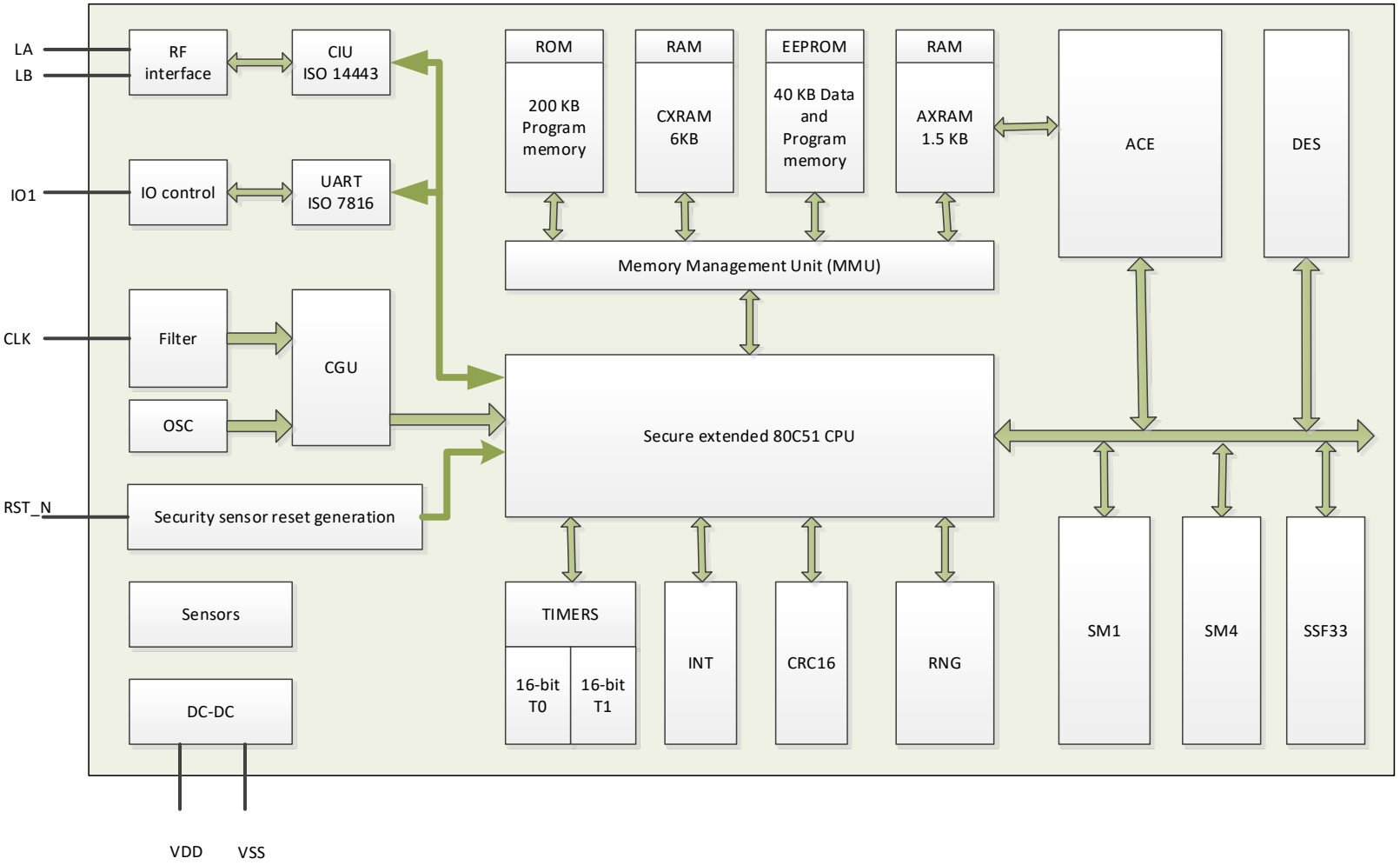
