面向物联网的通用MCU设计与应用开发实践

国民技术股份有限公司

钟新利

执行总监

目录

国民技术股份有限公司

2000年成立

2010年上市
股票代码：300077

技术领域
安全、SOC、射频

科研成就

- “863 计划”、“03 专项”、“核高基”
- 拥有1400多项国内外专利，其中发明专利超过1000项
- 2017年摘得国家知识产权最高荣誉——中国专利金奖
- 获得8项中国专利优秀奖
- RCC（限域通信）技术于 2017年 5 月正式成为国家标准
- 推动并参与了可信计算新一代 ISO/IEC 国际标准的制定

服务能力

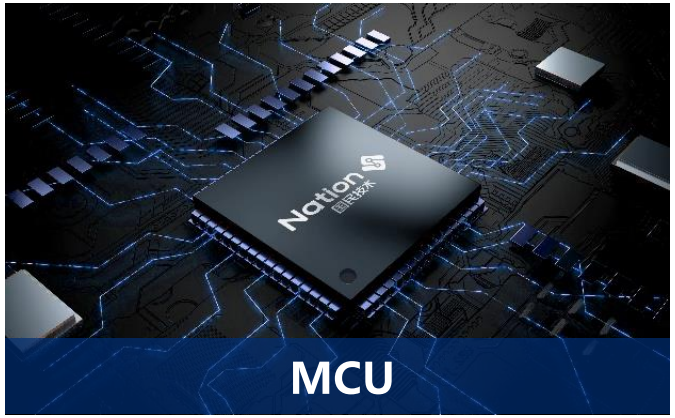
- 累计芯片稳定供货超13亿颗
- 国际化研发团队
- 本土化的技术服务团队
- 提供从芯片到应用的整体解决方案

资质与荣誉

- 中国上市公司协会副会长
- 国家级高新技术企业
- 国家规划布局内重点集成电路设计企业
- 国家级博士后科研工作站
- 深圳自主创新行业龙头企业
- 深圳市工程技术研究开发中心
- 深圳市重点实验室
- 公安部“中关村安信网络身份认证产业联盟”发起单位
- 中央网信办“中国网络空间安全协会”理事单位
- “中关村可信计算产业联盟”副理事长单位

主要产品

UKey主控、OTP主控、金融支付终端主控、物联网安全芯片、版权保护芯片、设备认证芯片、RCC移动安全



超值系列、低功耗系列、通用基本系列
增强系列、互联系列、无线MCU、行业专用

PC、工控机、服务器、IoT设备

银行卡、社保卡、居民健康卡、电子工商执照、残联卡、交通卡 ETC、旅行证件

BLE、NFC Reader、5.8G RF

二维码支付、安全云平台、人脸识别支付
IoT设备认证、车载T-BOX安全方案
工业互联网安全

交付能力与产业链合作伙伴

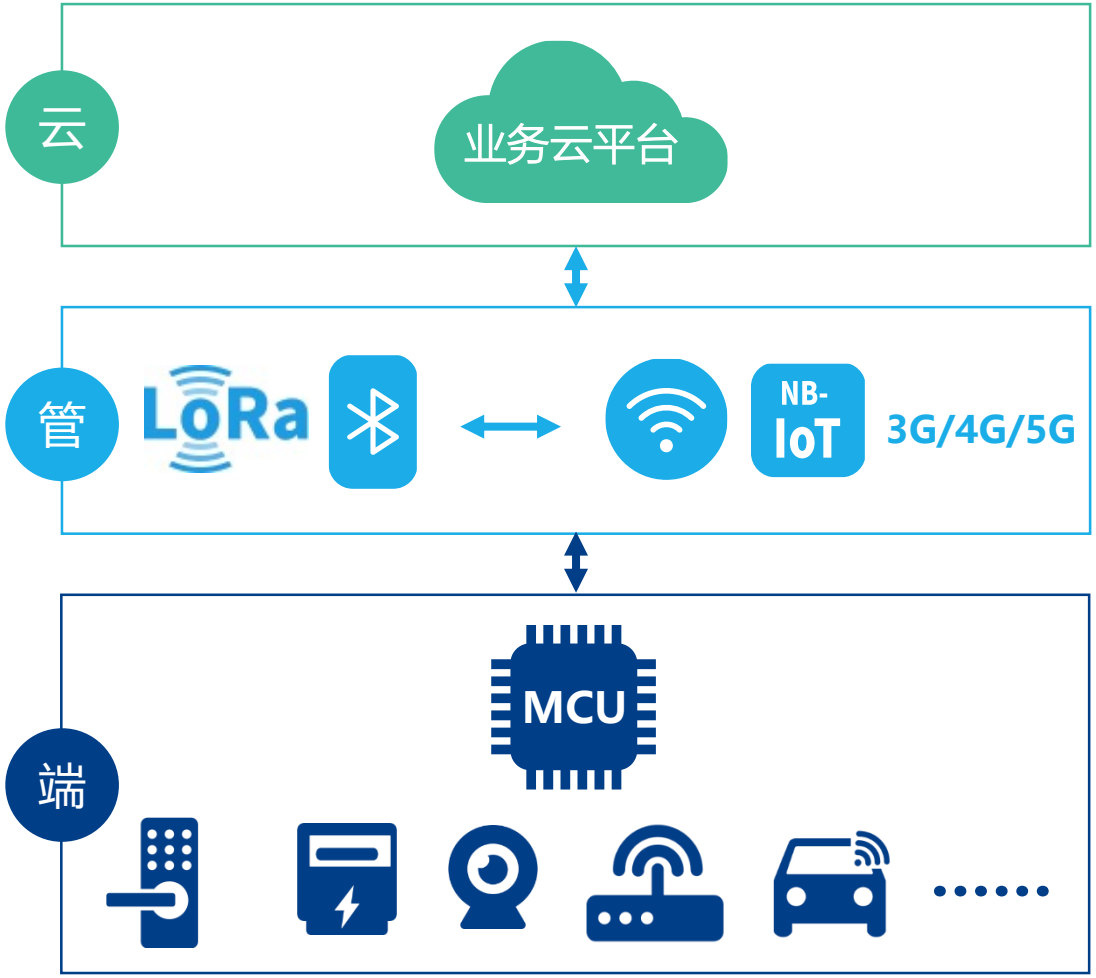
与全球一流圆片和封测厂商建立战略合作伙伴关系，打造稳定、高质量产品
每一颗芯片都经过严谨的质量控制流程，确保合格交付

