# M-Mode

20 марта 2025 г.

В любой момент времени hart (a.k.a. hardware thread - физическое ядро на процессоре) исполняется в каком-то привилегированном режиме. На данный момент в RISC-V определено 3 режима:

| Уровень | Кодировка | Имя | Аббревиатура |
|---|---|---|---|
| 0 | 00 | User | U |
| 1 | 01 | Supervisor | S |
| 2 | 10 | Reserved | |
| 3 | 11 | Machine | M |

Привилегированные режимы существуют для предоставления безопасности между компонентами системы. Попытки исполнения нелегальных для конкретного режима операций приводят к возникновению исключений, которые обрабатываются в состояниях с высшими привилегиями.

CSR - control and status register, регистры, которые отвечают за состояние системы. M-Mode может использовать любые CSR и ассоциированные с ними инструкции. Крайне важными для Machine Mode можно выделить следующие регистры:

- mstatus - отвечает за состояние ядра. Содержит в себе множество битов-статусов, определяющий контекст исполнения, например, режим, из которого мы только вернулись (MPP биты).
- mie/mip - маскируют пилингующиеся и доступные прерывания. Если i-ый бит в маске установлен, значит сработало i-ое прерывание/i-ое прерывание включено
- mcause - первый бит регистра показывает, что провал в M-Mode был вызван либо прерыванием, либо исключением, остальные - номер прерывания.
- mepc - адрес возврата после прерывания.
- mtvec - регистр, содержащий адрес таблицы прерываний.
- mtime/mtimecmp - регистры, отвечающие за время. mtime во времени увеличивается на константное значение. Когда mtime становится больше установленного mtimecmp происходит прерывание, если установлен бит MTIE в регистре mie.

Привилегированные режимы общаются с помощью ECALL'ов. Каждый привилегированный режим создаёт свой уникальный interrupt, по которому можно понять, откуда идёт запрос.

В случае, когда мы ожидаем определённого действия, в M-Mode можно воспользоваться инструкцией WFI - wait for interrupt. Она останавливает исполнение кода до появления прерывания. Причём WFI можно пользоваться, когда прерывания выключены, т.е. WFI смотрит на пилингующие прерывания в mie, независимо от того, включены ли они в mip. Существуют особенные NMI(Non-Maskable Interrupt) прерывания, вызываемые железом. Такие прерывания полностью игнорируют состояния CSR регистров и переходят в обработчики соответствующей прерыванию функции.

При перезагрузке (reset), режим исполнения ядра устанавливается в M-Mode. В процессе инициализации работы hart'а происходит заполнение CSR'ов определёнными значениями - например, misa выставляет максимальный набор доступных расширений, а pc устанавливается на заранее известное место в памяти. Причина reset'а будет располагаться в регистре mcause, что позволяет написать обработчики конкретных случаев перезагрузки.

PMA - не только про хорошее настроение. PMA отвечает за менеджмент памяти - Physical Memory Attributes. Какие-то области в памяти не обладают возможностью к чтению, какие-то к исполнению, существуют области, в которых неисполнимы атомики. Соединение виртуальная-физическая память реализуется в M-Mode с помощью специальных pmpcfg и pmpaddr регистров. Правила для i-ой области памяти

лежат в однобайтовой ячейке памяти pmp_i_cfg, а адрес соответствующей области лежит в полноценном регистре pmpaddr_i. pmp_i_cfg сгруппированы в одни цельные регистры pmpcfg_i. Так, например, в pmpcfg_0 для RV32 будут лежать конфигурации для первых 4 (pmp0cfg, pmp1cfg, pmp2cfg, pmp3cfg) областей памяти, которым будут соответствовать 4 регистра pmpaddr0, pmpaddr1, pmpaddr2, pmpaddr3.

Память имеется 3х видов - main memory, I/O devices и vacant. Main memory обязана обладать определёнными свойствами, в то время как конкретных требований для I/O - нет, например, I/O память может быть неидемпотентной. Главная память обязана:

- поддерживать чтение и запись любой ширины, которую могут потребуют присоединённые девайсы;
- LR/SC инструкции для работы с атомиками, а так же работа с положенными не по смещению атомиками;
- используемая определённым hart'ом область памяти должна быть видна всем остальным hart'ам, так же как и всем девайсам;
- идемпотентность.

Итак, M-Mode отвечает за обработку исключений и прерываний, общение с периферией, инициализацию ресурсов приложениям, охрану памяти от некорректного использования, установление состояние после перезагрузки. Иными словами - предоставление интерфейсов общения между высокоуровневыми и низкоуровневыми компонентами системы и её гарантии безопасности.