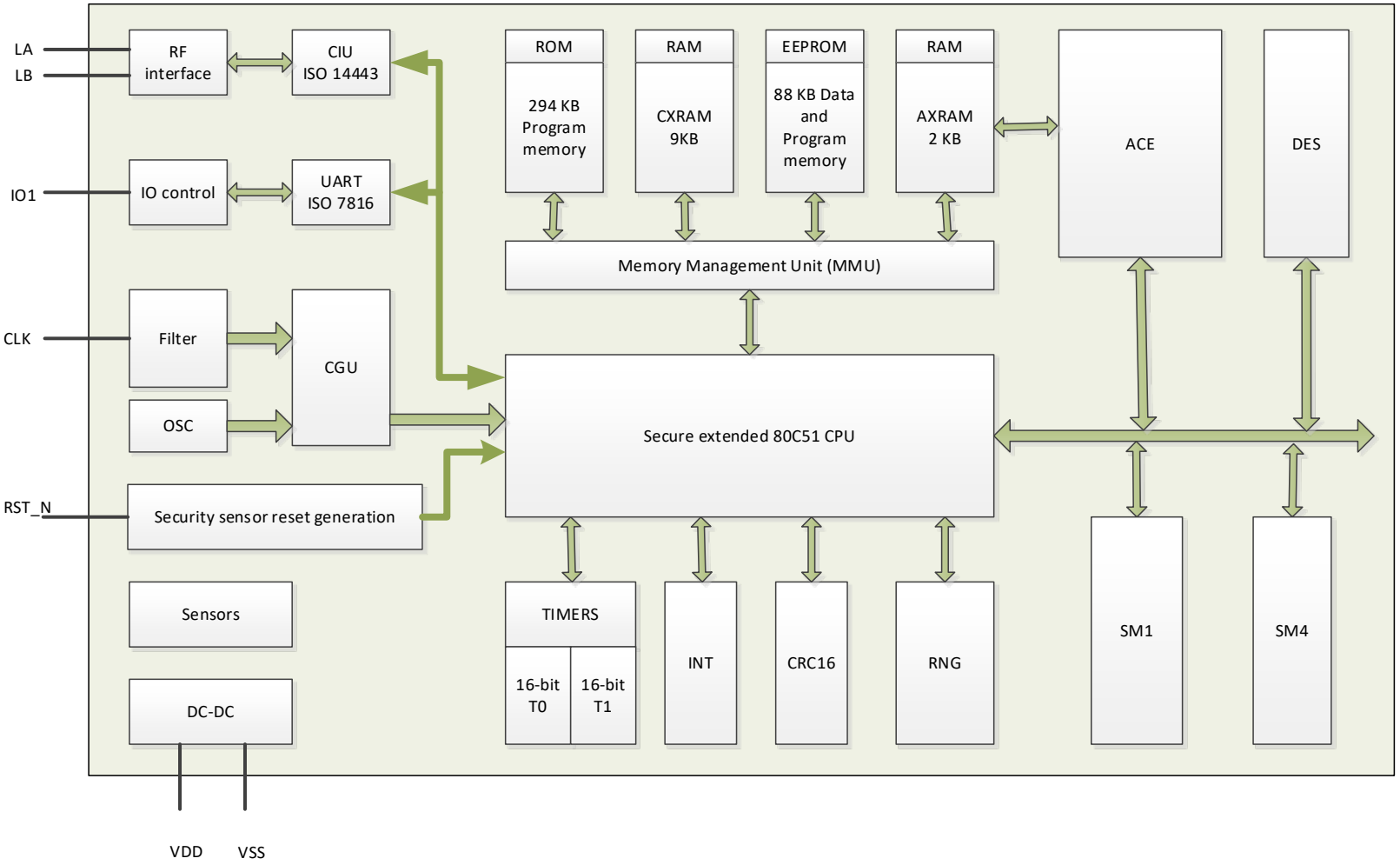
基于8051处理器的CVF安全芯片