130 000 万+颗
已累计出货

15 000 万颗
年交付客户

面向物联网的通用MCU设计挑战

典型的嵌入式物联网构架



物联网应用开发中的设计挑战

Nation 国民技术

广连接

- ✓ Sub-G
- ✓ LoRa
- ✓ BLE
- ✓ Zigbee
- ✓ NB-IoT
- ✓ WiFi
- ✓ 4G/5G

高能效

- ✓ 极低的静态功耗
- ✓ 可快速响应
- ✓ 低动态功耗
- ✓ 更智能的外设接口
- ✓ 更宽的工作电压

更安全

- ✓ 固件安全性
- ✓ 设备合法性
- ✓ 秘钥安全存储
- ✓ 关键数据存储
- ✓ 通信数据加密

物联网应用对通用MCU提出新的需求

低功耗

- 具备静态低功耗
- 动态低功耗
- us级快速唤醒
- 多种功耗管理模式
- 支持在低功耗下可工作的外设接口

高能效

- 传感器采集的信息计算越来越多在端侧设备完成
- 在达到运算性能的情况下尽可能降低总电流消耗

高可靠性

- 更宽的温度范围-40~105°C
- 带电ESD (HBM) 4~8KV
- 长达10年的寿命
- 更宽的工作电压

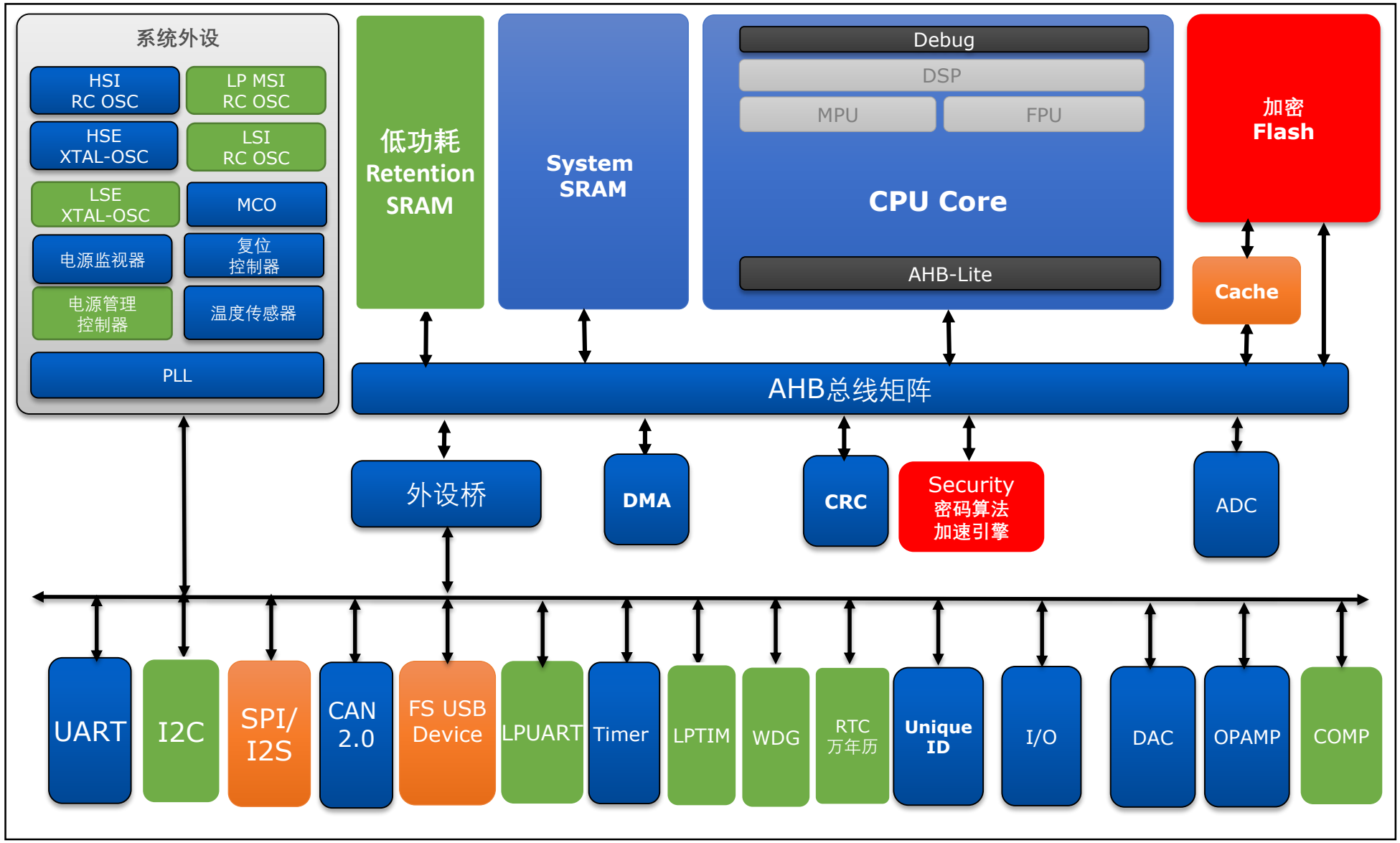
数模混合高集成度

- 集成常规模拟接口，如ADC，DAC
- 集成运算放大器，模拟比较器
- 集成电容式触摸控制单元
- 集成多种显示驱动器如Segment LCD
- 集成常规通信接口，部分接口需要支持低功耗模式
- 无线通信接口

安全

- 安全存储
- 安全启动及安全更新
- 通信数据加密
- 身份认证

物联网通用MCU设计构架



主电域

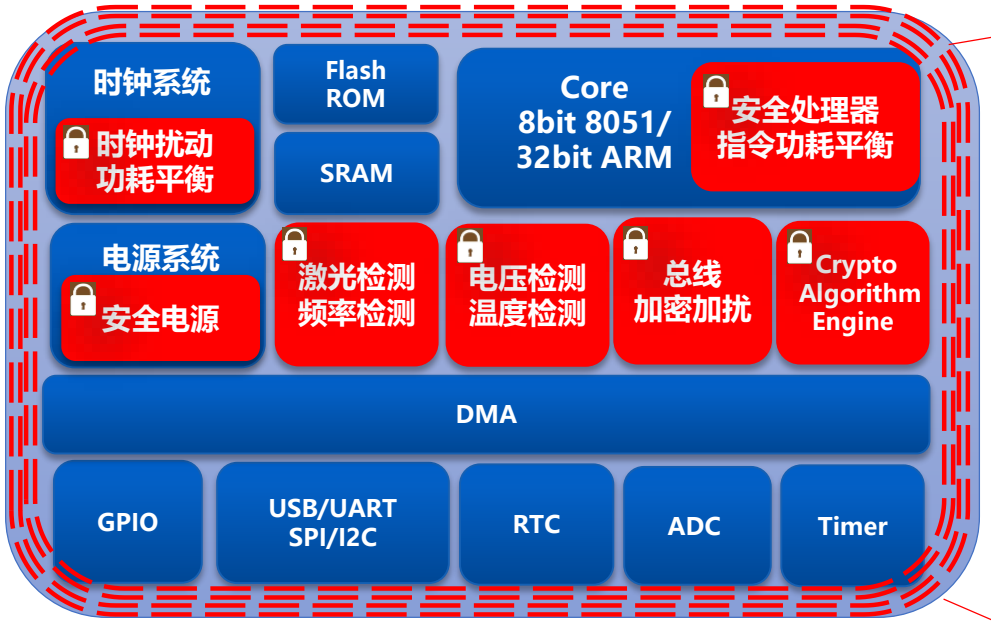
低功耗供电域

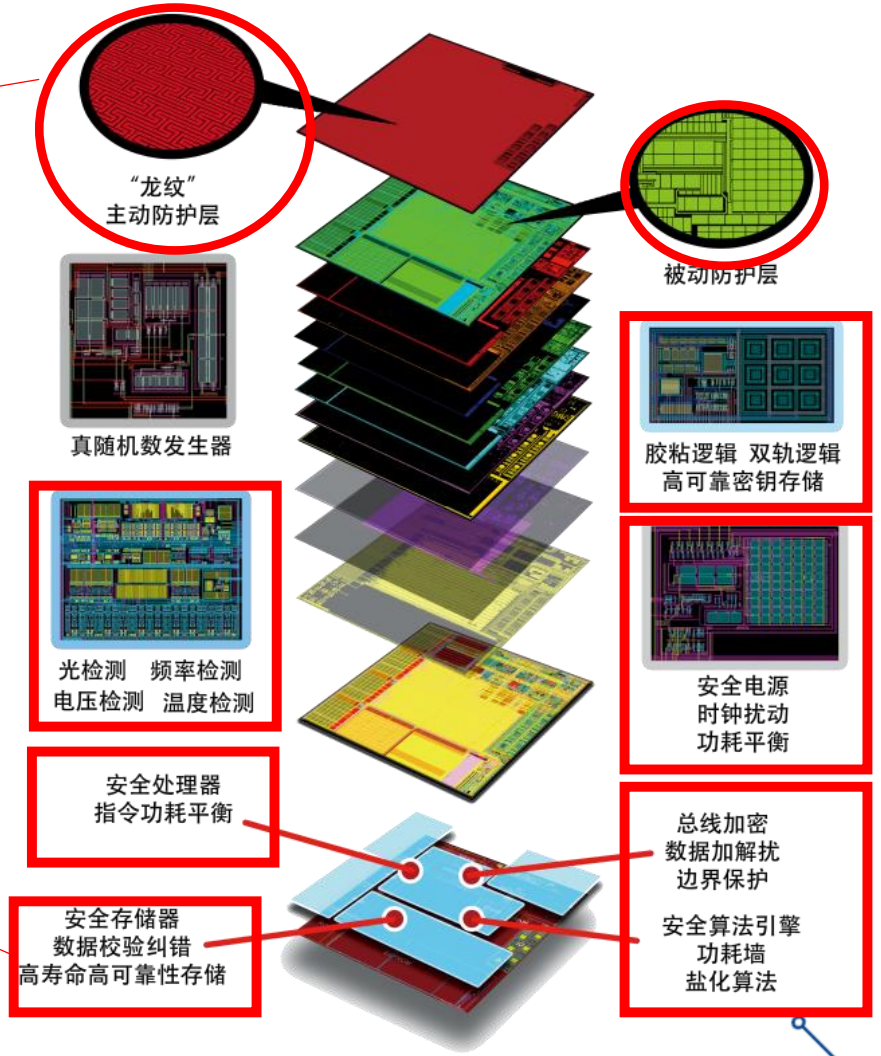
安全区域

通用MCU与专用MCU的差异

专用安全芯片与通用MCU的差异

安全芯片框架





- **安全芯片与MCU的异同**

相同点：两者都属于微控制器（MCU）SOC构架，具有相同的外设功能

差异点：安全芯片加强了芯片关键信息存储、运算过程的保护和抗攻击能力。
MCU无或弱化安全性，侧重于外设接口多样性。

通用MCU与专用MCU的差异

差异点	专用MCU	通用MCU
CPU内核与指令集	RISC，MIPS，DSP，ARM，8051	8051，ARM，RISC-V
电源管理	1.工作电压依据应用场景而定，有可能集成高压DC-DC 2. 工作电源模式以及待机电流依据场景而定	1.工作电压通常是1.8V~3.6 或5.5V 2.相对固定的电源模式，待机电流通常从几uA到几百uA级别
时钟系统	内置时钟或外置时钟，依据应用场景	内置或外置高频低频都支持
存储器	依据应用量身定制存储器大小，寿命，速度	通常根据IP厂商提供的成熟规格
算术加速协处理器	根据使用场景以内核性能有可能增加	通常无
模拟外设	根据信号采集需求决定	通常配置SAR ADC，部分产品配置放在器，比较器，温度传感器
数字外设	通信接口，IO个数依据实际应用决定	通常配备常用通信接口如UART，SPI,I2C,USB,CAN等
专用外设	通常将应用场景中的某部门电路或运算逻辑直接硬件化到MCU内部	无
成本	与应用匹配度高，成本相对较低	适用面更广泛，成本相对较高

