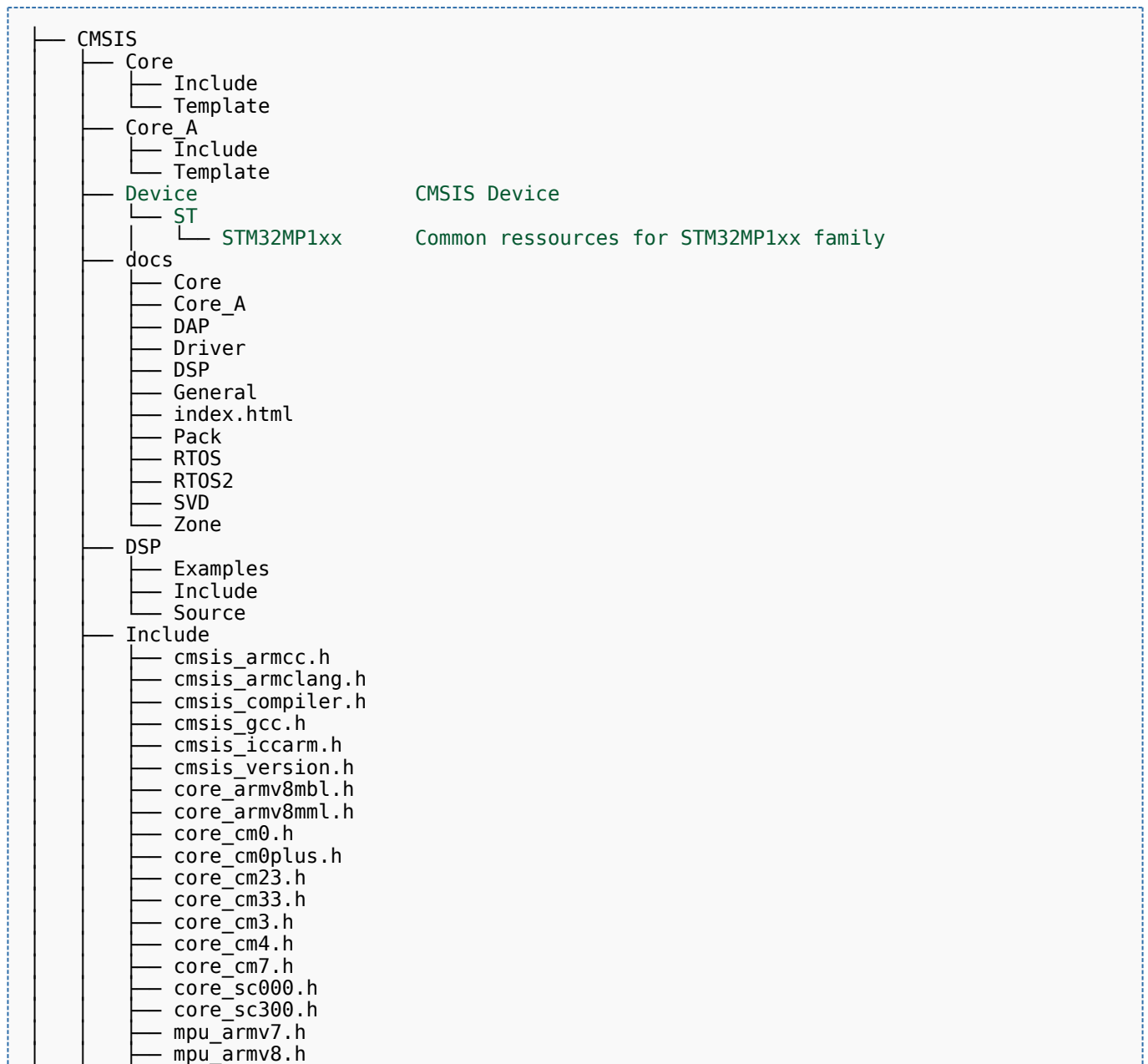
The **Cortex Microcontroller Software Interface Standard** (CMSIS) is a vendor-independent hardware abstraction layer for the Cortex-M processor series.

- Please refer to article [CMSIS](#) to get more information on CMSIS component

The CMSIS component also provides specific common resources for device support. It enables consistent and simple software interfaces to the processor and the peripherals, simplifying software re-use, reducing the learning curve for microcontroller developers, and reducing the time to market for new devices

This vendor part is called **CMSIS Device** and it provides interrupt list, peripherals registers description and associated defines for all registers bit fields.

