ST Restriced – Subject to Non-Disclosure Agreement – Do not copy

STM32MP15 ecosystem release note

Contents

Stable: 18.11.2021 - v3.1.0 Revision: 18.11.2021 - v3.1.0

A quality version of this page, approved on *18 November 2021*, was based off this revision.

This article describes the content of ***STM32MP15-ecosystem-v3.1.0*** release of *STM32MPU Embedded Software distribution* and its associated ecosystem.

Contents

1 Delivery purpose and scope 4
2 Intended audience 5
3 Licensing 6
4 Main features / main highlights 7
4.1 Boards 7
4.2 Embedded software 8
4.2.1 OpenSTLinux (Cortex®-A7) 8
4.2.2 Buildroot (Cortex®-A7) 9
4.2.3 STM32CubeMP1 (Cortex®-M4) 9
4.3 STM32CubeProgrammer, Signing tool, Keygen 10
4.4 STM32CubeMX 10
4.5 STM32CubeIDE 11
4.6 Miscellaneous 11
5 Main restrictions 12
5.1 Embedded software 12
5.1.1 OpenSTLinux (Cortex®-A7) 12
5.1.2 Buildroot (Cortex®-A7) 12
5.1.3 STM32CubeMP1 (Cortex®-M4) 12
5.2 STM32CubeProgrammer, Signing tool and Keygen 12
5.3 STM32CubeMX 12
5.4 STM32CubeIDE 12
5.5 Miscellaneous 12
6 Minor release updates 14
7 Reference documents 15
8 How to download the software and start with this release? 19
9 STM32MPU Embedded Software distribution detailed release notes 20
10 Referenced tools release notes 21
11 References 22
12 Archives 23

1 Delivery purpose and scope

The STM32MP15-ecosystem-v3.1.0 release is dedicated to STM32MP15 microprocessors. It is a major release of STM32 MPU Mass Market based on new community components version (Yocto LTS Dunfell 3.1.11, Kernel 5.10.61 LTS, U-Boot v2020.10, TF-A 2.4, OP-TEE 3.12).

As for the previous releases, the STM32MP15-ecosystem-v3.1.0 aims at:

- providing a full ecosystem for the STM32MP15x devices,
- working efficiently with STM32MP15 boards, using one of the packages (Starter Package, Developer Package or Distribution Package) developed by STMicroelectronics for the STM32 MPUs.

Refer to Which Package better suits your needs for more information on these packages.

This ecosystem release consists of:

- the STM32MPU Embedded Software distribution
- STM32 referenced tools (more details are provided in the Referenced tools release notes chapter below)
  - STM32CubeIDE
  - STM32CubeMX
  - STM32CubeProgrammer
  - Keygen tool
  - Signing tool
- the Package Repository Service
  - hosted at the non-browsable URL http://packages.openstlinux.st.com
  - enabled by default in the Starter Package
  - providing regularly updated or additional packages
- Documentation
  - the present user guide in wiki format
  - the documentation package (for more details refer to Reference documents chapter below)
- Supported STM32MP15 boards
  - STM32MP15 Evaluation boards
  - STM32MP15 Discovery kits

  More details are provided in the Board chapter below.

2 Intended audience

The targeted audience is STM32MP15 customers or partners.

3 Licensing

This software package is licensed under a SOFTWARE LICENSE AGREEMENT FOR ST MATERIALS (SLA). Customers may not use this package except in compliance with the software license agreement (SLA).

4 Main features / main highlights

4.1 Boards

This STM32MP15-ecosystem-v3.1.0 release supports the same boards as STM32MP15-ecosystem-v3.0.0 ones.