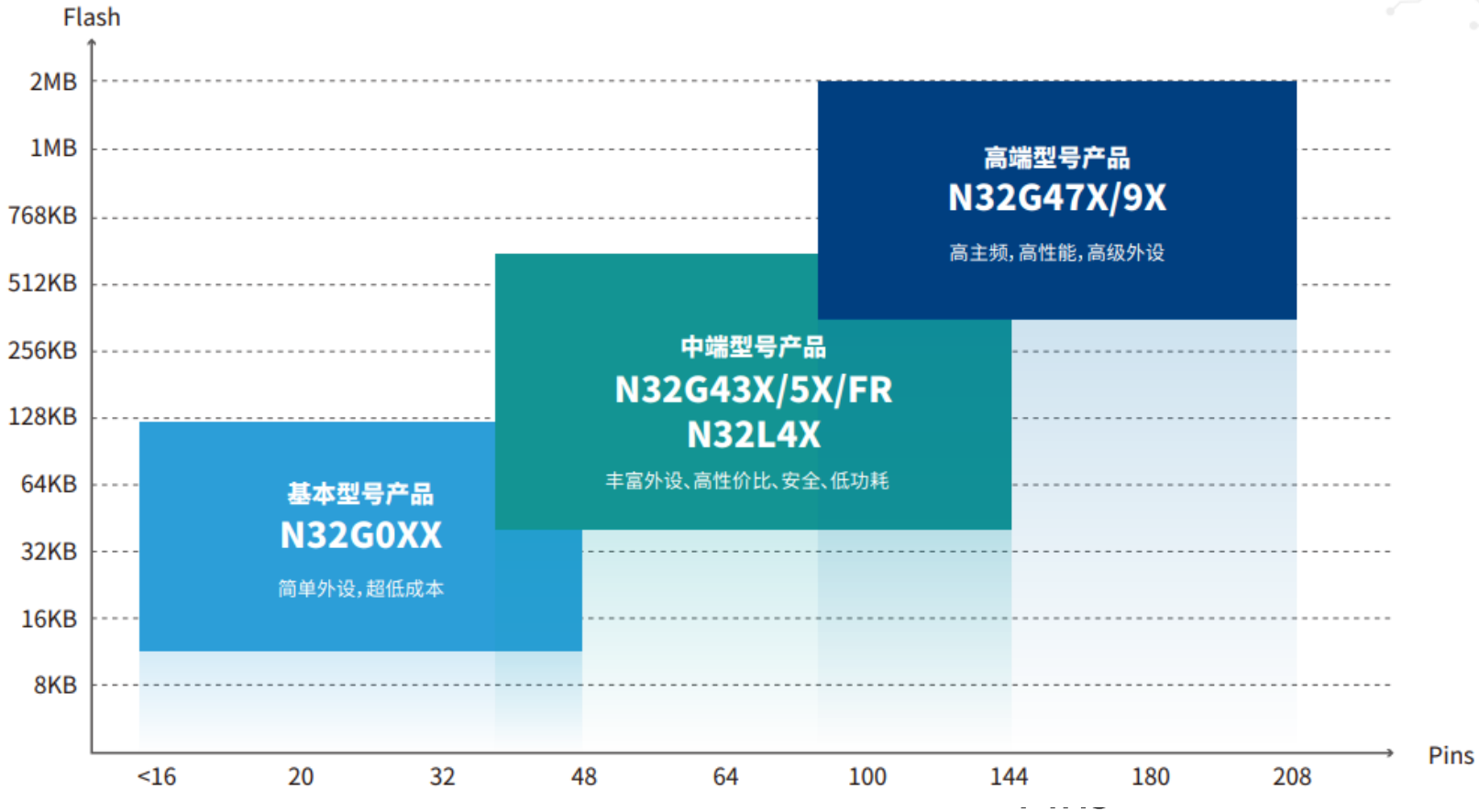
国民技术通用MCU特性详解

国民技术MCU产品规划

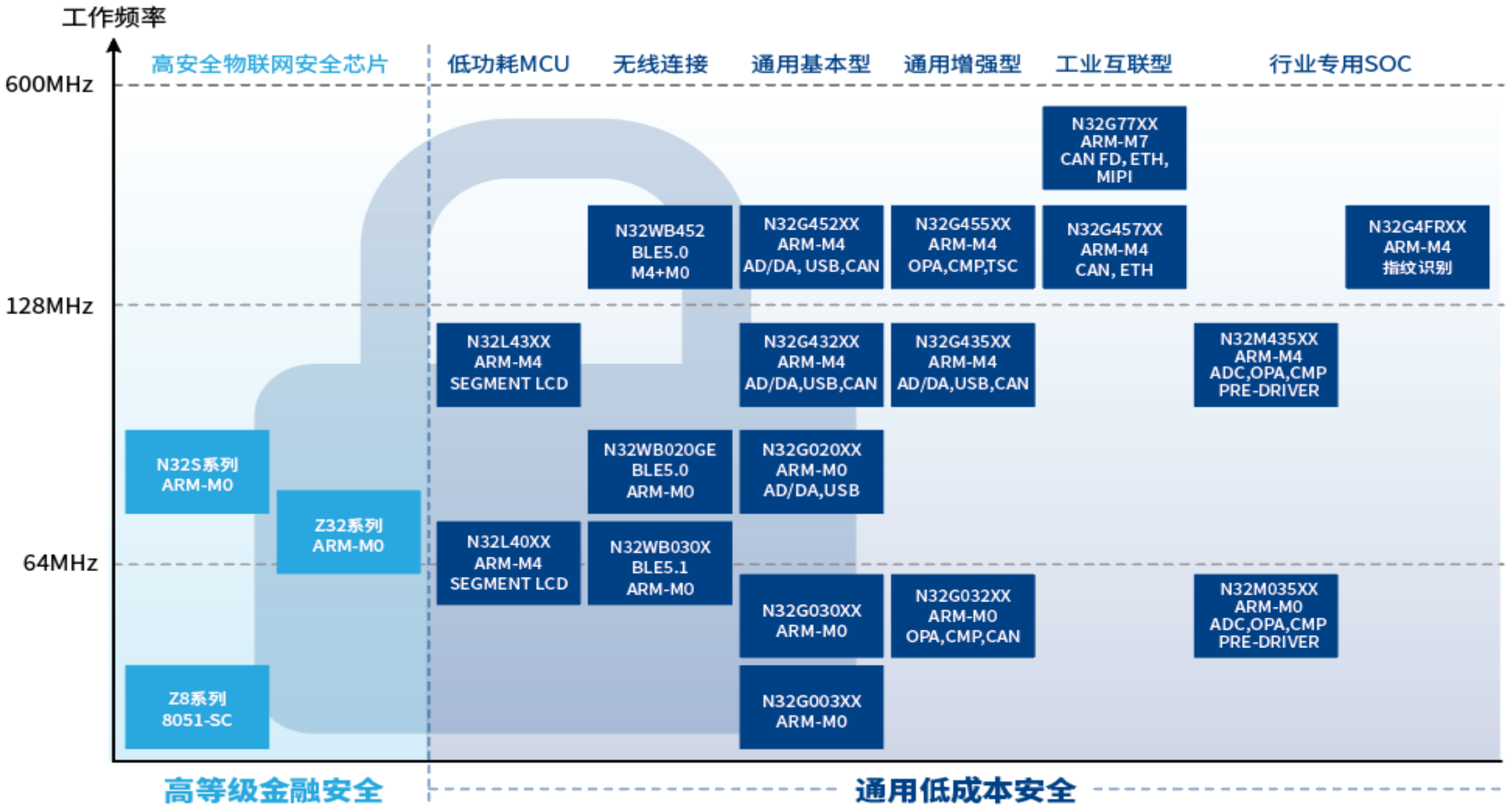
持续创新，为各行业提供超过100款芯片型号

基于ARM Cortex-M系列32位处理器内核，结合公司十余年SoC芯片研发技术积累，内置嵌入式高速闪存、低功耗电源管理，集成数模混合电路，并内置硬件密码算法加速引擎以及安全单元，形成高集成度、高性能、低功耗等特色的安全芯片产品和通用安全MCU产品，全系列产品覆盖多种应用场景。

