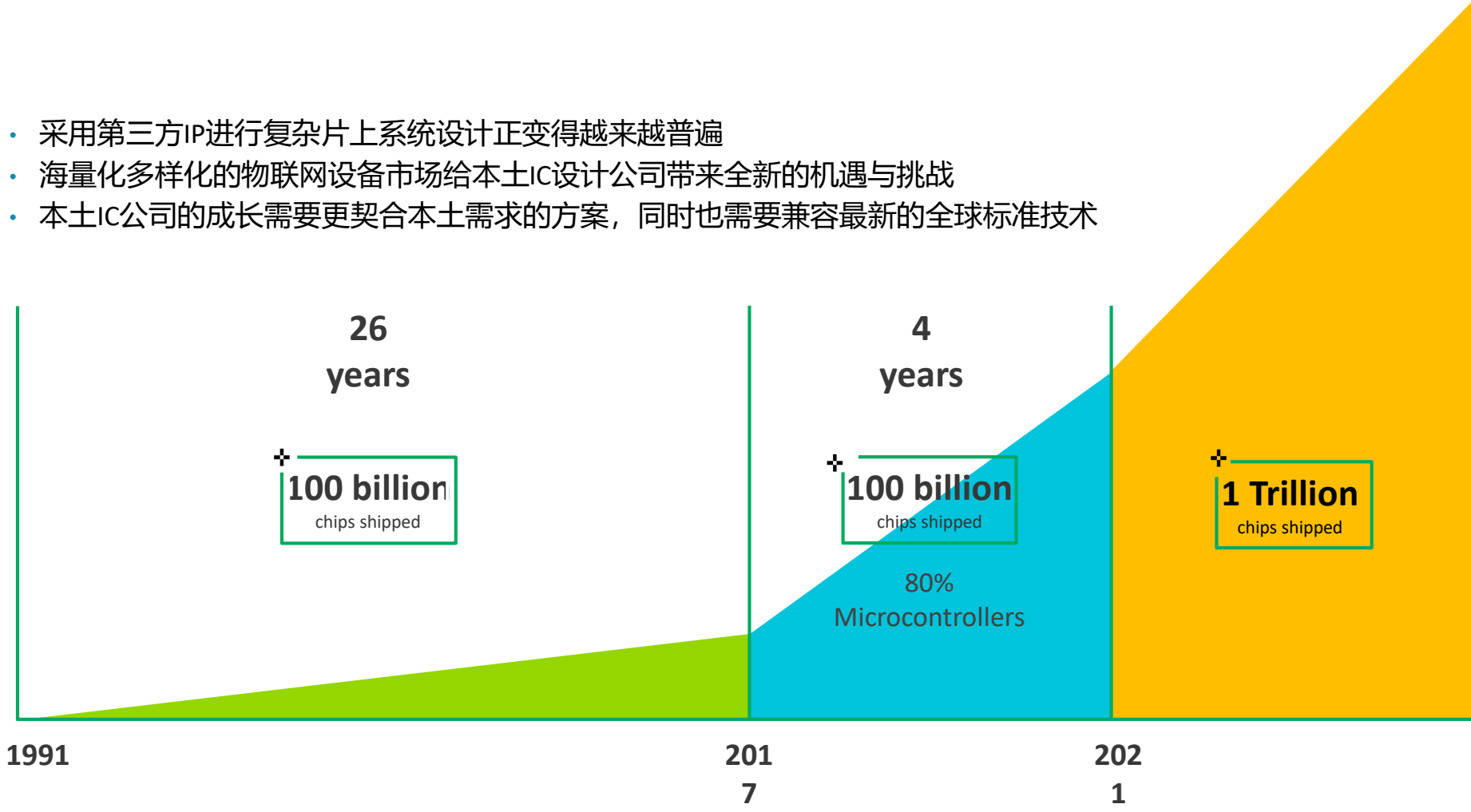
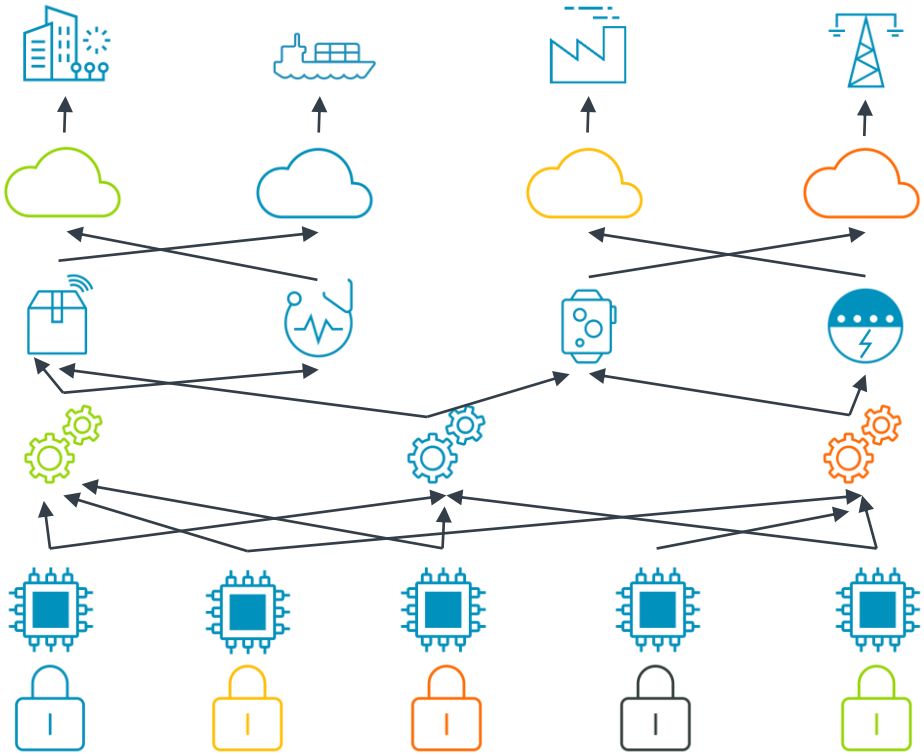
万亿规模的物联网设备市场