- **CMSIS** structure overview:





3 STM32Cube MP1 Package versus legacy STM32Cube MCU Package

STM32 MPU devices introduce light differences with STM32 MCU. So please find hereafter a short description of the main differences between **STM32Cube MP1 Package** and **STM32Cube MCU Package**:

- The middleware and BSP components offered is smaller in **STM32Cube MP1 Package** as we can take advantage of a rich OS like Linux[®] running on Cortex-A core for networking, USB, visual and audio services

Information

Notes:

- All Middlewares provided by **STM32Cube MCU Package** should be compatible with MPU environment even if not provided in **STM32Cube MP1 Package** (it means they are not tested)
- All BSP components provided by **STM32Cube MCU Package** are not compatible with MPU environment as they are managed by Linux OS on main processor Cortex A
- There is no Flash HAL driver as there is no volatile embedded FLASH dedicated to Cortex-M in MPU devices
- Specific pieces of software have been added to handle multi-core operations:
 - [OpenAMP](#) middleware for Intercommunication processeur between cortex A and cortex M (RPMsg protocol implementation)
 - [Resource Manager](#) library for system resource management
 - Virtual UART driver (specific usage when Linux is used on Cortex-A)
 - Linux script to load **STM32Cube MPU** firmware running on Cortex-M core (specific usage when Linux is used on Cortex-A)

Information

Note:

- Please refer to [Getting_started_with_STM32_MPU_devices](#) article to get an overview of STM32 MPU devices



4 References

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



Cortex®

Cortex Microcontroller Software Interface Standard

Hardware Abstraction Layer

Board support package

Linux® is a registered trademark of Linus Torvalds.

Device Tree

Low layer of STM32Cube

Inter-Integrated Circuit (Bi-directional 2-wire bus standard for efficient inter-IC control.)

Universal Asynchronous Receiver/Transmitter

Direct Memory Access

Pulse Width Modulation

Analog-to-digital converter. The process of converting a sampled analog signal to a digital code that represents the amplitude of the original signal sample.

Consumer Electronics Control (HDMI standard)

Cyclic redundancy check calculation unit

Cryptographic processor

Digital-to-analog converter (Electronic circuit that converts a binary number into a continuously varying value.)

Digital Camera Memory Interface

Digital Filter for Sigma-Delta Modulator

External Interrupt

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.)

Hardware Semaphore

Inter-Processor Communication Controller

low-power timer (STM32 specific)

Reset and Clock Control

Random Number Generator

Real Time Clock

Serial Audio Interface (Mechanism used to transfer non-buffered audio data between processors and/or audio converters.)



Serial Peripheral Interface

Universal Synchronous/Asynchronous Receiver/Transmitter

System Configuration

Evaluation board

Discovery kit

Real Time Operating System

(Software)Integrated development/design/debugging environment

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.)

Microprocessor Unit

Operating System

Stable: 23.09.2020 - 13:22 / Revision: 12.06.2020 - 13:25

A quality version of this page, approved on 23 September 2020, was based off this revision.



1 STM32CubeMX overview

This article describes STM32CubeMX, an official STMicroelectronics graphical software configuration tool.

The STM32CubeMX application helps developers to use the STM32 by means of a user interface, and guides the user through to the initial configuration of a firmware project.

It provides the means to:

- configure pin assignments, the clock tree, or internal peripherals
- simulate the power consumption of the resulting project
- configure and tune DDR parameters
- generate HAL initialization code for Cortex-M4
- generate the Device Tree for a Linux kernel, TF-A and U-Boot firmware for Cortex-A7

It uses a rich library of data from the STM32 microcontroller portfolio.

The application is intended to ease the initial development phase by helping developers to select the best product in terms of features and power.



2 STM32CubeMX main features

- Peripheral and middleware parameters
Presents options specific to each supported software component
- Peripheral assignment to processors
Allows assignment of each peripheral to Cortex-A Secure, Cortex-A Non-Secure, or Cortex-M processors
- Power consumption calculator
Uses a database of typical values to estimate power consumption, DMIPS, and battery life
- Code generation
Makes code regeneration possible, while keeping user code intact
- Pinout configuration
Enables peripherals to be chosen for use, and assigns GPIO and alternate functions to pins
- Clock tree initialization
Chooses the oscillator and sets the PLL and clock dividers
- DDR tuning tool
Ensures the configuration, testing, and tuning of the MPU DDR parameters. Using U-Boot-SPL Embedded Software.



3 How to get STM32CubeMX

Please, refer to the following link [STM32CubeMX](#) to find STM32CubeMX, the Release Note, the User Manual and the product specification.