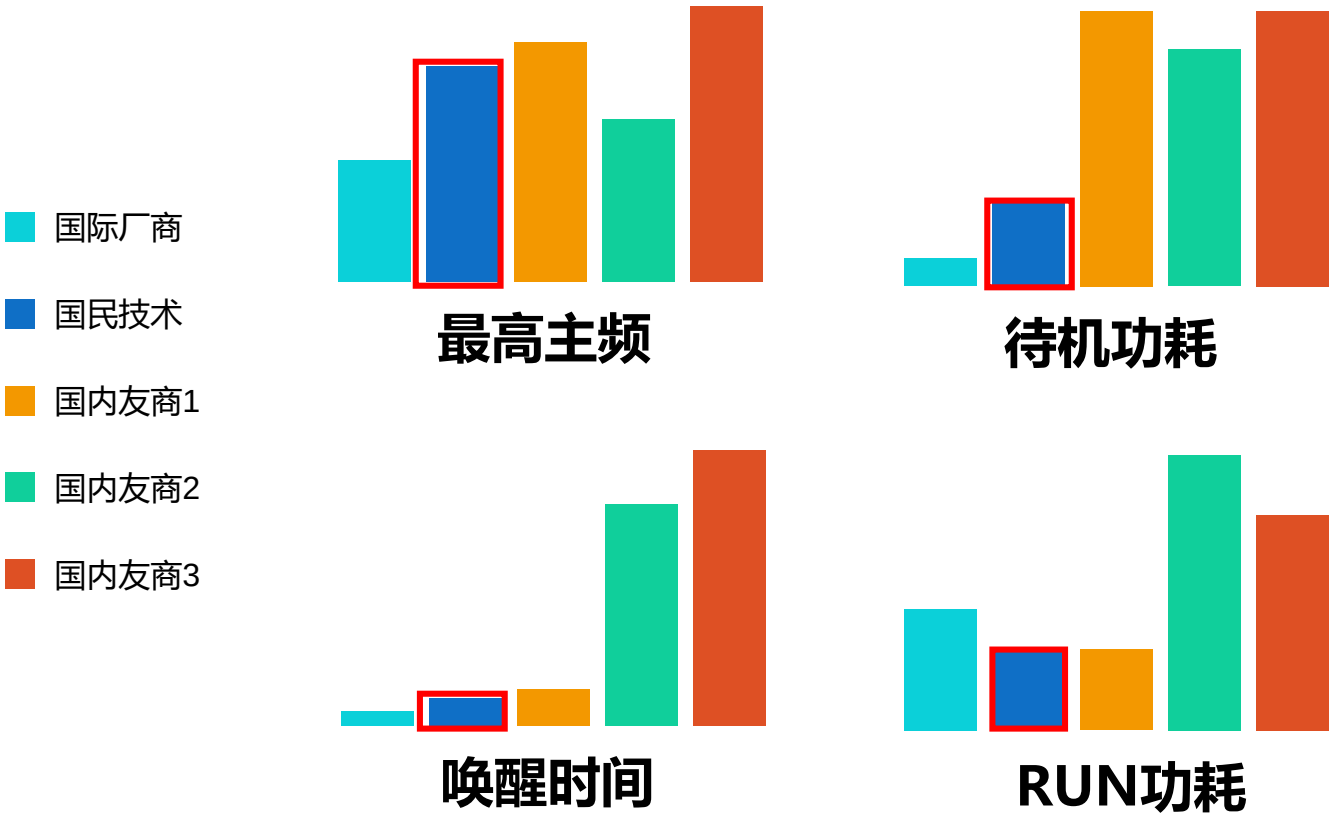
可广泛应用于穿戴式设备、智能家庭物联终端设备（如智能家电，智能门锁/门禁等）、电机控制、智慧城市节点控制、工业控制、智能表计、医疗、电池及能源管理、生物识别、光通信、传感器控制以及机器人等领域。



丰富的MCU产品组合

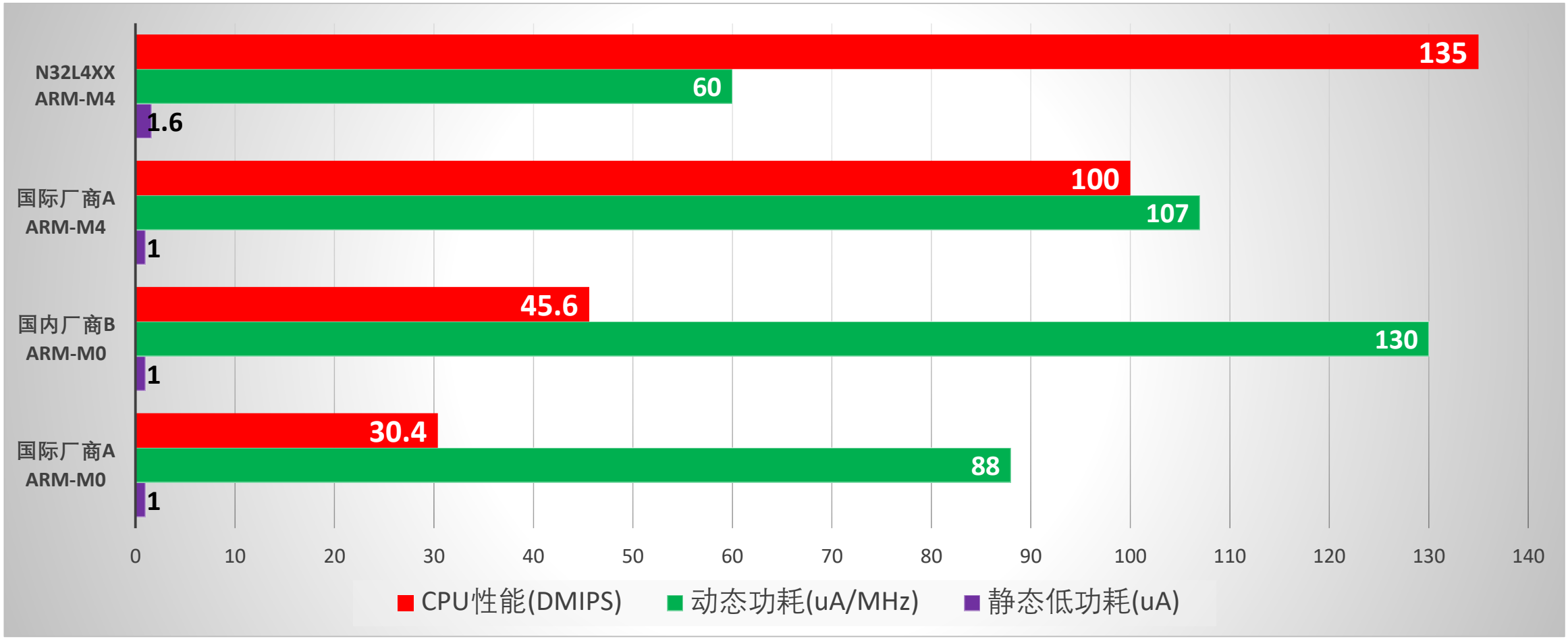


极佳的处理能效1/2



N32G45x系列
CoreMark : 486.26 @144MHz
Active Run: 13mA @144MHz
Standby mode: 2.5uA

极佳的处理能效2/2



高集成度及针对应用优化的外设模块

Nation 国民技术

高精度PWM

- 144MHz的PWM输入时钟，在电机控制应用中更高载波的情况下，输出更细腻的控制电流
- PWM可配置为延时生效或即时生效模式

每秒可采样5百万样本数据的高速12位ADC

- 支持定时器事件自动触发采样，确保ADC能同步于PWM采样。支持DMA数据传输，减少CPU中断次数
- 支持多种灵活的精度配置，支持12/10/8/6bit模式，其中6bit下可达到每秒9百万样本数据采集
- 采样窗口最小值仅需200nS，在电机控制应用中场景中，可以逼近100%的调制深度，提高能效。
- 内置最多4个独立的ADC，可以对4个模拟信号并行同步采样，提高相电流的采样精度，减少噪音