- 采用第三方IP进行复杂片上系统设计正变得越来越普遍
- 海量化多样化的物联网设备市场给本土IC设计公司带来全新的机遇与挑战
- 本土IC公司的成长需要更契合本土需求的方案，同时也需要兼容最新的全球标准技术



PSA为应对物联网信息安全的挑战而生

- 整个产业链没有明确的**设备安全规范**定义
- 没有明确的架构可以满足**不同尺寸不同能力**的物联网设备安全需求
- 没有明确的方式保证设备的**远程安全管理**需求



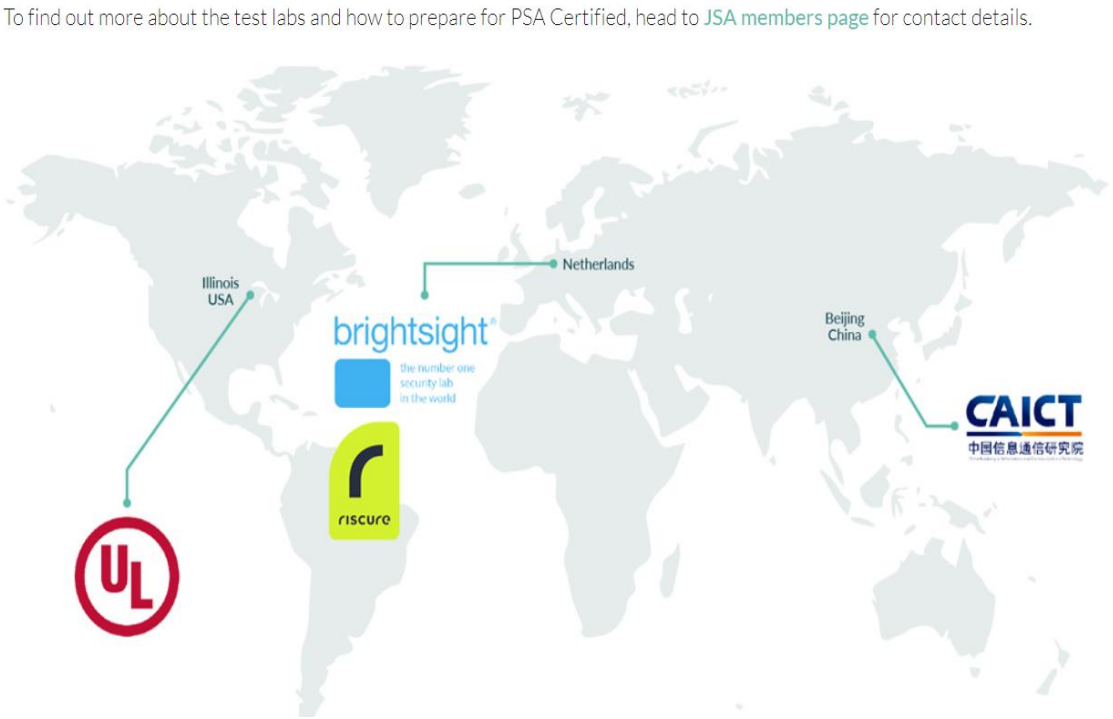
arm CHINA

PSA是全球性的平台安全架构

Arm全系列处理器支持的平台安全架构

产业链厂商广泛参与

专业实验室提供检测和认证



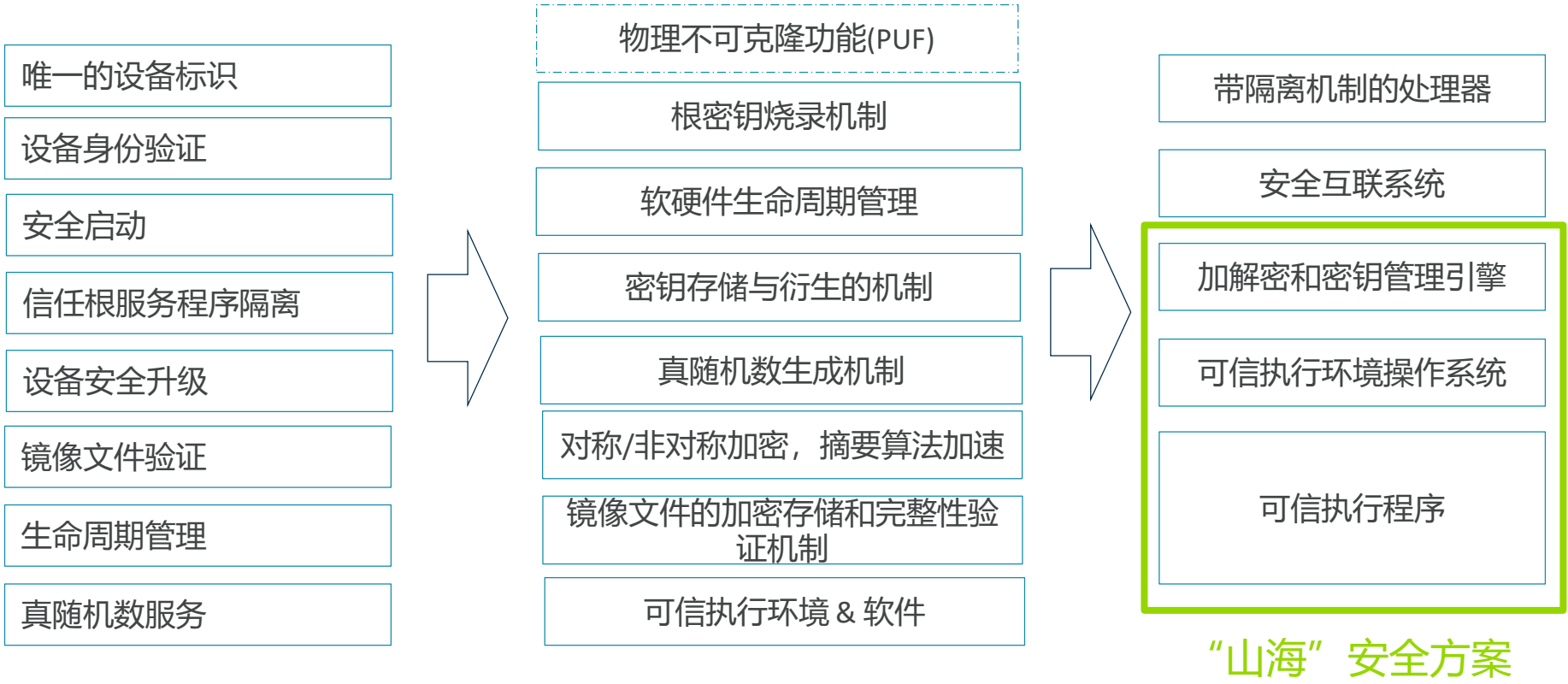
arm CHINA

PSA 安全模型 – 10个设计目标

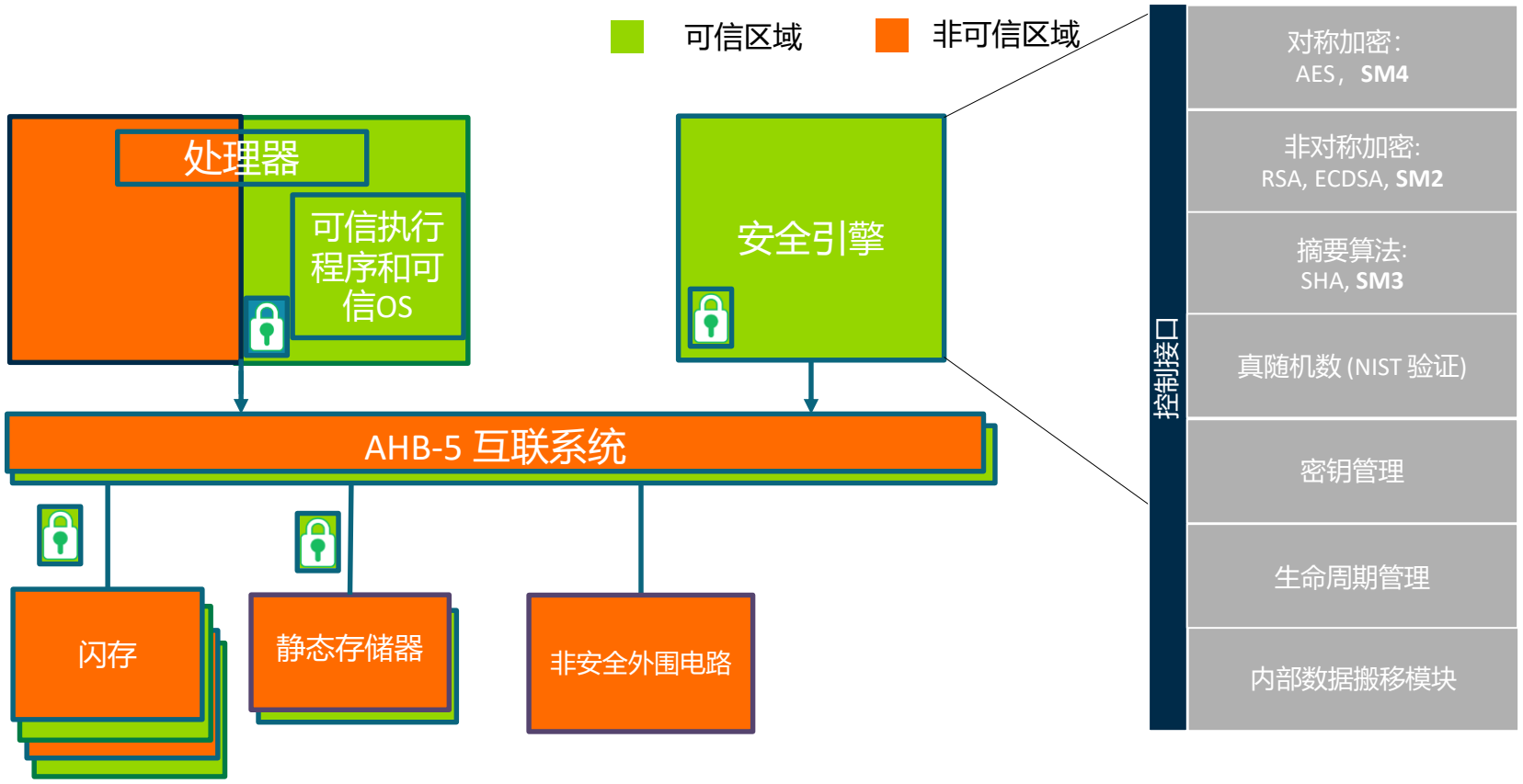
- 唯一的设备标识
- 设备身份验证
- 安全启动
- 信任根服务程序隔离
- 设备安全升级
- 镜像文件验证
- 生命周期管理
- 真随机数服务

arm CHINA

从需求到产品



一个典型的安全系统



arm CHINA

安谋中国对中国物联网安全的愿景

- 引入全球最新安全技术，帮助客户对接世界、参与世界的技术，引领技术的发展;
- 本地化更多的安全技术，支持国家和产业自主设计的发展需求;
- 丰富Arm的生态系统，积极参与安全软件服务开发和安全标准制定，帮助安全技术在更多行业快速落地。