Boards	PCBs list	Content	Availability
STM32MP157C-EV1 board (board with Crypto)	• MB1263C (Daughter) • MB1262C (Mother) • MB1230C (Display) • MB1379A (Camera)	• STM32MP1 STM32MP157CAA3 Rev.B • PMIC STPMIC1APQR cut1.2 • External oscillator	Jan '19
STM32MP157A-EV1 board (board without Crypto)	• MB1263C (Daughter) • MB1262C (Mother) • MB1230C (Display) • MB1379A (Camera)	• STM32MP1 STM32MP157AAA3 Rev.B • PMIC STPMIC1APQR cut1.2 • External oscillator	Jan '19
STM32MP157F-EV1 board (board with Crypto ; CPU at 800MHz)	• MB1263C (Daughter) • MB1262C (Mother) • MB1230C (Display) • MB1379A (Camera)	• STM32MP1 STM32MP157FAA3 Rev.Z • PMIC STPMIC1APQR cut2.0 • External oscillator	Jun '20
STM32MP157D-EV1 board (board without Crypto ; CPU at 800MHz)	• MB1263C (Daughter) • MB1262C (Mother) • MB1230C (Display) • MB1379A (Camera)	• STM32MP1 STM32MP157DAA3 Rev.Z • PMIC STPMIC1APQR cut2.0 • External oscillator	Nov '20
	• MB1272C (Mother)	• STM32MP1 STM32MP157CAC3 Rev.B	

Boards	PCBs list	Content	Availability
STM32MP157C-DK2 board (board with Crypto)	• MB1407B (Display)	• PMIC STPMIC1APQR cut1.2 • External oscillator	Jan '19
STM32MP157F-DK2 board (board with Crypto ; CPU at 800MHz)	• MB1272C (Mother) • MB1407B (Display)	• STM32MP1 STM32MP157FAC3 Rev.Z • PMIC STPMIC1APQR cut2.0 • External oscillator	Nov '20
STM32MP157A-DK1 board (board without Crypto)	• MB1272C (Mother)	• STM32MP1 STM32MP157AAC3 Rev.B • PMIC STPMIC1APQR cut1.2 • External oscillator	Jan '19
STM32MP157D-DK1 board (board without Crypto ; CPU at 800MHz)	• MB1272C (Mother)	• STM32MP1 STM32MP157DAC3 Rev.Z • PMIC STPMIC1APQR cut2.0 • External oscillator	Nov '20

Information

STLINK in EVAL and DISCO Rev.C boards integrates the latest firmware STLINK (V2J32M22) which requires upgraded USB PC drivers - Windows USB driver

4.2 Embedded software

4.2.1 OpenSTLinux (Cortex®-A7)

openstlinux-5.10-dunfell-mp1-21-11-17 is the new version delivered with the STM32MP15-ecosystem-v3.1.0 release. This software set consists of the following components:

- Build process
  - OpenEmbedded LTS Dunfell (v3.1.11) ***- NEW***
  - GCC version v9.3
- Software components
  - Kernel version LTS v5.10.61 ***- NEW***
  - TF-A version v2.4
  - U-Boot version v2020.10
  - OP-TEE version v3.12.0
  - OpenOCD version v0.11.0
- Applicative components
  - Weston version v8.0.0
  - GStreamer version v1.16.3

- GCnano version v6.4.3

- **Main NEW features of the STM32MP15-ecosystem-v3.1.0 release**
  - Coprocessor firmware Authentication support
  - QSPI NAND performance improvements
  - Linux KGDB support
  - DMA pause & resume support
  - stm32key command update for easy evaluation of STM32MP15 secure boot
  - Enabling LPDDR2 / LPDDR3 PHY built-in Read Valid training (RVTRN)

Warning

Basic boot has been removed since STM32MP15-ecosystem-v2.0.0, if using basic boot with U-BOOT-SPL to load U-BOOT and the Kernel, use now the ST reference boot scheme replacing U-BOOT-SPL by TF-A as FSBL as explained in Boot chain overview.

- **Internal peripheral assignment at boot time**
  - At boot time, select one of both kernel configurations:
    - Configuration 1: all internal peripherals are assigned to Cortex-A7 for Linux drivers. Cortex-M4 coprocessing firmware TTY is executed by default.
    - Configuration 2: some internal peripherals are assigned to Cortex-M4 to execute Cortex-M4 delivered examples on the board (EVAL or DISCO) see (How to run Cortex-M4 examples).

