# 嵌入式系统内容

- 可靠
- 安全

# 嵌入式系统概论

- 嵌入式系统安全 = 安全 + 可靠
- 最主要的特征

  > 可裁剪

- 书上的细节是某一个芯片的手册
- 一定要了解体系结构(冯诺依曼、哈佛、超哈佛)差异
- 指令集差异和特点
  - 嵌入式一般使用精简指令集

    > 复杂指令集出错时PC指针可能指向操作数；RISC永远是指向完整的指令

- 最重要的认证
  - 安全认证

    > 例如国内的3C

  - 电磁兼容性
- 操作系统不是必须的
  - 带来了不确定性、不可测试性；降低了可靠性
  - 只有不得已才使用操作系统
- 常用不挥发存储器(ROM/Flash/OTP/EEPROM)
  - 基本差异、开销、功耗、成本、可靠性
  - Flash 以页为单位

    > 时间长、出错概率高

  - EEPROM 以一个字节(大部分)/二进制为单位

    > 可靠性较Flash高

- 振荡器
- 复位
  - 时长和振荡器的频率相关
  - 了解不同的复位之间的关系

- 有时候为了可靠性需要降低频率
- 死机
    - CPU仍在运行但没有按照预期运行
- WDT的工作原理、分类
    - 硬件WDT + 软件WDT
- 冷热复位
- 端口输出差异
    - 推挽输出
        - 功耗大、驱动能力大、信号快
        - 板间
    - OC/OD输出
        - 板内
- Cortex
    - 命名规则
    - M3 架构、特权模式、合法模式转换、中断和异常机制
    - Thumb和ARM指令集的主要区别
    - 安全处理器的主要措施
    - 大小端、主存辅存
- 接口
    - UERT
        - RS232、RS485区别
        - 重点关注**串口注意事项(P16)**
    - I2C
        - 多主控、两根信号线必须OC开漏
    - SPI
        - 时序由从设备决定
        - 单总线(不需要具体了解)
    - 晶体管
        - 功率因素?
    - 继电器
        - 步进电机节拍、失步
        - BLDC马达加载时序
- 嵌入式软件设计
    - 适合的好
- 难以测试最坏的情况
    - 例如中断溢出
    - 不了解库函数堆栈空间的使用时慎用

    - 较为简单的嵌入式任务中通常使用全局变量
        - 全局变量直接寻址
        - 局部变量会使得速度变慢，空间增加

- 侧信道攻击的基本方法和防御方法
- TrustZone
    - 通过边界寄存器控制范围(开放和安全的空间)
- 追求基本概念，不要太细节
- GP的概念、功能、不同角色的责任、主要安全通道协议种类、统筹考虑、错误注入攻击、功耗攻击、时间攻击的概念和主要防范方法、TEE、安全审计等(见PPT)
- cos和soc
    - cos

        > chip operating system(芯片操作系统)，一般指智能卡、USB-KEY等安全产品的操作系统

    - soc

        > system on a chip(片上系统)