arm CHINA

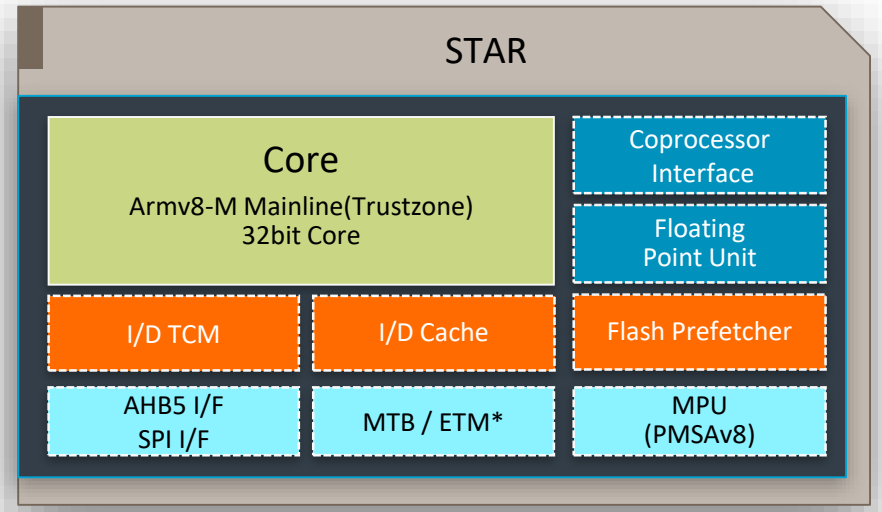
Star Processor
“星辰”处理器

arm CHINA

“星辰”, 面向智能互联安全IoT应用需求的处理器

高效计算

- 性能与功耗均衡的配置
- 1.50 DMIPS/MHz & 4.02 Coremark/MHz



安全基石

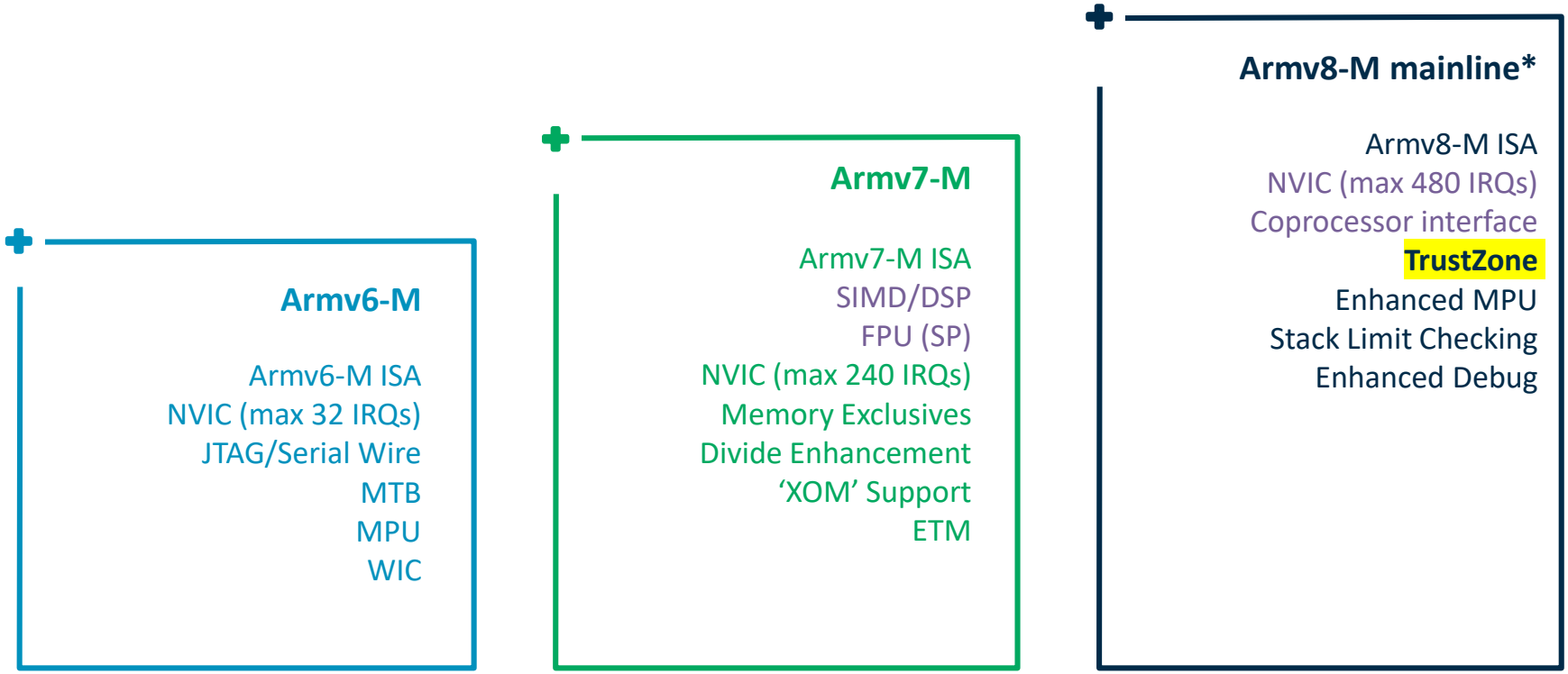
- 基于Trustzone的系统级安全方案带来整个系统的安全能力提升
- 针对安全/非安全区，都有专门的内存保护模块进行保护

