操作系统的状态机模型.

Bare-metal与程序员的约定

- CPU reset后,处理器处于某个确定的状态
  - PC指针一般指向一段memory-mapped ROM
    ROM存储了厂商提供的firmware(固件)
  - 处理器的大部分特性处于关闭状态
    缓存、虚拟存储.
- Firmware(固件,厂商提供的代码)
  - 将用户数据加载到内存
    例如存储介质上的第二级loader(加载器)
    或者直接加载操作系统(嵌入式系统)

鸡和蛋的问题的解决

- 代码直接存在于硬件里
- CPU reset后Firmware会执行.
  - 加载512字节到内存 然后功成身退

Firmware的另一用处

- 放置一些绝对安全的代码
  - BIOS中断
  - ARM Trusted Firmware

Firmware和boot loader共同完成操作系统的加载

- 初始化全局变量和栈;分配堆区.
- 为main函数传递参数

Abstract Machine

TRM(Turing Machine) + MPE(Multi-Processor Extension)

- 完全等同于多线程(处理器相当于线程)
- IOE(I/O Extension):完全是普通的库函数
  - 同一设备的数据竞争 = undefined behavior

CTE(Context Extension)

- 允许创建多个执行流(类比协程)
- yield主动切换;会被中断被动打断.
- on_interrupt会拦截到中断事件

VME(Virtual Memory Extension)

- 允许创建一个"经过地址翻译的执行模式"
- 通过CET API管理