可编程运算放大器

MCU内置最多4个独立的前置运算放大器，可工作在PGA模式，放大倍数可编程设置，比如在多电机控制应用中可以灵活控制电流采样增益

高速比较器，支持低功耗模式

支持窗口比较模式，支持数字滤波、支持输入信号防抖、可内部直接控制PWM刹车等事件

低功耗定时计数器

支持在极低功耗下运行，除常规定时，输入捕获、比较输出功能外，同时支持脉冲计数功能、正交及非正交编码计数功能

低功耗无磁流量计量单元

片内集成低功耗无磁流量计量单元，基于LC无磁检测技术，支持自适应采样速率、可在极低功耗下运行。

更强的安全特性

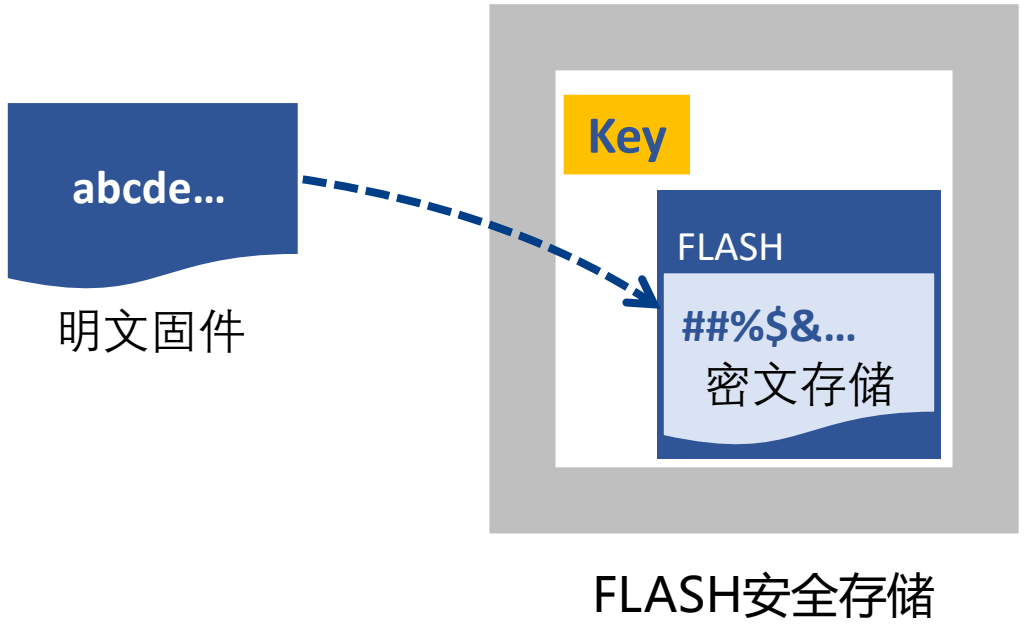
安全存储技术

保密性

- 存储数据加密，默认使能，不可配置
- 程序执行时自动解密
- 每颗芯片有不同的秘钥

完整性

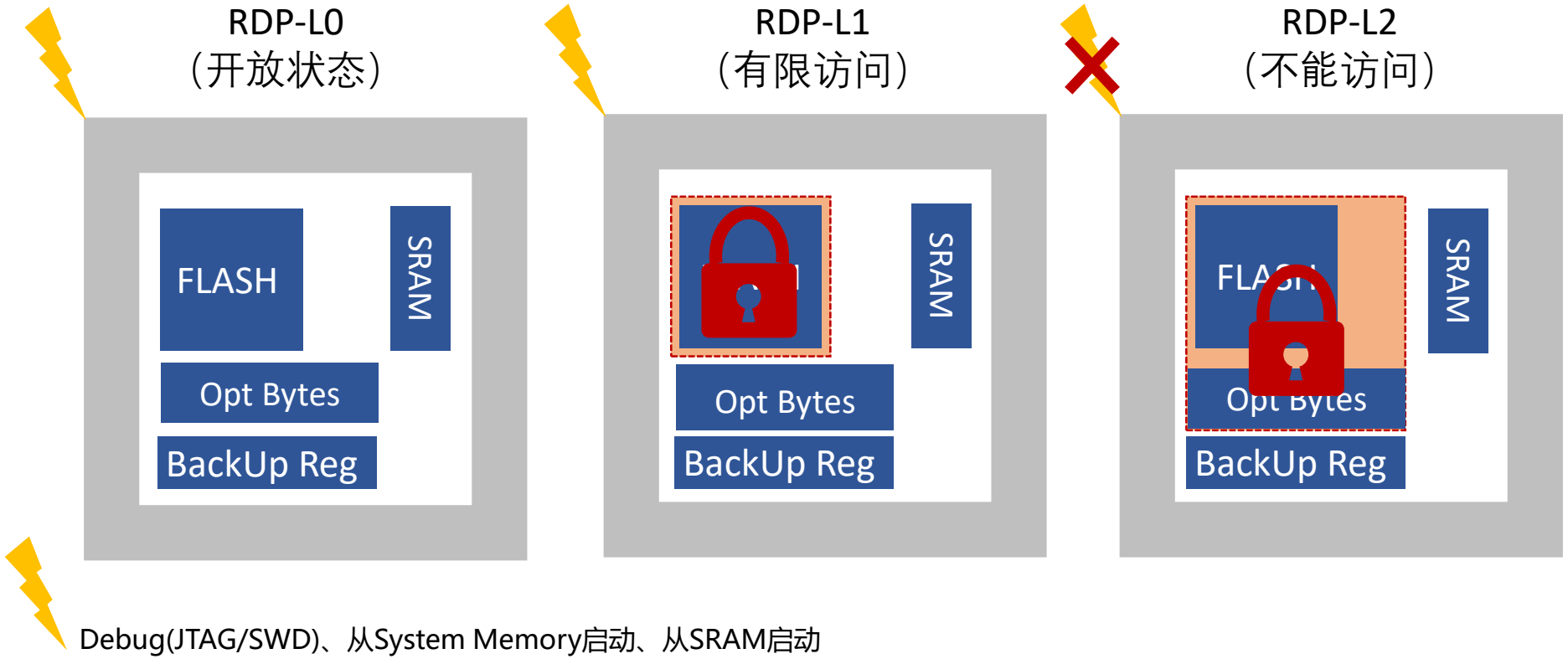
- 数据1-bit检错
- 数据1-bit纠错



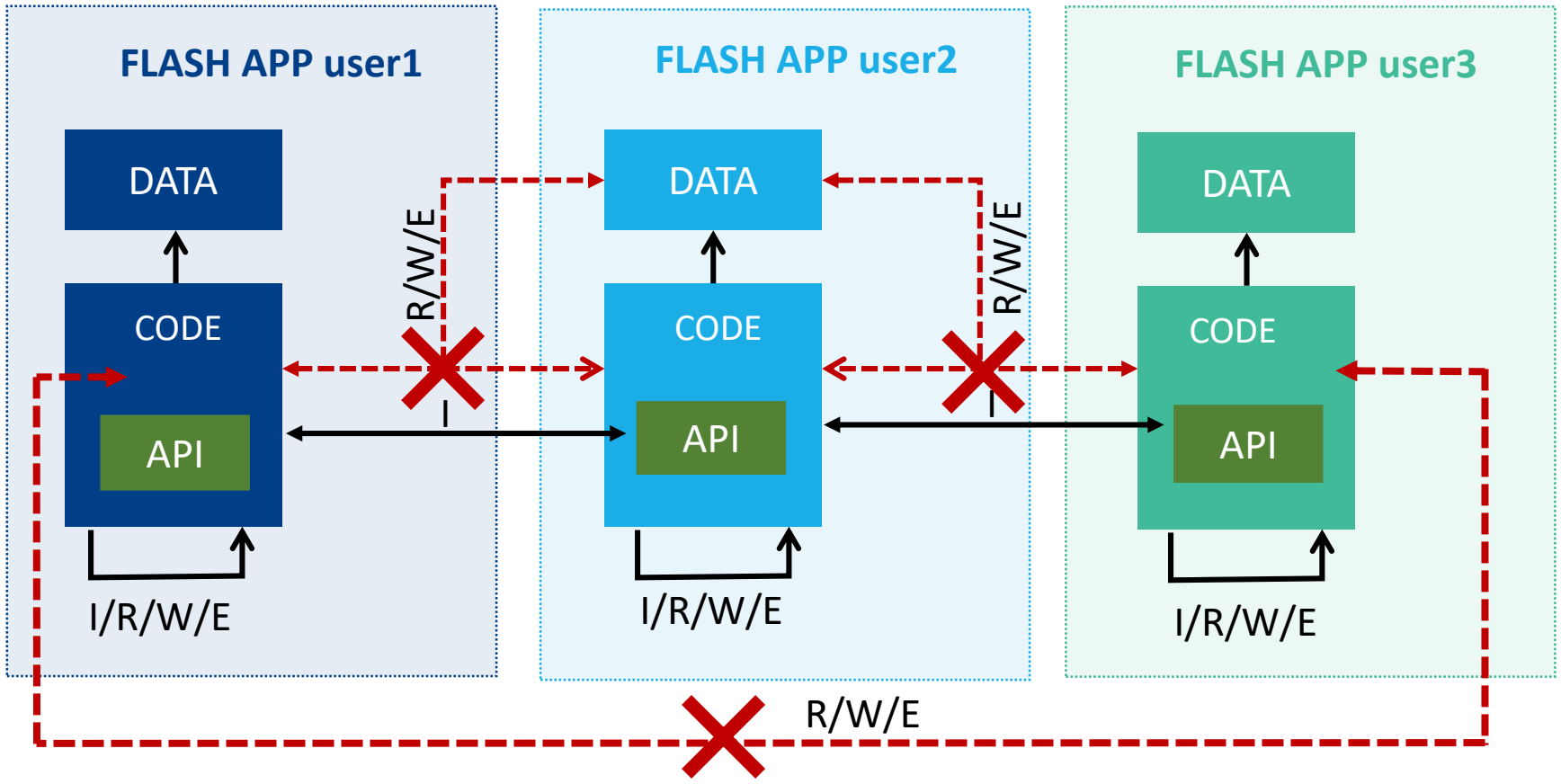
存储器读写保护技术

- 固件读出保护：Main Flash数据/代码读保护
- 选项字节保护：锁定Option Bytes
- 调试接口保护：禁用调试接口 → 设置RDP-L2，永久禁用