      Configuration 1 is activated by default if "2" is not specified in the U-Boot console.
      More information is available in the How to assign an internal peripheral to a runtime context article.

4.2.2 Buildroot (Cortex®-A7)

1st Buildroot distribution based on ST Linux BSP from Openstlinux-5.10-dunfell-mp1-21-11-17 is delivered with STM32MP15-ecosystem-v3.1.0 release with the tag openstlinux-5.10-buildroot-2021.02-mp1-21-11-17 on following URL [1].

4.2.3 STM32CubeMP1 (Cortex®-M4)

STM32CubeMP1-v1.5.0 version - ***NEW*** version versus STM32MP15-ecosystem-v3.0.0 release

Main NEW features of STM32CubeMP1-v1.5.0, delivered within STM32MP15-ecosystem-v3.1.0 release

- General updates to fix known defects and enhancements implementation for HAL, LL, CMSIS, BSP
- **HAL and LL Drivers**
  - Update the way to declare licenses in STM32Cube
  - **I2C, LPTIM, RNG, SPI**
    - Alignment with other STM32 families (No API change)
- **Cortex-M CMSIS**:
  - New version V5.6.0
- **OPENAMP**:
  - New version V2021.04
- **PROJECTS**:
  - Application:
    - Update openamp.c and openamp.h in application (alignment with OpenAMP Release V2021.04
    - Update OpenAMP_FreeRTOS_echo project to rely on libmetal FreeRTOS
  - All projects:
    - Update Linker script to prevent text section to override data

- Remove SW4STM32 Projects (obsolete IDE, replaced by STM32CubeIDE)

4.3 STM32CubeProgrammer, Signing tool, Keygen

STM32CubeProgrammer v2.9.0 is the new version delivered within the STM32MP15-ecosystem-v3.1.0 release. This is an evolutive maintenance release for STM32CubeProgrammer.

Main NEW features of STM32CubeProgrammer-v2.9.0, delivered within STM32MP15-ecosystem-v3.1.0 release

- Download command verifies all binaries are available before launching the programming
- Same version (v2.9) for Signing Tool, Key generator, Trusted Package Creator and STM32CubeProgrammer
- Support PKCS#11 in Signing tool

Features already available in previous STM32CubeProgrammer-v2.8.0 version

- STM32CubeProg installer including STM32CubeProgrammer, Keygen and Signing tools
- Flash programming of SD Card, eMMC, NAND, NOR images through USB and UART for STM32MP157C-EV1, STM32MP157A-EV1, STM32MP157A-DK1, STM32MP157C-DK2 boards
- Private and public key generation
- Image signatures
- Flashlayout file format change
- STM32MP1 fuse management (with console interface only)
- PMIC NVM management (with console interface only)
- SSP (Secure Secrets Provisioning) UI.

Warning

OpenSTLinux generates flashlayout files only for USB programming mode.
For UART usage, refer to Using_STM32Programmer_over_UART article to modify those files.

4.4 STM32CubeMX

STM32CubeMX-v6.4.0 is the new version delivered within STM32MP15-ecosystem-v3.1.0 release

Main NEW features of STM32CubeMX-v6.4.0, delivered within the STM32MP15-ecosystem-v3.1.0 release

- Device tree (Cortex-A7)
  - New database based on openstlinux-5.10-dunfell-mp1-21-11-17
- STM32Cube (Cortex-M4)
  - OpenAMP-2021.04 support

Features already available in previous version

- Ubuntu 20.04 support
- I/O muxing and clock tree configuration
- STM32MP1 contexts management (A7 non-secure, A7 secure, M4)
- ST32MP1Cube code generation
- Tuning of DDR settings
- Device tree code generation
  - dtsi and header file inclusions
  - pinctrl and clock generation
  - System-on-chip device node positioning
  - multi-core related configurations (ETZPC binding, resources manager binding, peripheral assignment).