Doubledata rate (memory domain)

Hardware Abstraction Layer

Cortex®

Linux® is a registered trademark of Linus Torvalds.

Trusted Firmware for Arm Cortex-A

Das U-Boot -- the Universal Boot Loader (see [U-Boot_overview](#))

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

Stable: 17.11.2020 - 17:06 / Revision: 10.11.2020 - 07:49

A quality version of this page, approved on *17 November 2020*, was based off this revision.

All the resources for the STM32MP1 Series are located in the Resources area of the [STM32MP1 Series web page](#).

The resources below are referenced in some of the articles of this user guide.

Information

The different **STM32MP15** microprocessor **part numbers** available (with their corresponding internal peripherals, security options and packages) are described in the [STM32MP15 microprocessor part numbers](#).








means that the document (or its version) is new compared to what was delivered within the previous ecosystem release.

Reference	Name	Link	Version
Application notes			
AN4803	High-speed SI simulations using IBIS and board-level simulations using HyperLynx® SI on STM32 MCUs and MPUs	AN4803.pdf	v2.0
AN5027	Interfacing PDM digital microphones using STM32 MCUs and MPUs	AN5027.pdf	v2.0
AN5031	Getting started with STM32MP15 Series hardware development	AN5031.pdf	v2.0
		AN503	






Reference	Name	Link	Version
Application notes			
AN5036	Thermal management guidelines for STM32 applications	6.pdf	v3.0
AN5109	STM32MP1 Series using low-power modes	AN5109.pdf	 v4.0
AN5122	STM32MP1 Series DDR memory routing guidelines	AN5122.pdf	v3.0
AN5168	STM32MP1 series DDR configuration	AN5168.pdf	v1.0
AN5225	USB Type-C™ Power Delivery using STM32xx Series MCUs and STM32xxx Series MPUs	AN5225.pdf	 v3.0
AN5253	Migration of microcontroller applications from STM32F4x9 lines to STM32MP151, STM32MP153 and STM32MP157 lines microprocessor	AN5253.pdf	v1.0
AN5256	STM32MP151, STM32MP153 and STM32MP157 discrete power supply hardware integration	AN5256.pdf	v2.0
AN5260	STM32MP151/153/157 MPU lines and STPMIC1B integration on a battery powered application	AN5260.pdf	v1.0
AN5275	USB DFU/USART protocols used in STM32MP1 Series bootloaders	AN5275.pdf	v1.0
AN5284	STM32MP1 series system power consumption	AN5284.pdf	v1.0
AN5348	FDCAN peripheral on STM32 devices	AN5348.pdf	v1.0
AN5431	The STPMIC1 PCB layout guidelines	AN5431.pdf	v1.0
AN5438	STM32MP1 Series lifetime estimates	AN5438.pdf	v1.0
AN5510	Overview of the secure secret provisioning (SSP) on STM32MP1 Series	AN5510.pdf	v1.0
Datasheets^[1]			
DS12505	STM32MP157C/F datasheet (secure)	DS12505.pdf	 v4.0
DS12504	STM32MP157A/D datasheet (basic)	DS12504.pdf	 v4.0
DS12503	STM32MP153C/F datasheet (secure)	DS12503.pdf	 v4.0
	STM32MP153A/D datasheet	DS125	



Reference	Name	Link	Version
Application notes			
DS12502	(basic)	02.pdf	 v4.0
DS12501	STM32MP151C/F datasheet (secure)	DS12501.pdf	 v4.0
DS12500	STM32MP151A/D datasheet (basic)	DS12500.pdf	 v4.0
DS12792	STPMIC1 datasheet	stpmic1.pdf	 v5.0
Errata sheets			
ES0438	STM32MP15xx device errata	ES0438.pdf	v5.0
Reference manuals^[1]			
RM0436	STM32MP157 reference manual (STM32MP157xxx advanced Arm [®] -based 32-bit MPUs)	RM0436.pdf	v4.0
RM0442	STM32MP153 reference manual (STM32MP153xxx advanced Arm [®] -based 32-bit MPUs)	RM0442.pdf	v4.0
RM0441	STM32MP151 reference manual (STM32MP151xxx advanced Arm [®] -based 32-bit MPUs)	RM0441.pdf	v4.0
Boards schematics			
MB1262 schematics	STM32MP157C-EV1 motherboard schematics MB1262-C01 board schematic (Evaluation board)	MB1262-C01.pdf	v1.0
MB1263 schematics	STM32MP157C-EV1 daughterboard schematics MB1263-C01 board schematic (Evaluation board)	MB1263-C01.pdf	v1.0
 MB1263 schematics	STM32MP157F-EV1 daughterboard schematics MB1263-C04 board schematic (Evaluation board)	MB1263-C04.pdf	v4.0
MB1230 schematics	DSI 720p LCD display daughterboard schematics MB1230-C board schematic (Evaluation board)	MB1230-C.pdf	v1.1
MB1379 schematics	Camera daughterboard schematics MB1379-A01 board schematic (Evaluation board)	MB1379-A01.pdf	v1.0
MB1272 schematics	STM32MP157x-DKx motherboard schematics MB1272-DK2-C01 board schematic (Discovery kit)	MB1272-C01.pdf	v1.0