- 防错误写（防擦），防止程序跑飞后意外改变
- 生成仅可读的保护区
- 保护FLASH里的内容不被内外攻击写入



存储器分区隔离保护技术



防复制/防篡改/防擦除

I：可调用API

R：可读

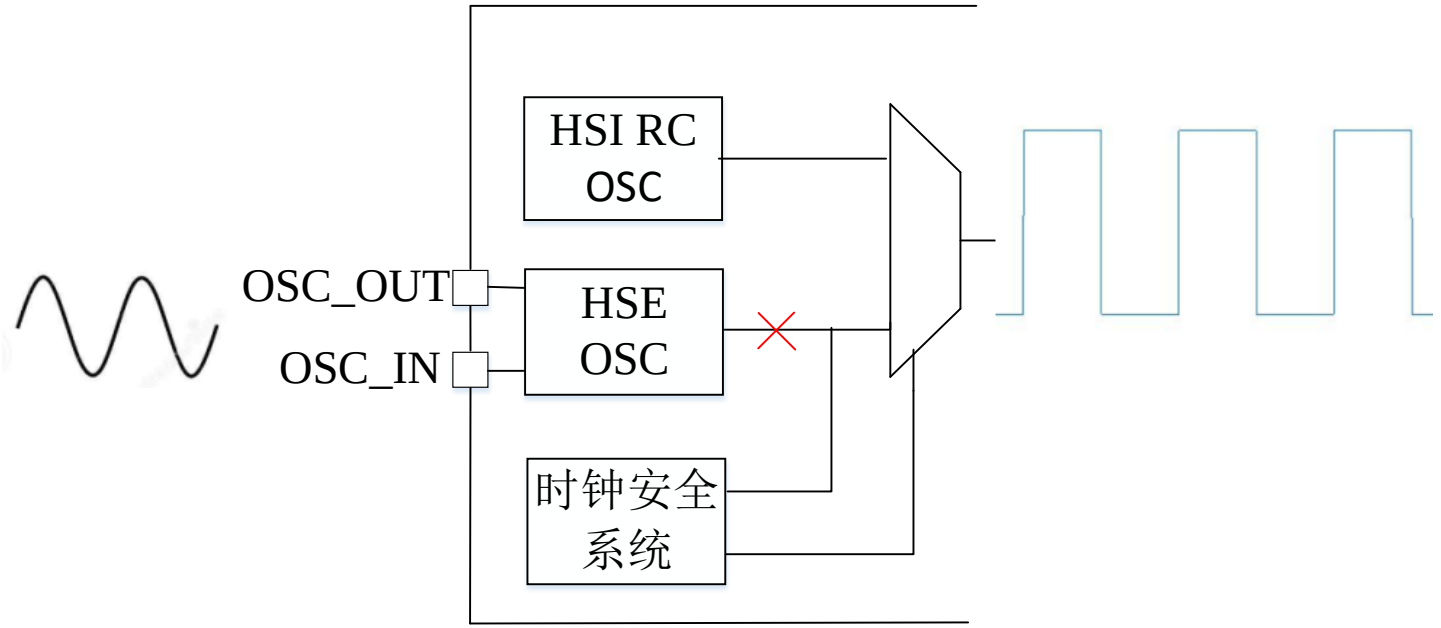
W：可写

E：可擦除

- 至多可划分为3个区域
- 分区大小可设置，颗粒度为16KB

注：只能设置一次，无法重置

时钟安全系统



主要功能：时钟安全系统时刻监控MCU外部时钟晶体，一旦外部时钟晶体因被攻击或其它原因导致失效，时钟安全系统将会把时钟自动切换到内部RC振荡器，在外部时钟晶体恢复后再由用户选择切换时钟源

密码算法

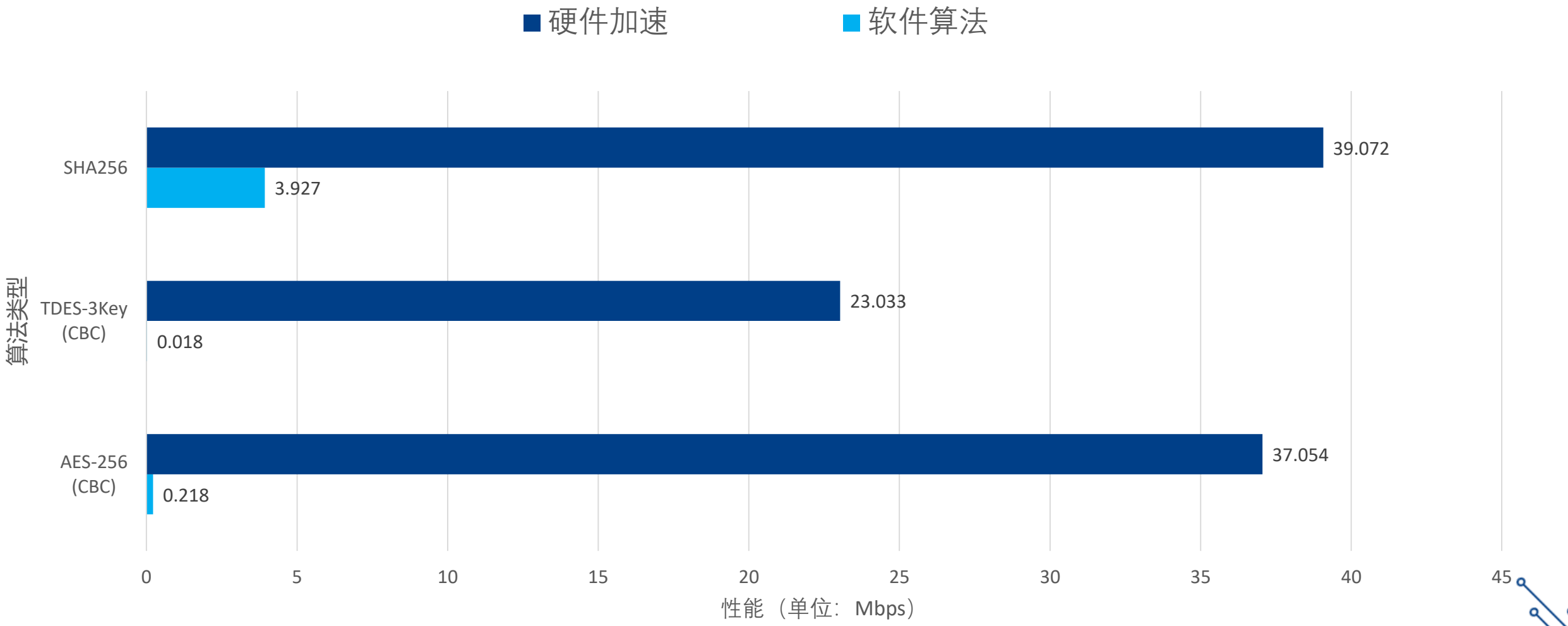
密码算法安全功能

常见密码算法	特点	典型用途	常见算法
随机数	利用熵源产生种子，生成随机数	• 生成密钥（密钥对/会话密钥等） • 生成nonce/challenge（抗重放攻击）	TRNG
哈希算法	将任意长度的消息压缩到某一固定长度的消息摘要：单向函数；消息变化，摘要变化	• 与签名、加密功能配合保证数据完整性 • 消息验证码MAC	SHA-1、SHA-224/256/384/512、SHA-3、SM3等
对称算法	加解密密钥相同，优点计算量小、效率高，缺点密钥分发困难	• 通信加密 • HMAC	DES、AES、SM1、SM4、SM7等
非对称算法	通信双方各拥有一对密钥（私钥保密/公钥公开），加解密密钥不同，缺点速度慢，适合少量数据	• 身份认证（签名/证书等） • 密钥协商	RSA、ECC、SM2、SM9等