- DMA config generation - DMA nodes

Information

Note: The other device tree parameters must be filled manually in user section tags (from /* USER CODE BEGIN <node> */ to /* USER CODE END <node> */)

4.5 STM32CubeIDE

STM32CubeIDE-v1.8.0 is the new version delivered within STM32MP15-ecosystem-v3.1.0 release

Main NEW features of STM32CubeIDE v1.8.0, delivered within the STM32MP15-ecosystem-v3.1.0 release

- Bootloaders target update support (TF-A, U-boot, OP-TEE)

Features already available in previous version

- Ubuntu 20.04 support
- Application and libraries userland Cortex-A7 support based on OpenSTLinux Developer Package and Yocto SDK.
- Cortex-M4 STM32CubeMP1 in "Production mode" and "Engineering mode"
- Cortex-M4 Firmware compilation, loading and debugging
- PC Linux with ethernet (recommended) or serial link
- PC Windows with ethernet or ethernet over USB link
- Cortex-M4 Firmware installation directory configurable.
- OpenSTLinux Developer Package support with
  - TF-A component project compilation with native dt selected or external dt (for example, generated from CubeMX)
  - U-BOOT component project compilation with native dt selected or external dt (for example, generated from CubeMX)
  - OP-TEE component project compilation with native dt selected or external dt (for example, generated from CubeMX)
  - KERNEL component project compilation with native dt selected or external dt (for example, generated from CubeMX)
  - KERNEL component project artefacts update on running target
  - For more information refer to How to manage OpenSTLinux projects in STM32CubeIDE article

4.6 Miscellaneous

Detailed features are available in the release notes of the different components that constitute this delivery.

See sections STM32MPU Embedded Software distribution detailed release notes, Referenced tools release notes and Reference documents

5 Main restrictions

5.1 Embedded software

5.1.1 OpenSTLinux (Cortex®-A7)

None

5.1.2 Buildroot (Cortex®-A7)

None

5.1.3 STM32CubeMP1 (Cortex®-M4)

- Use the HAL RTC with caution since this driver is also used by Linux. To remove any risk of contention between Linux and the HAL, proceed as follows:
  - The write protect (wpr) must be disabled by default and it must never be enabled in any driver (Linux nor HAL).
  - The HAL must use only Alarm B, since Linux uses Alarm A.
  - The RTC interrupt must be shared between Linux and the HAL to be able to receive alarm notifications on both sides.

5.2 STM32CubeProgrammer, Signing tool and Keygen

Warning

Key generation is functional with STM32MP_KeyGen_CLI on Linux from Ubuntu 18.04 and upper versions.

5.3 STM32CubeMX

Warning

When opening a previous project built with STM32CubeMX version older than V6.4.0, the migration does not take into account the user section part. This part needs to be updated manually according the **openstlinux-5.10-dunfell-mp1-21-11-17** manifest.

5.4 STM32CubeIDE

- Using OpenOCD with ST-LINK does not check nor force ST-LINK firmware update at debug launch. It is therefore recommended to manually update the latest ST-LINK firmware for the best debug experience. Use the Help > ST-LINK Upgrade menu".

5.5 Miscellaneous

Restriction lists are available in the sub-components release notes, which are available in the following chapters:

- STM32MPU Embedded Software distribution detailed release notes
- Referenced tools release notes

Moreover, the software workarounds implemented to provide solutions to the STM32MPU device errata are listed in STM32MP15 ecosystem errata sheet.

6 Minor release updates

STMicroelectronics regularly delivers updates through the following github® components: tf-a, u-boot, optee-os, Linux kernel. Those components can be incorporated the Developer Package (refer to STM32MP1 Developer Package) or Distribution Package.