灵活扩展

- 引入TCM、Cache和Prefetcher增强存储系统效率
- 协处理器接口允许客户灵活定义与处理器耦合的协处理器，提升系统效率

* ETM are independent IP

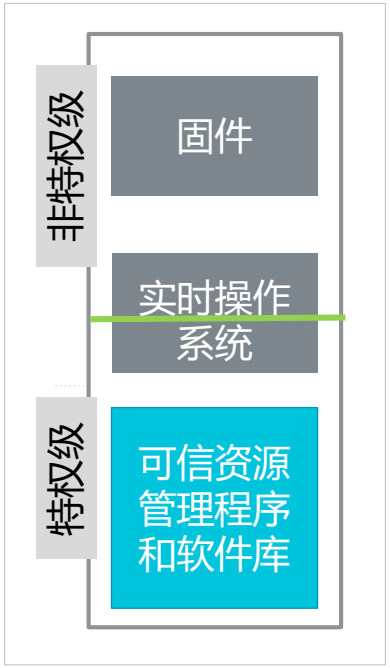
“星辰”处理器支持最新的Armv8-M Trustzone-M技术



*The purple parts are additional features over Armv8-M baseline

简化软件设计，提升安全级别

传统嵌入式安全软件系统



资源隔离

代码和数据放在一个内存区域，有很宽的攻击面

切换开销

由操作系统管理，上下文切换代码和延迟都比较大

软件接口

各家自定义的软件接口，难以统一开发

基于Trustzone的嵌入式安全软件系统

资源隔离

资源物理隔离，非安全区对安全区所有资源不可见

切换开销

类似“函数调用”的方式切换，极小的切换开销