Reference	Name	Link	Version
Application notes			
MB1407 schematics	STM32MP157x-DKx daughterboard schematics MB1407-LCD-C01 board schematic (Discovery kit)	MB1407-C01.pdf	v1.0
Boards user manuals			
UM2535	STM32MP157x-EV1 evaluation board user manual	UM2535.pdf	v2.0
UM2534	STM32MP157x-DKx discovery board user manual	UM2534.pdf	v1.0
Tools user manuals			
UM2563	STM32CubeIDE installation guide	UM2563.pdf	v1.0
UM2579	Migration guide from System Workbench to STM32CubeIDE	UM2579.pdf	v1.0
UM2553	STM32CubeIDE quick start guide	UM2553.pdf	v1.0
AN5360	Getting started with projects based on the STM32MP1 Series in STM32CubeIDE	AN5360.pdf	v1.0
UM2609	Description of the integrated development environment for STM32 products	UM2609.pdf	v1.0
UM1718	STM32CubeMX user manual	UM1718.pdf	 v32.0
UM2237	STM32CubeProgrammer tool user manual	UM2237.pdf	 v12.0
UM2238	STM32 Trusted Package Creator tool user manual	UM2238.pdf	 v7.0
UM2542	STM32 Series Key Generator tool user manual	UM2542.pdf	v1.0
UM2543	STM32 Series Signing tool user manual	UM2543.pdf	v1.0

- 1.01.1 The part numbers are specified in STM32MP15 microprocessor part numbers



Archives

STM32MP15 release	ST documentation
STM32MP15-Ecosystem-v2.0.0	STM32MP15 resources - v2.0.0
STM32MP15-Ecosystem-v1.2.0	STM32MP15 resources - v1.2.0 page for the v1 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v1.1.0	STM32MP15 resources - v1.1.0 page for the v1 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v1.0.0	STM32MP15 resources - v1.0.0 page for the v1 ecosystem releases (in archived wiki)

Doubledata rate (memory domain)

USB port or connector

Microprocessor Unit

Device Firmware Upgrade

Universal Synchronous/Asynchronous Receiver/Transmitter

Printed Circuit Board

Secure Secret Provisioning

Secure secrets provisioning

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



Display Serial Interface (MIPI® Alliance standard)

Stable: 25.09.2020 - 09:15 / Revision: 25.09.2020 - 09:13

A quality version of this page, approved on 25 September 2020, was based off this revision.