To update the Distribution Package, proceed as follows:

1. Switch the Distribution package reference source code to github mode.
2. Use the **devtool modify <recipe name>** command to access to the git source code repository used by the build process.
3. In the freshly cloned source code, check out the required revision to start from via **git checkout -b WORK** *<github® TAG>* .

STMicroelectronics also delivers dedicated fixes on layers through github®. These changes can be integrated (via git commands: **git checkout -b WORK** *<github® commit SHA1>*) into the local STM32MP1 Distribution Package environment. The github® links corresponding to each layers in the following list:

- meta-st-stm32mp
- meta-st-openstlinux
- meta-st-stm32mp-addons

7 Reference documents

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**.

NEW 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	v3.0
AN5036	Thermal management guidelines for STM32 applications	AN5036.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	NEW v2.0
AN5225	USB Type-C™ Power Delivery using STM32xx Series MCUs and STM32xxx Series MPUs	AN5225.pdf	NEW v5.0
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
	STM32MP151/153/157 MPU lines and STPMIC1B integration on	AN526	

Reference	Name	Link	Version
Application notes			
AN5260	a battery powered application	0.pdf	v2.0
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 guidlines	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	NEW v6.0
DS12504	STM32MP157A/D datasheet (basic)	DS12504.pdf	NEW v6.0
DS12503	STM32MP153C/F datasheet (secure)	DS12503.pdf	NEW v6.0
DS12502	STM32MP153A/D datasheet (basic)	DS12502.pdf	NEW v6.0
DS12501	STM32MP151C/F datasheet (secure)	DS12501.pdf	NEW v6.0
DS12500	STM32MP151A/D datasheet (basic)	DS12500.pdf	NEW v6.0
DS12792	STPMIC1 datasheet	DS12792.pdf	NEW v8.0
Errata sheets			
ES0438	STM32MP15xx device errata	ES0438.pdf	v6.0
Reference manuals[1]			
RM0436	STM32MP157 reference manual (STM32MP157xxx advanced Arm®-based 32-bit MPUs)	RM0436.pdf	v5.0
	STM32MP153 reference manual	RM044	

Reference	Name	Link	Version
Application notes			
RM0442	(STM32MP153xxx advanced Arm®-based 32-bit MPUs)	2.pdf	v5.0
RM0441	STM32MP151 reference manual (STM32MP151xxx advanced Arm®-based 32-bit MPUs)	RM0441.pdf	v5.0
Boards schematics			
MB1262 schematics	STM32MP157C-EV1 motherboard schematics MB1262-C01 board schematic (Evaluation board)	MB1262-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
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	NEW v3.0
UM2579	Migration guide from System Workbench to STM32CubeIDE	UM2579.pdf	v1.0
UM2553	STM32CubeIDE quick start guide	UM2553.pdf	NEW v3.0
AN5360	Getting started with projects based on the STM32MP1 Series in STM32CubeIDE	AN5360.pdf	v1.0

Reference	Name	Link	Version
Application notes			
UM2609	STM32CubeIDE user guide	UM2609.pdf	NEW v5.0
UM1718	STM32CubeMX user manual	UM1718.pdf	NEW v36.0
UM2237	STM32CubeProgrammer tool user manual	UM2237.pdf	NEW v17.0
UM2238	STM32 Trusted Package Creator tool user manual	UM2238.pdf	NEW v9.0
UM2542	STM32 Series Key Generator tool user manual	UM2542.pdf	NEW v2.0
UM2543	STM32 Series Signing tool user manual	UM2543.pdf	NEW v2.0

8 How to download the software and start with this release?

The list of embedded software packages available for download depends on the selected packages.

The table below provides the available board part numbers as well as information in order to:

- get started with one of the three available Packages (Starter, Developer or Distribution Package)
- get started with the board
- find the associated embedded software distributions
- **download** source code
- **build** a piece of embedded software.