软件接口

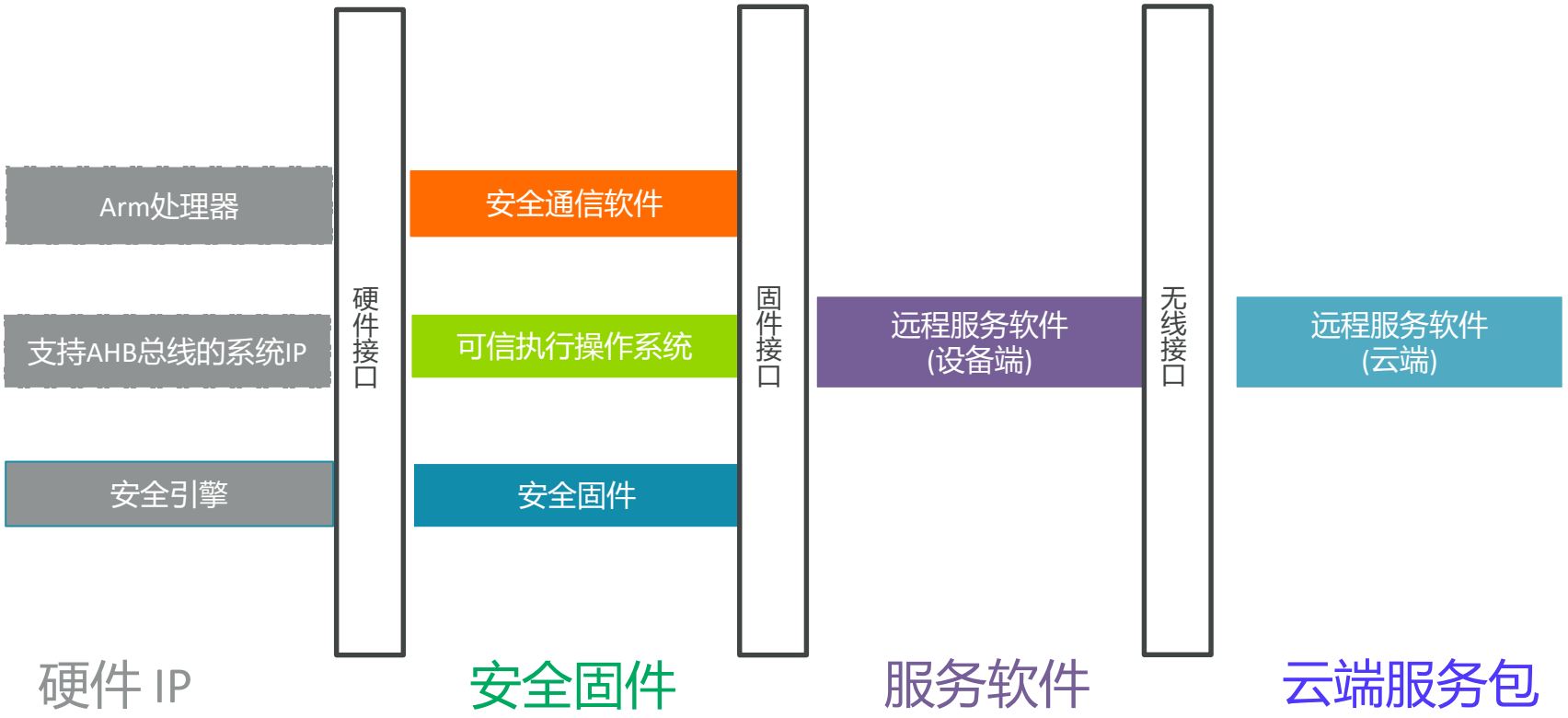
标准PSA接口，业界统一的安全测试规范

arm CHINA

“山海”安全方案

“山海”安全方案

由硬件，软件，和云服务开发包组成的全栈解决方案



“山海”价值主张

面向物联网设备

可灵活配置安全架构，满足不同类型的物联网设备需求

支持Cortex-M系列处理器内核

降低安全设计门槛

包含硬件，软件，和云服务开发包的全栈解决方案

与PUF等不可复制身份技术预集成，增加设备安全能力

可量化可测量的安全方案

预先通过PSA 2级安全测试

兼容PSA 程序设计接口

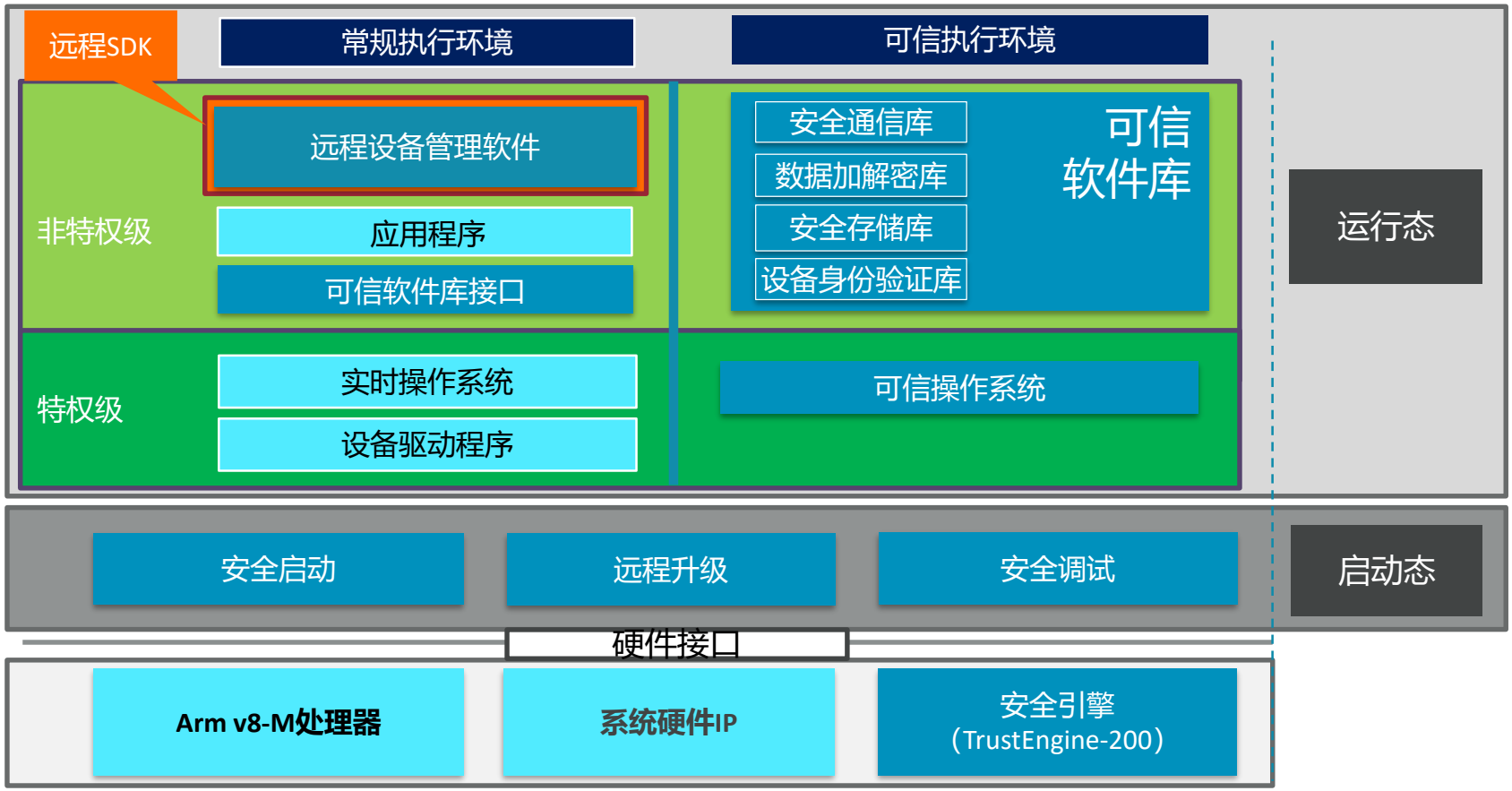
支持国密算法

除了国际主流加密算法，”山海”方案也率先支持国密算法加速

满足国密要求的真随机数发生器

arm CHINA

山海安全方案框架



arm CHINA

典型的应用案例