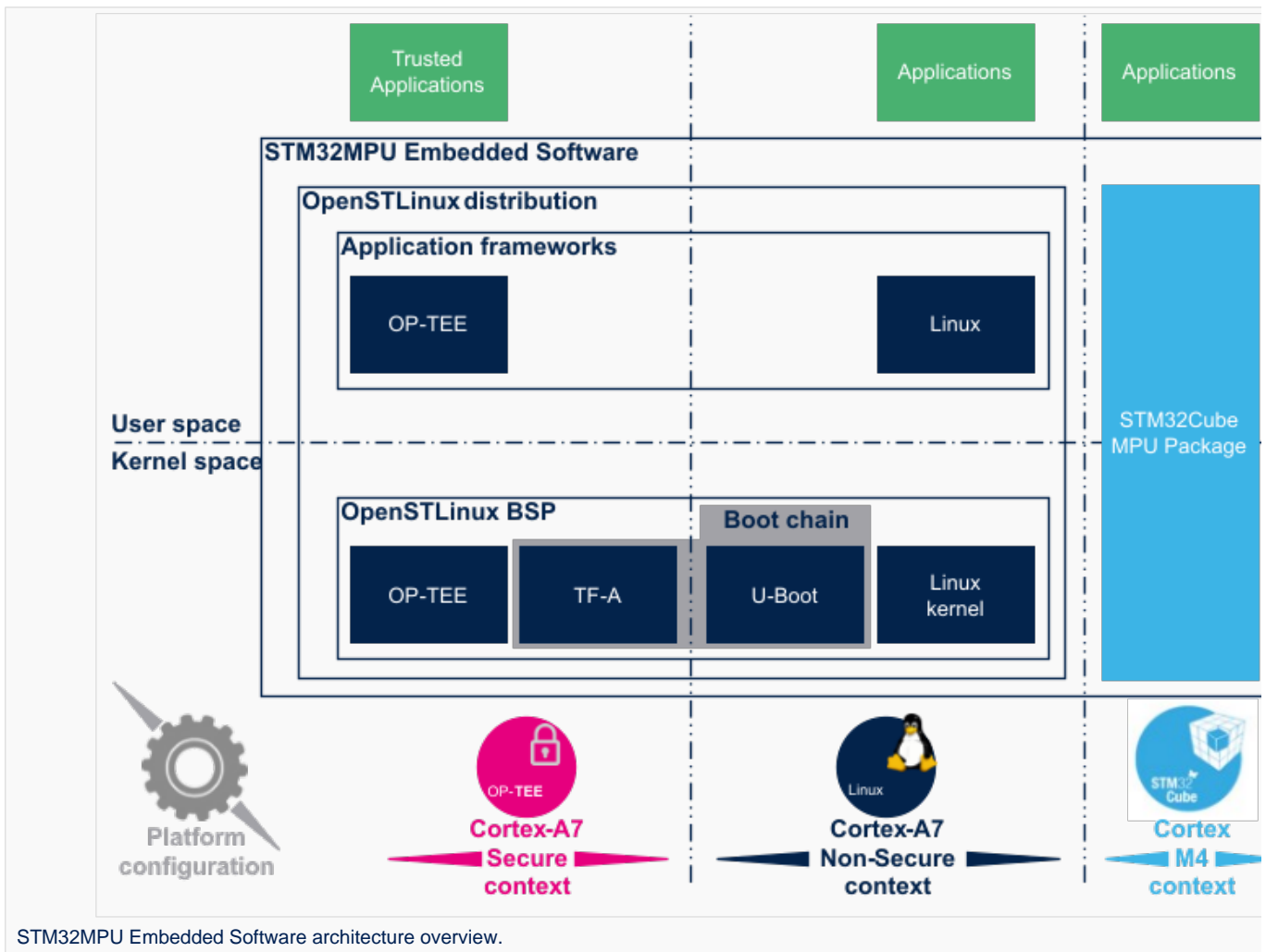


1 STM32MPU Embedded Software overview

The diagram below shows STM32MPU Embedded Software distribution main components:

- The **OpenSTLinux distribution**, running on the Arm®Cortex®-A, including:
 - The **OpenSTLinux BSP** with:
 - The **boot chain** based on TF-A and U-Boot.
 - The **OP-TEE** secure OS running on the Arm®Cortex®-A in secure mode.
 - The **Linux® kernel** running on the Arm®Cortex®-A in non-secure mode.
 - The **application frameworks** are composed of middlewares relying on the BSP and providing API:
 - on the **OP-TEE** side to run **Trusted Applications (TA)** that allow to manipulate secrets (not visible from the Linux and STM32Cube MPU Package)
 - on the **Linux** side to run **Applications** that typically interact with the user via the display, the touchscreen, etc.
- The **STM32Cube MPU Package** is running on the Arm®Cortex®-M: it is based on HAL drivers and middlewares, like other STM32 microcontrollers, completed with coprocessor management.

The figure below is clickable so that the user can directly jump to one of the sub-levels listed above.







2 Open Source Software (OSS) philosophy

The **Open source software** source code is released under a license in which the copyright holder grants users the rights to study, change and distribute the software to anyone and for any purpose^[1].

STMicroelectronics maximizes the using of open source software and contributes to those communities. Notice that, due to the software review life cycle, it can take some time before getting all developments accepted in the communities, so

STMicroelectronics can also temporarily provide some source code on github^[2], until it is merged in the targeted repository.



3 References

- https://en.wikipedia.org/wiki/Open-source_software
- STM32MP1 Distribution Package

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

Cortex[®]

Board support package

Operating System

Linux[®] is a registered trademark of Linus Torvalds.

Application programming interface

Open Portable Trusted Execution Environment

Trusted Application

Microprocessor Unit

Hardware Abstraction Layer

Open Source Software