Board part number	Jump to
STM32MP157x-EV1 Evaluation board	STM32MP15 Evaluation boards - getting started, including software download
STM32MP157x-DKx Discovery kit	STM32MP15 Discovery kits - getting started, including software download

9 STM32MPU Embedded Software distribution detailed release notes

The table below lists the software packages available in the STM32MPU Embedded Software distributions, and provides the corresponding release notes.
The release notes give more information and details about the features and content of the packages.
They do not explain how to download the software. Refer to How to get the software and start with this release.

Firmware	Release note	Version
OpenSTLinux Distribution	STM32MP15 OpenSTLinux release note - v3.1.0	openstlinux-5.10-dunfell-mp1-21-11-17
Buildroot Distribution	STM32MP15 Buildroot release note - v3.1.0	openstlinux-5.10-buildroot-2021.02-mp1-21-11-17
STM32Cube MPU Package	STM32CubeMP1 Package release note - v1.5.0	STM32CubeMP1-v1.5.0

10 Referenced tools release notes

The table below lists the available tools, and provides links to the corresponding release notes.

Each release note gives information on how to install and use the corresponding tool.

The set of tools that can be downloaded depends on the package that is used (double check Which Package better suits your needs article for more information on each package).

Tools	Release notes	Host PC		Which Package may need the tool ?		
STM32MPU ecosystem v3.1.0 release	Availability on ST.com since 28 November, 2021	**Linux version**	**Windows version**	**Starter Package**	**Developer Package**	**Distribution Package**
STM32CubeIDE	STM32CubeIDE_release_note	1.8.0	1.8.0			
STM32CubeMX	STM32CubeMX release note	6.4.0	6.4.0			
STM32CubeProg	STM32CubeProgrammer release note	2.9.0	2.9.0			
Keygen	KeyGen release note	2.9.0	2.9.0			
Signing tool	Signing tool release note	2.9.0	2.9.0			

11 References

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

12 Archives

STM32MP15 release	Ecosystem release note
STM32MP15-Ecosystem-v3.0.0	STM32MP15 ecosystem release note - v3.0.0 page for the previous v3 ecosystem release
STM32MP15-Ecosystem-v2.1.0	STM32MP15 ecosystem release note - v2.1.0 page for the v2 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v2.0.0	STM32MP15 ecosystem release note - v2.0.0 page for the v2 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v1.2.0	STM32MP15 ecosystem release note - v1.2.0 page for the v1 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v1.1.0	STM32MP15 ecosystem release note - v1.1.0 page for the v1 ecosystem releases (in archived wiki)
STM32MP15-Ecosystem-v1.0.0	STM32MP15 ecosystem release note - v1.0.0 page for the v1 ecosystem releases (in archived wiki)

Microprocessor Unit

Das U-Boot -- the Universal Boot Loader (see U-Boot_overview)

Trusted Firmware for Arm® Cortex®-A

Open Portable Trusted Execution Environment

Power Management Integrated Circuit

Central processing unit

Evaluation board

Discovery kit

Cortex®

Linux® is a registered trademark of Linus Torvalds.

Direct Memory Access

Secondary Program Loader, *Also known as* ***U-Boot SPL***

First Stage Boot Loader

TeleTYpewriter

Board support package

Hardware Abstraction Layer

Low layer of STM32Cube

Cortex Microcontroller Software Interface Standard

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

low-power timer (STM32 specific)

Random Number Generator

Serial Peripheral Interface

Application programming interface

(Software)Integrated development/design/debugging environment

former spelling for e•MMC ('e' in italic)

Universal Asynchronous Receiver/Transmitter

Non Volatile Memory, like a flash memory

Secure Secret Provisioning

Secure secrets provisioning

User Interface

Doubledata rate (memory domain)

Extended TrustZone Protection Controller

Software development kit (A programming package that enables a programmer to develop applications for a specific platform.)

Real Time Clock

USB port or connector

Device Firmware Upgrade

Universal Synchronous/Asynchronous Receiver/Transmitter

Printed Circuit Board

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

Display Serial Interface (MIPI® Alliance standard)