芯片组成-CVF1040D



芯片组成-CVF1088D



技术指标-整体技术指标

- 使用台积电 CMOS 14-1P5M和ROM掩膜工艺；
- CVF1040D容量为200KB ROM、40KB EEPROM、7.5KB RAM；
- **CVF1088D容量为294KB ROM、88KB EEPROM、11KB RAM；**
- **扩展80C51的低功耗安全处理架构，最高**时钟频率72MHz；
- 采用32位高性能、低功耗算法加速协处理器，**最高时钟频率72MHz**；
- 支持32个外部中断源，4级中断优先级；
- **支持硬件补丁机制；**
- **同时支持接触界面和可选触的非接界面。**

技术指标-电气特性和通讯接口

- 支持低功耗模式：自动打盹模式、休眠模式、IDLE模式
- 供电电压：1.62V-5.5V， 内核电压：1.8V
- 典型功耗：12mW， 支持低功耗模式，最低功耗小于30uA
- 典型工作电流：12mA @ 36MHz
- 最大工作电流：32mA @ 36MHz
- 工作温度：-25℃ ~ +85℃
- ESD保护：4000V以上
- 支持ISO/IEC 7816接口，接口时钟频率为1-12MHz
- 支持ISO/IEC 14443 Type A/B射频协议，波特率106K/212K/424K/848Kbps，正常工作场强范围1.5A/m~7.5A/m

技术指标-安全性功能指标

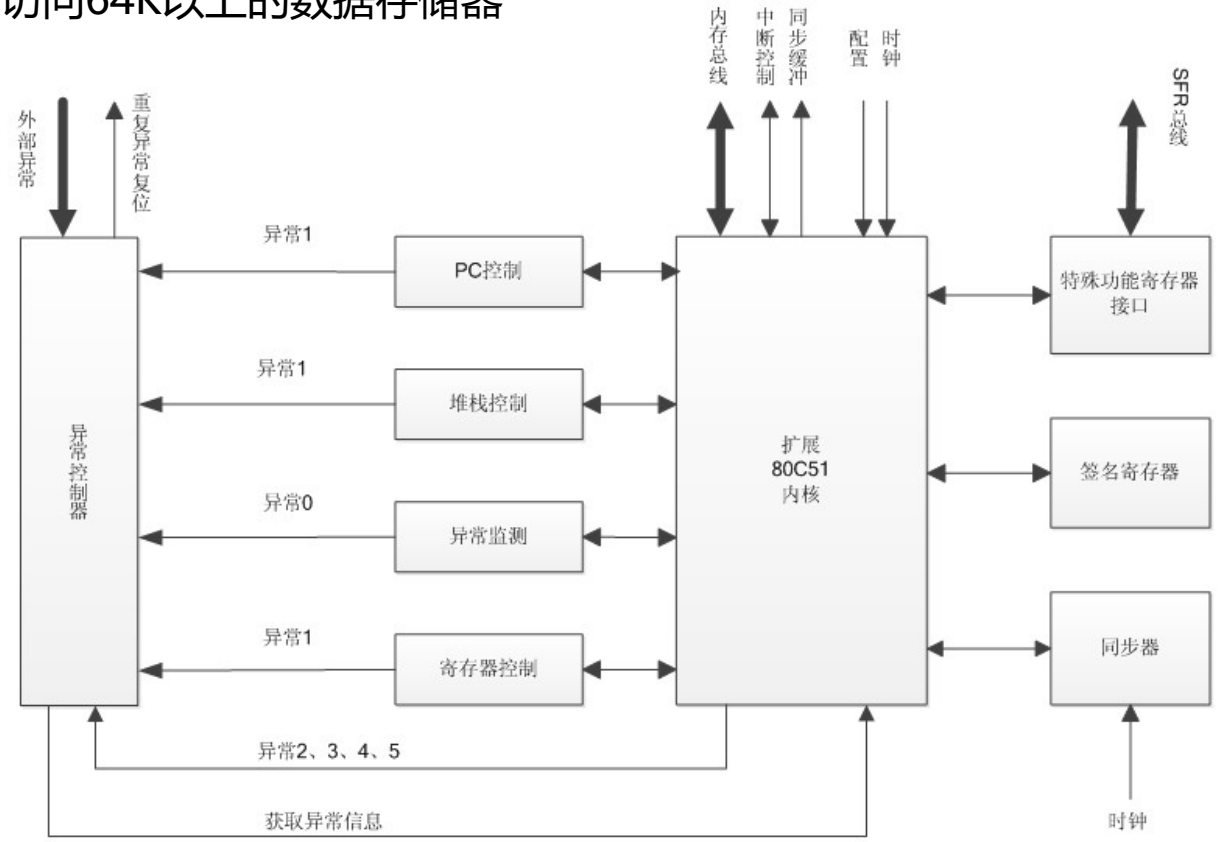
- SM2算法、RSA2048算法、SM3算法使用软硬协同实现：
- 硬件采用高级加密引擎ACE，ACE支持大数（2048比特）模乘、模幂、乘法运算协处理；
- 软件由安全算法库完成，并由安全算法库提供用户接口；
- SM2密码算法模块：支持签名和验证、密钥生成；
- RSA2048密码算法模块：支持签名和验证、密钥生成。
- SM1、SM4和SSF33密码算法支持ECB模式，加解密由硬件完成，通过安全算法库提供用户接口。
- 真随机数发生器遵循国密局《随机性检测规范》技术要求。