密码算法分类

密码算法加速技术

硬件加速后的算法性能是软件算法的数十倍甚至百倍



测试条件：N32G45x ARM Cortex-M4F 内核MCU 运行144MHz下测得

MCU安全性技术

加密下载

通过芯片出厂内置的引导程序可实现对加密的bin文件进行下载

读写保护

用户可配置的不同保护级别(L0/L1/L2)，实现外部接口读写保护

时钟安全系统

外部时钟晶体失效时自动切换到内部RC振荡器

分区权限管理

- Flash区最多可划分为3个分区，分区大小用户可配置，不同用户之间建立防火强进行隔离
- 可用于保护多用户开发应用下的核心知识产权

安全存储

- 明文bin文件下载进MCU后以密文方式进行存储，防止暴力破解
- MCU执行程序时自动解密
- 秘钥存储，隐私数据存储

固件安全更新

通过密码算法对固件进行签名及认证，实现固件安全更新的功能

侵入检测

检测外部非法侵入，即使主电源断电也可将敏感数据清除

密码算法加速

支持AES,DES/T-DES, SHA,SM1, *SM2、SM3,SM4,SM7,MD5, TRNG,CRC

国民技术通用MCU技术特点

亚阈值及电源管理技术

- 低至100nA的休眠功耗
- 低至60uA/MHz动态低功耗技术
- us级快速唤醒
- 多种功耗管理模式

总线并发架构技术

- 比同级别运算性能高30%+
- CPU无等待指令访问Flash

高可靠性技术

- 工业级温度-40~105°C
- 带电ESD (HBM) 4~8KV
- Flash 100K次擦写
- Flash数据保持50年
- 更宽的工作电压
- 符合IEC60730B

数模混合设计架构技术

- 多通道高达5Msps 12bit ADC
- 多通道1Msps 12bit DAC
- 集成运算放大器，模拟比较器
- 集成电容式触摸控制单元
- 集成多种显示驱动器
- 集成多种高速通信接口
- 内存扩展接口
- 以太网控制器
- 低功耗无线连接

安全架构技术

- 存储加密，隔离防火墙
- 安全启动及安全更新
- 多级用户权限管理
- 时钟失效监测、防拆监测
- 多种国际标准、国密加解密算法

通用MCU的物联网应用开发

物联网应用开发中的设计挑战

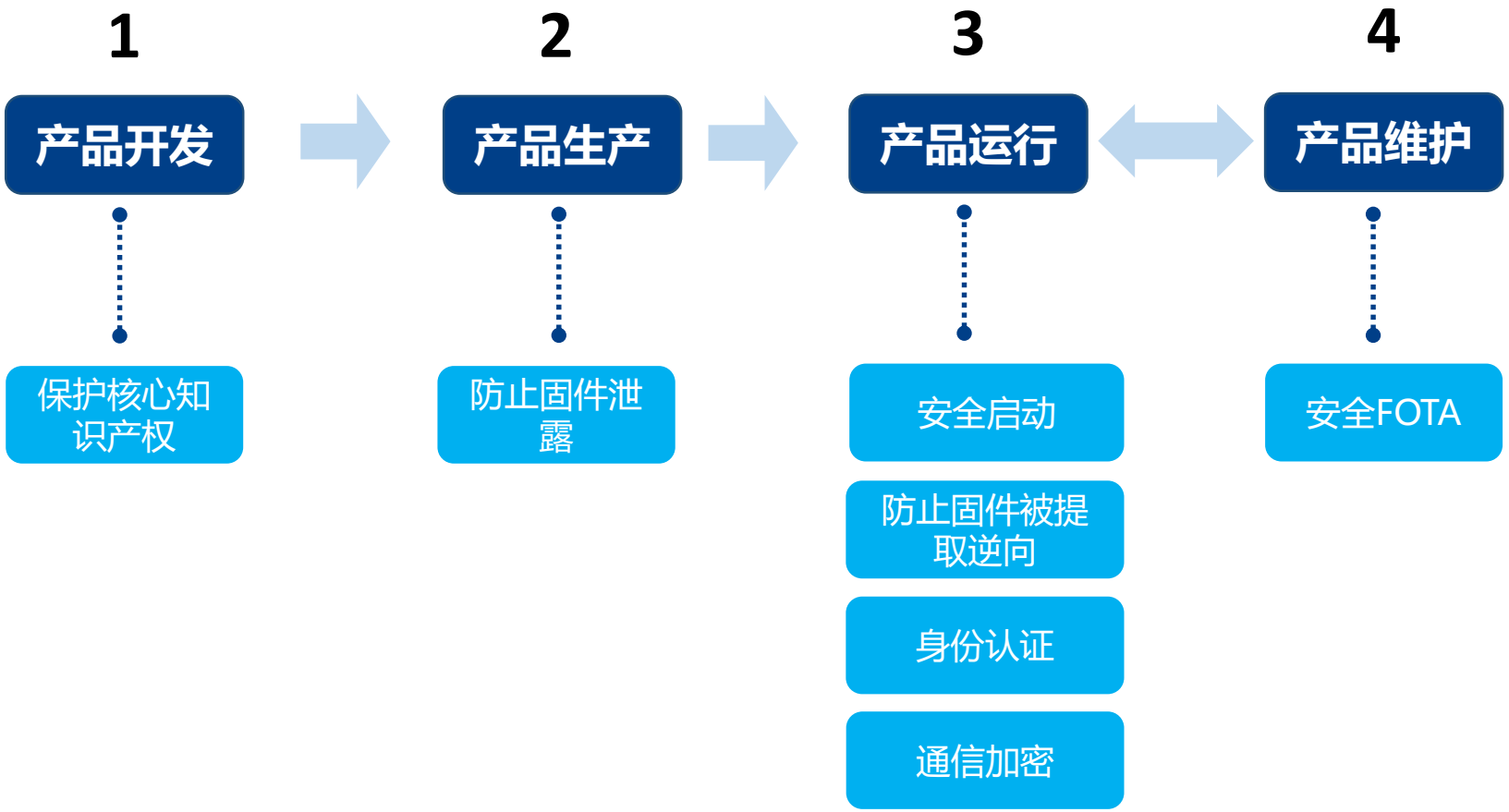
Nation 国民技术

☐ 如何选择适合的MCU	☐ 如何保护核心知识产权	☐ 如何保障合法性与唯一性	☐ 如何保障隐私数据安全
✓ 应用场景	✓ 保护核心算法	✓ 固件合法性	✓ 秘钥安全存储
✓ 产品功能特点	✓ 可便利的支持二次开发	✓ 云服务器的合法性	✓ 关键数据安全存储
✓ 工作环境	✓ 防止固件被暴力获取	✓ 设备合法性	✓ 通信数据加密
✓ 寿命	✓ 防止固件泄露		