智能锁

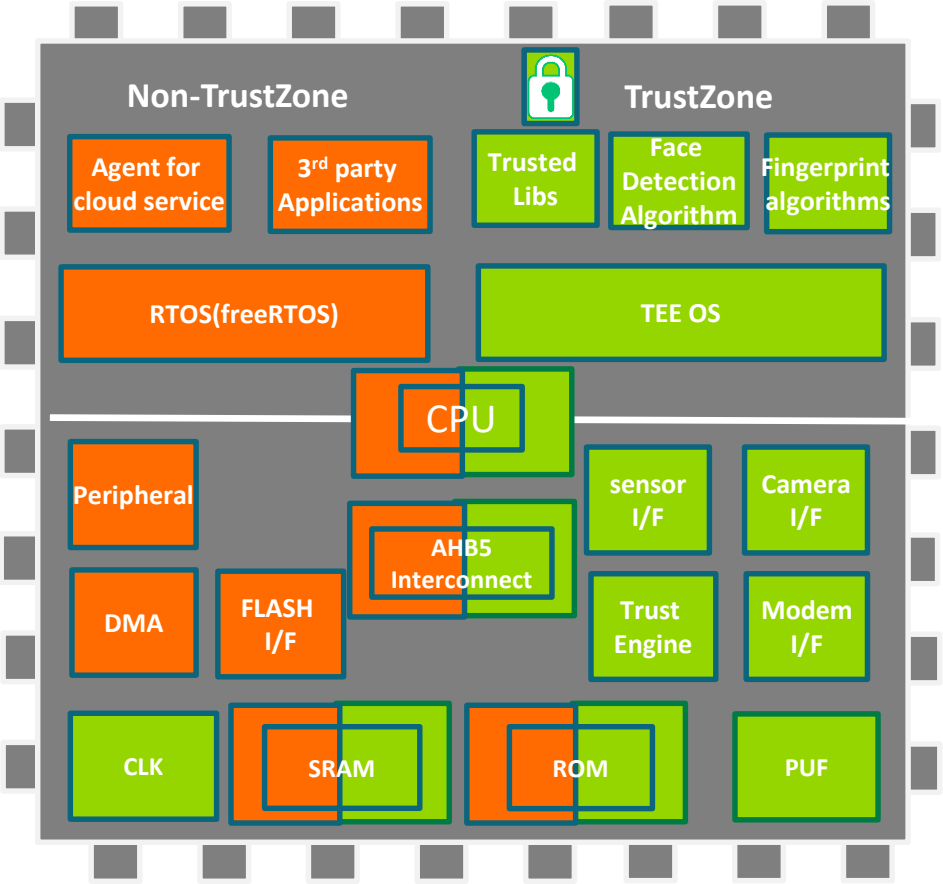
#1 CPU with TrustZone
- 允许软件运行在可信区/非可信区

#2 Agent SW
- 支持设备软件远程升级和设备远程管理

#3 第三方应用
- 认证过的第三方软件可以部署在可信执行区域

#4 外围电路接口
- 外围电路可以开放给第三方用于应用开发

#5 存储系统
- 一个物理存储系统可以被区分成安全/非安全两个区域



#6 可信应用
- 可信应用程序存储在安全区，代码和数据对非安全区不可见

#7 可信硬件
- 可信硬件资源对非安全区不可见

#8 硬件隔离
- 互联系统确保安全区和非安全区在系统上相互隔离

#9 安全引擎
- 进行加解密运算
- 密钥管理和鉴权
- 生命周期管理

#10 信任根
- 信任根可以被PUF技术进行进一步保护

arm CHINA

谢 谢
Thanks

arm CHINA

www.armchina.com