安全特性

- 安全检测与防护单元：高低电压检测、高低频率检测、高低温检测、光照检测、电源毛刺检测
- 超级用户模式、系统模式、用户模式三级安全机制，采用独立寄存器组
- 独立的电源模块、内部时钟模块和内部复位逻辑
- 主动防护层检测
- 安全存储分区和存储区访问控制
- 存储区加密、校验
- 总线加扰、CPU时钟加扰
- 异常中断日志存储
- 运行时数据签名
- 安全固件输入参数检查
- 过程检查、 随机延时
- 关键路径检查、处理分支消除
- 密钥导入随机化、 RAM随机化

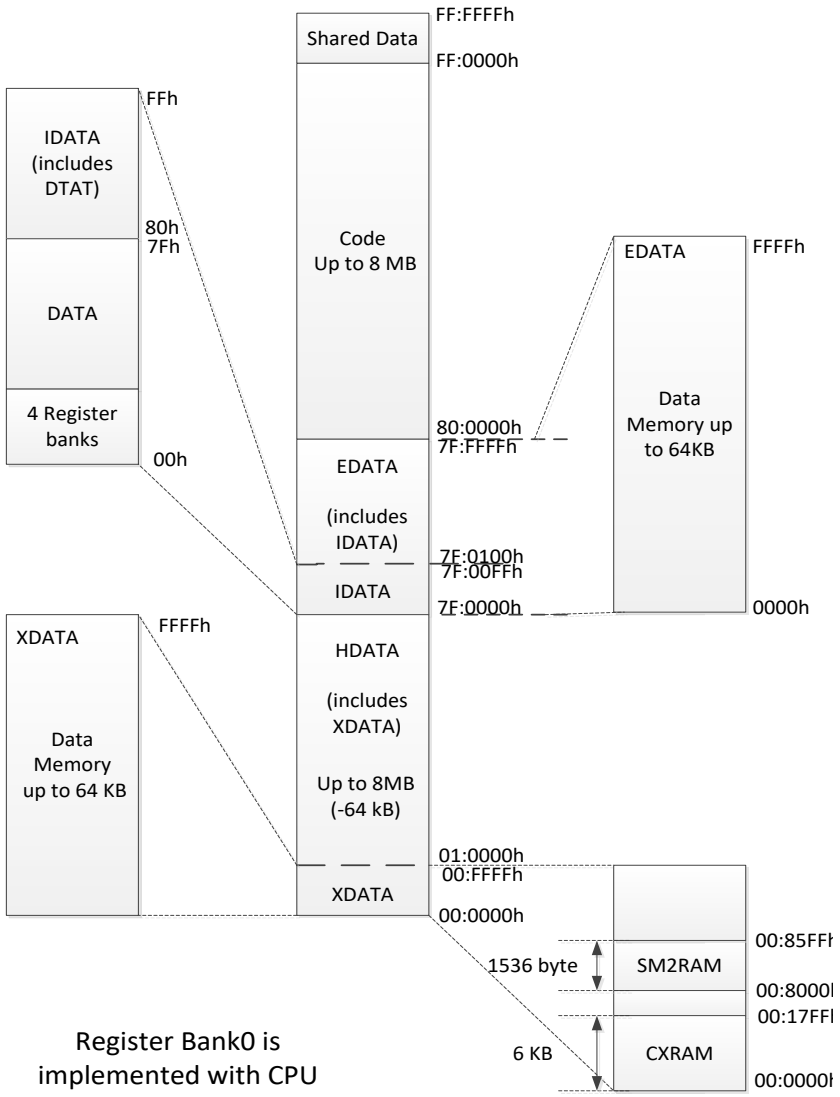
CPU

- **增加新的寻址模型，支持对所有除SFR外数据和代码区的单指令访问**
- **增加两个独立可选的堆栈模式，压栈地址可扩展到24位，支持栈空间可扩展**
