Последовательность загрузки СнК BE-M1000

История изменений

Версия	Дата	Описание
1.0	26.07.2021	Начальная версия

Содержание

1 Введение

Документ описывает процесс начальной загрузки микропроцессора BE-M1000 и даёт краткое описание программных и аппаратных средств, участвующих в этом процессе.

Поскольку для каждой платы с микропроцессором BE-M1000 может использоваться свой вариант прошивки BIOS, процесс начальной загрузки может быть уникальным для каждого типа платы. Данный документ описывает процесс начальной загрузки для материнской платы MBM1.0 (форм-фактор mini-ITX), которая была спроектирована при участии компании «Т-Платформы».

2 Используемые при загрузке аппаратные модули

В процессе начальной загрузки микропроцессора участвуют следующие аппаратные модули:

- *System Control Processor* (**SCP**) – управляющий процессор Модуля Управления Системой
- *Application Processor* (**AP**) – любое из 8 ядер Arm® Cortex-A57
- `system_flash` - микросхема энергонезависимой внешней SPI FLASH памяти, подключенной к интерфейсу Boot SPI (SPI0, имена контактов - `SPI0_*`)

3 Процесс начальной загрузки BE-M1000

3.1 Запуск СнК BE-M1000

Модуль управления системой BE-M1000 имеет один входной синхросигнал с референсной частотой 25 MHz (контакт `CLK25M`) и один входной сигнал сброса-установки с активным низким уровнем (контакт `RESET_N`).

Запуск производится в следующем порядке:

1. Подается и устанавливается рабочий уровень напряжения питания;
2. В произвольном порядке:
    - подаётся опорная частота `CLK25M`

- выставляется активным сигнал сброса RESET_N

3. Снятие RESET_N производится не менее чем через 1 микросекунду после стабилизации поданной опорной частоты CLK25M;
4. Запускается бортовой конечный автомат, который автоматически:
   a. выводит кристалл в рабочее состояние
   b. производит запуск блока первичной SCP загрузки.

3.2 Последовательность загрузки

В общем случае загрузка BE-M1000 производится в следующей последовательности:

1. Загрузка начинается со старта SCP и исполнения на нем неизменяемого первичного SCP загрузчика, размещенного в SCP ROM.
2. После исполнения этого кода производится загрузка программного раздела вторичного SCP загрузчика из внешней system_flash.
3. Вторичный SCP загрузчик проводит конфигурирование BE-M1000 и включение его отдельных компонент.
4. После этого вторичный SCP загрузчик производит загрузку стартового кода для AP. Этот код может быть прочитан либо из system_flash через Boot SPI контроллер, либо через любой другой периферийный контроллер, в том числе и из пространства AP.
5. После загрузки стартового кода для AP производится запуск AP (одного из ядер Cortex-A57).
6. Далее на AP запускается первичный AP загрузчик, который выполняет первичную инициализацию AP, проверяет и загружает вторичный AP загрузчик из SPI (SRAM) в DRAM, после чего передает управление вторичному AP загрузчику.
7. Вторичный AP загрузчик производит дополнительную инициализацию AP, проверяет и загружает образы ARM Trusted Firmware (EL3 runtime) и Secure payload, S-EL1/0 (TEE) из SPI (SRAM) в DRAM, после чего возвращает управление первичному AP загрузчику.
8. Первичный AP загрузчик производит необходимые действия и передает управление ARM Trusted Firmware (EL3 runtime) на уровне EL3.
9. ARM Trusted Firmware (EL3 runtime) производит необходимые действия и передает управление Secure payload, S-EL1/0 (TEE).
10. Secure payload, S-EL1/0 (TEE) производит необходимые действия и передает управление UEFI tianocore, который загружает основную операционную систему.

3.3 Управление тактовой частотой SCP во время загрузки

В зависимости от уровня сигнала на контакте TURBO_BOOT микропроцессора, SCP запускается на частоте 500 МГц в режиме 0 (TURBO) или на частоте 250 МГц в режиме 1.

Примечание: Уровень сигнала на контакте TURBO_BOOT определяет тактовую частоту SCP только на период начальной загрузки BE-M1000 и не влияет на скорость дальнейшей работы системы.