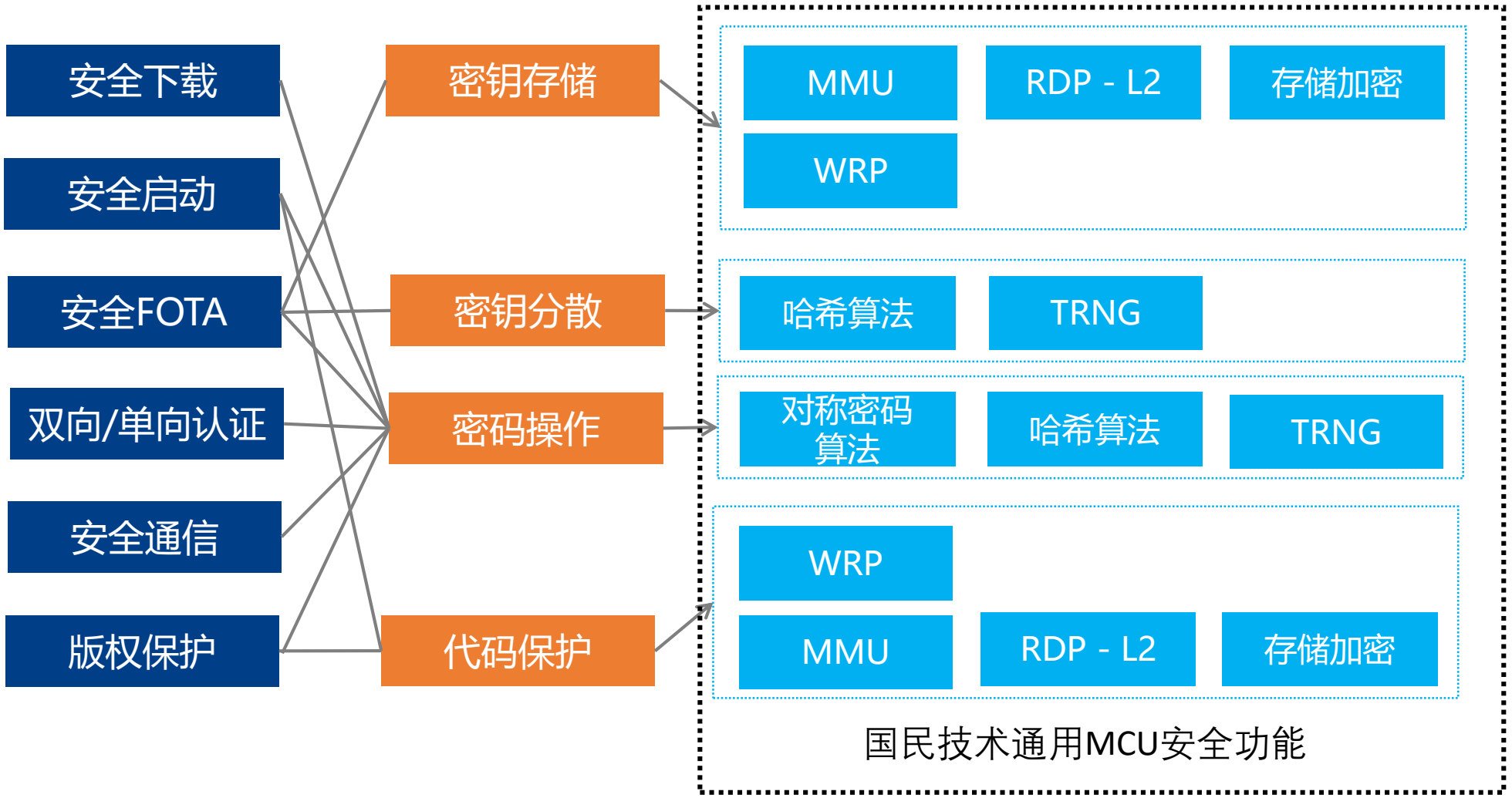
通用MCU的物联网应用开发

- **选择联网方式**
  - 供电方式
  - 通信频次
  - 通信数据量
- **根据应用特点选择MCU**
  - 供电方式及使用时长评估MCU的功耗
  - 通信频率次
  - 根据主要功能，评估对MCU的算力要求
  - 根据功能及业务逻辑确定存储器大小
  - 根据外接传感器或其它器件确定MCU的数模外设接口
- **设计安全构架**
  - 固件安全
  - 访问安全
  - 通信数据安全

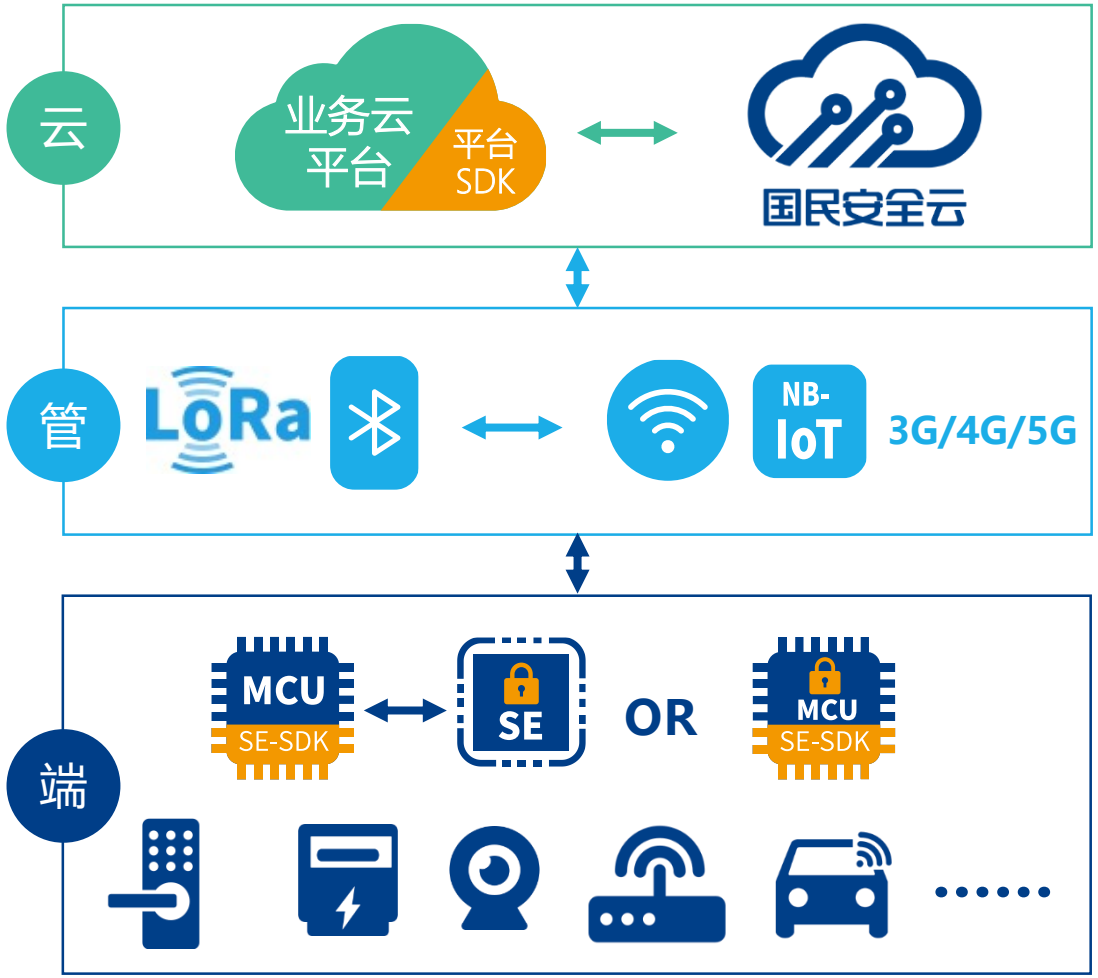
构建产品全生命周期的安全管理策略



基于国民技术MCU的安全特性构建产品全生命周期安全策略



国民云-端物联网安全系统架构解决方案



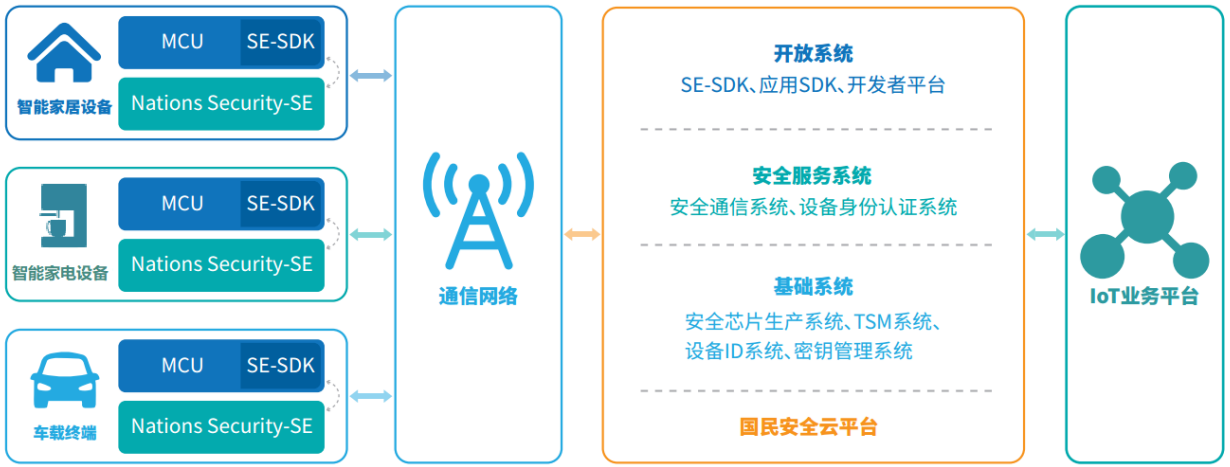
- 设备身份安全认证
- 云-端安全通信过程密钥协商（一次一密）
- 安全通信数据加解密
- 灵活的安全认证方式，单向认证/双向认证可选

- 应用级数据加密，不依赖于通信通道安全性，避免通信通道的安全性不可控

- 秘钥存储，隐私数据安全，通信数据加密
- 国际/国密、对称非对称算法
- 设备端提供敏感数据安全存储
- 版权保护 、核心代码保护、安全OTA、安全启动
- 适应不同场景的多种安全等级
- 单向认证/双向认证，支持多种认证方式
  - -对称密钥认证方式（3DES/SM4等）
  - -PKI/CA证书认证方式（SM2/RSA/ECC）
  - -CPK/IBC认证方式(SM2/ECC/SM9)

国民安全云解决方案平台概览

- 基于国密/国际算法对设备进行身份认证、密钥协商、通信数据加密等安全保护
- 支持密钥体系：
  - 对称算法（SM4/SM2/3DES/AES）
  - 非对称算法（SM2/ECC/RSA）
  - CPK/IBC算法（ECC/SM2/SM9）
- 设备端可快速集成SE-SDK和云端可快速集成安全云SDK，快速实现云&端对接
- 包含安全生产系统、密钥证书分发系统、设备ID/密钥管理系统、安全通信系统、设备身份认证系统、TSM空发系统等，实现产品从研发-生产-运行的全流程覆盖



灵活的对接部署模式

私有化部署方式：

- 提供安全云平台客户服务器私有化部署方式销售。同客户业务云平台进行集成。
- 特点优势：满足对运营数据敏感的客户需求；便于平台整体进行安全认证；提供部署/对接全方位技术服务。

公有云接入方式：

- 客户业务云集成安全云SDK，与国民安全云对接； 按照设计接入量进行计费。
- 特点优势：一次性投入费用低；可快速集成实现云-端高安全。

Nation 国民技术

国民技术MCU信息获取与沟通，可通过如下途径

国民技术微信公众号

官网： www.nationstech.com

业务合作

电话：0755-86916666

手机：18988772159（微信同号）

邮箱：sales@nationstech.com