- 新增24位数据指针，以方便访问64K以上的数据存储器
- **程序指针扩展到24位**



- 三种工作模式
  - 超级系统模式
  - 系统模式
  - 用户模式

存储器映射



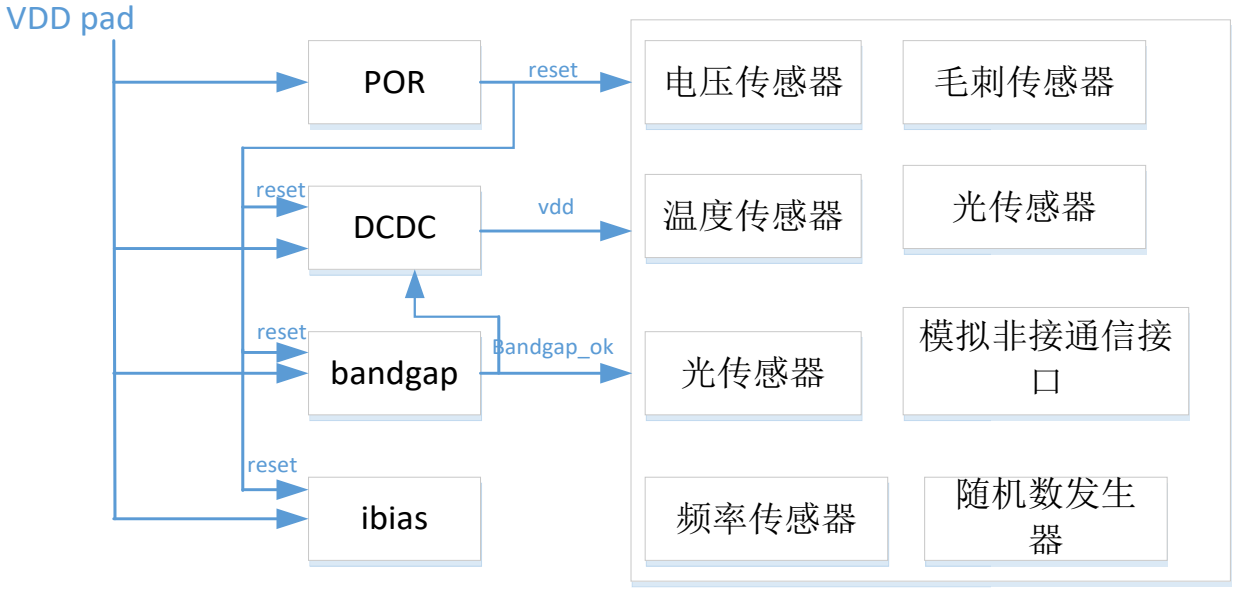
- 存储器采用统一编址
- RAM Shell通过MMU建立起RAM与CPU之间的连接，包括RAM本身以及RAM接口两部分
- 两种不同的RAM块，CXRAM只能通过MMU访问；AXRAM可被MMU和ACE访问，其中ACE拥有优先权
- AXRAM内含32位数据总线的SRAM硬核，再加上一些控制逻辑、数据加解密、地址加密逻辑
- CXRAM内含16位数据总线的SRAM硬核，再加上一些控制逻辑、数据加解密、地址加密逻辑

启动流程

- 芯片启动的顺序是模拟电路、数字电路、引导程序、芯片操作系统。
- 引导程序（BOOT程序）并决定进入芯片操作系统进入系统模式还是进入测试模式。
- 如果芯片进入系统模式，所有的防攻击措施全部生效，而在测试模式下，部分功能和sensor是可配置的，以便于调试。

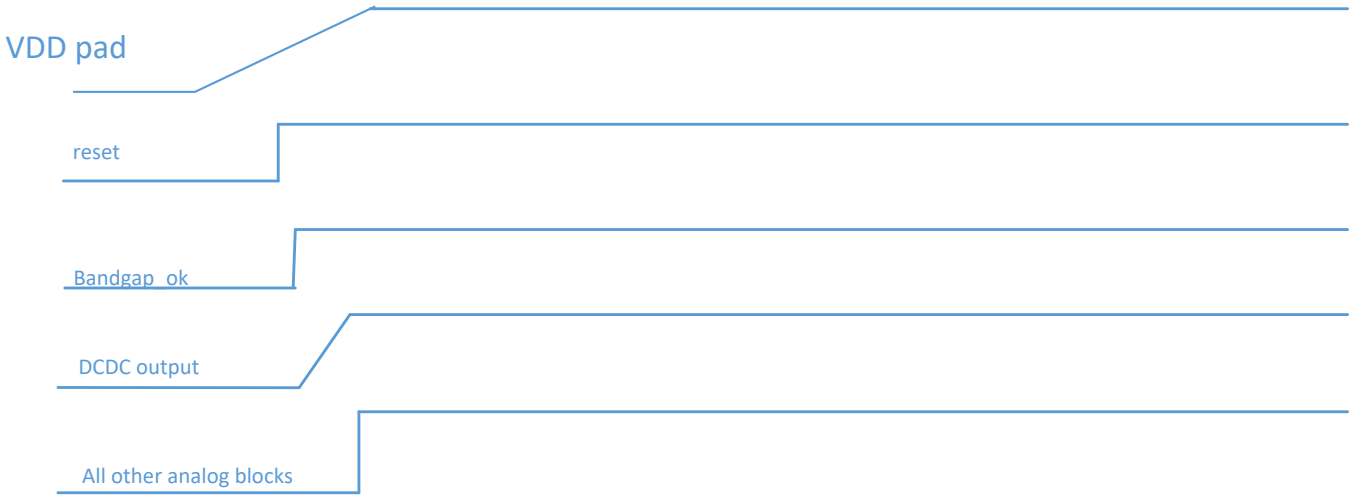
启动流程

- 模拟电路的启动流程
  - 在芯片上电的几乎同时，DCDC（）、POR（上电复位）、IBIAS（）、bandgap（带隙基准）即启动，POR模块在1.2V开始工作，即外部供电电压高于1.2V芯片即可复位。
  - Bandgap利用与温度成正比的电压与与温度成反比的电压之和，二者温度系数相互抵消，实现与温度无关的电压基准。
    - 为芯片提供一套精确的参考电压和参考电流，为所有的易受温度影响需独立供电的模拟部件供电，供电电压范围是1.1V~2.2V。输出稳定之后，产生”bandgap OK”信号。



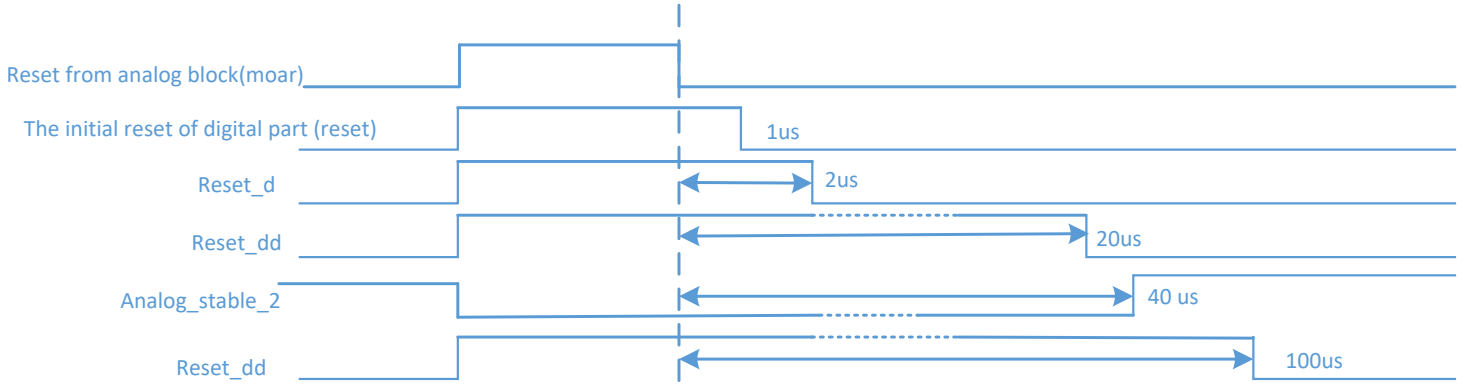
启动流程

- 模拟电路的启动流程
  - 一旦POR正常，DCDC立即启动，当接收到” bandgap OK”信号，DCDC的内部bandgap电压将来自于外部bandgap。
  - IBIAS模块的作用是通过一个反馈环产生一个基准电流，并将这个电流通过不同比例的电流镜输出至其他模块作为偏置电流。
  - 以上启动并达到稳定输出的时间小于50微秒。
  - 当bandgap输出稳定后，RC振荡器启动工作，在等待一定时间后产生稳定的内部时钟，之后所有的传感器和RNG启动，之后数字电路启动。



启动流程

- 数字电路的启动流程
  - 模拟电路启动并稳定之后数字电路激活，所有的数字模块不能同时启动，必须按时序启动。只要复位条件有效，复位逻辑始终保持在复位状态。复位条件失效，复位逻辑就会被禁止，时间为127us。
  - 复位源可被”~reset_delay”禁止，芯片若要进入测试模式必须在100us以内，以保证BootOS中没有复位发生。
  - 100us以后，所有的传感器皆可触发复位，在此之前，所有的复位源都是禁止的，不会产生复位。
  - 数字部分获得复位信号以后，大多数模块被激活。一些模块被reset_d激活，一些被reset_dd激活。而有一些模块还需等待analog_stable_2信号置位，例如频率传感器模块。



启动流程

- BOOT的流程
  - 硬件配置：
    - 1. CRC模块检查；
    - 2. RDS模块检查；
    - 3. RNG模块检查；
    - 4. EEPROM加密和RAM加密的初始化；
    - 5. 通过CRC检查EEPROM中的安全配置区首页内容的完整性；
    - 6. 通过RDS检查所有的EEPROM数据是否完整；
    - 7. 将EEPROM中的硬件配置写入RAM，然后从RAM写入SFR，检查一致性；
    - 8. 选择接口（接触式或非接触式）；
    - 9. 清除各种CPU模式所共享的寄存器。
  - 选择是进入测试模式还是系统模式。
    - 通过测试引脚输出测试多路复用器的输出信息。