



FTF 2016
TECHNOLOGY FORUM CHINA

使用QorIQ处理器来保护 您的IoT设备

FTF-NET-N1872

任晓锋

软件研发经理

2016年9月29日



议程

- 安全性成为物联网部署的一大障碍
- 安全威胁的类型
- 安全性解决方案



安全性成为物联网部署 的一大障碍

物联网安全性

2014年公开披露的**215**个安全漏洞暴露了超过**850**万条个人记录。
– 隐私权情报交换所

到**2020**年，将存在一个价值超过**50**亿美元的黑市，销售伪造传感器和视频数据，用于从事犯罪活动和保护个人隐私 - **Gartner**

物联网黑客攻击示例



汽车

- 黑客攻击远程信息处理（如OnStar），可：
 - 窃听
 - 控制ECU
 - 刷新ECU，触发TPMS值



销售点

- 安装在POS上的内存抓取程序
- POS泄漏信用卡信息



智能电视

- 用户数据泄漏
- 根访问和程序安装

利用的漏洞

缺陷验证

无符号代码

堆栈溢出

无ACL

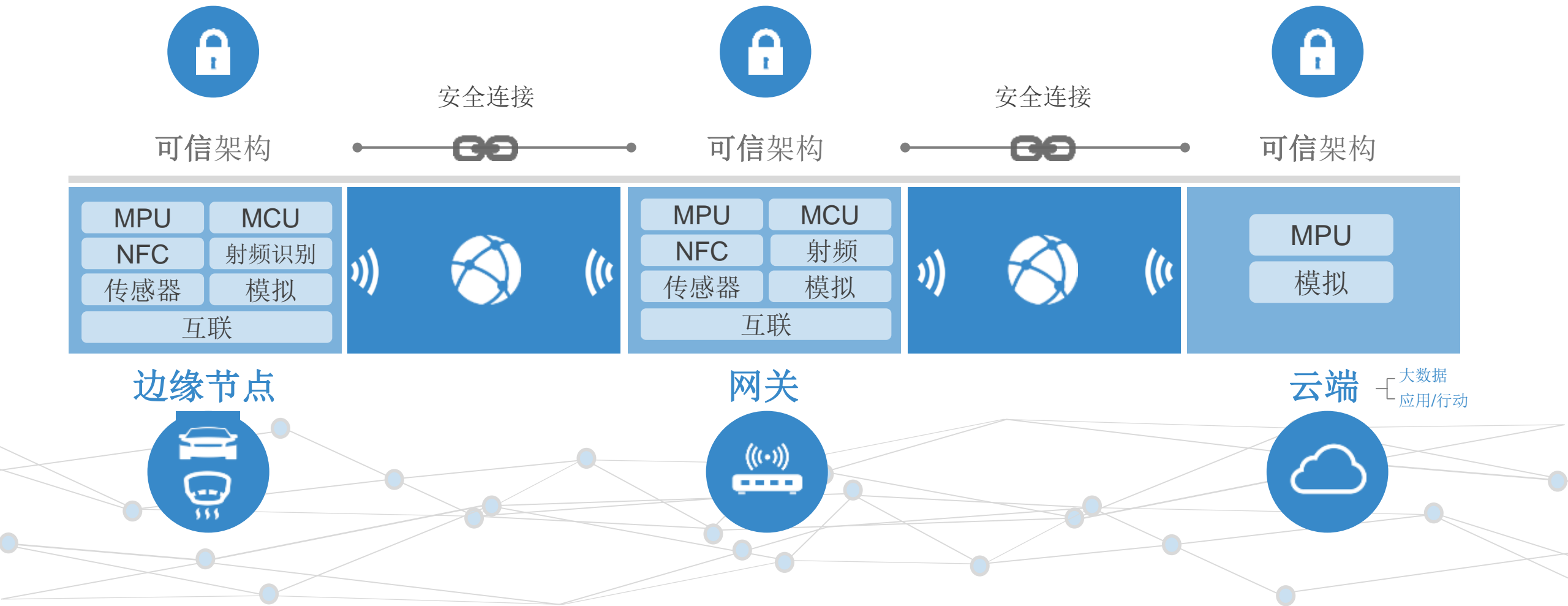
混杂通信

无端到端安全性

无存储器保护

安全威胁的类型

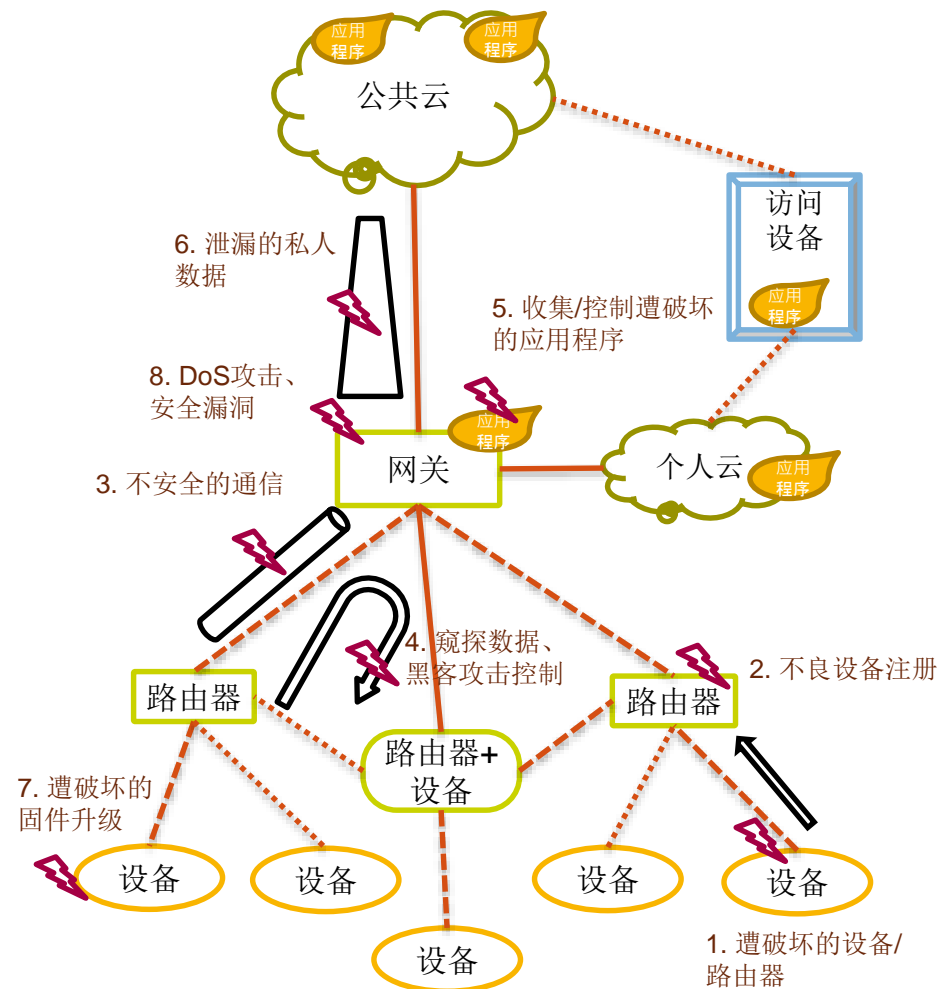
物联网安全性必须保护整个网络



物联网 – 安全问题

问题

1. 被入侵设备/路由器
2. 不良设备注册
3. 不安全的通信
4. 窥探数据、黑客攻击控制
5. 收集/控制遭破坏的应用程序
6. 泄漏的私人数据
7. 遭破坏的固件升级
8. DoS攻击、安全漏洞



安全性 解决方案



使用网关保护低成本终端节点

用作防火墙，并保护低成本节点免受外部攻击

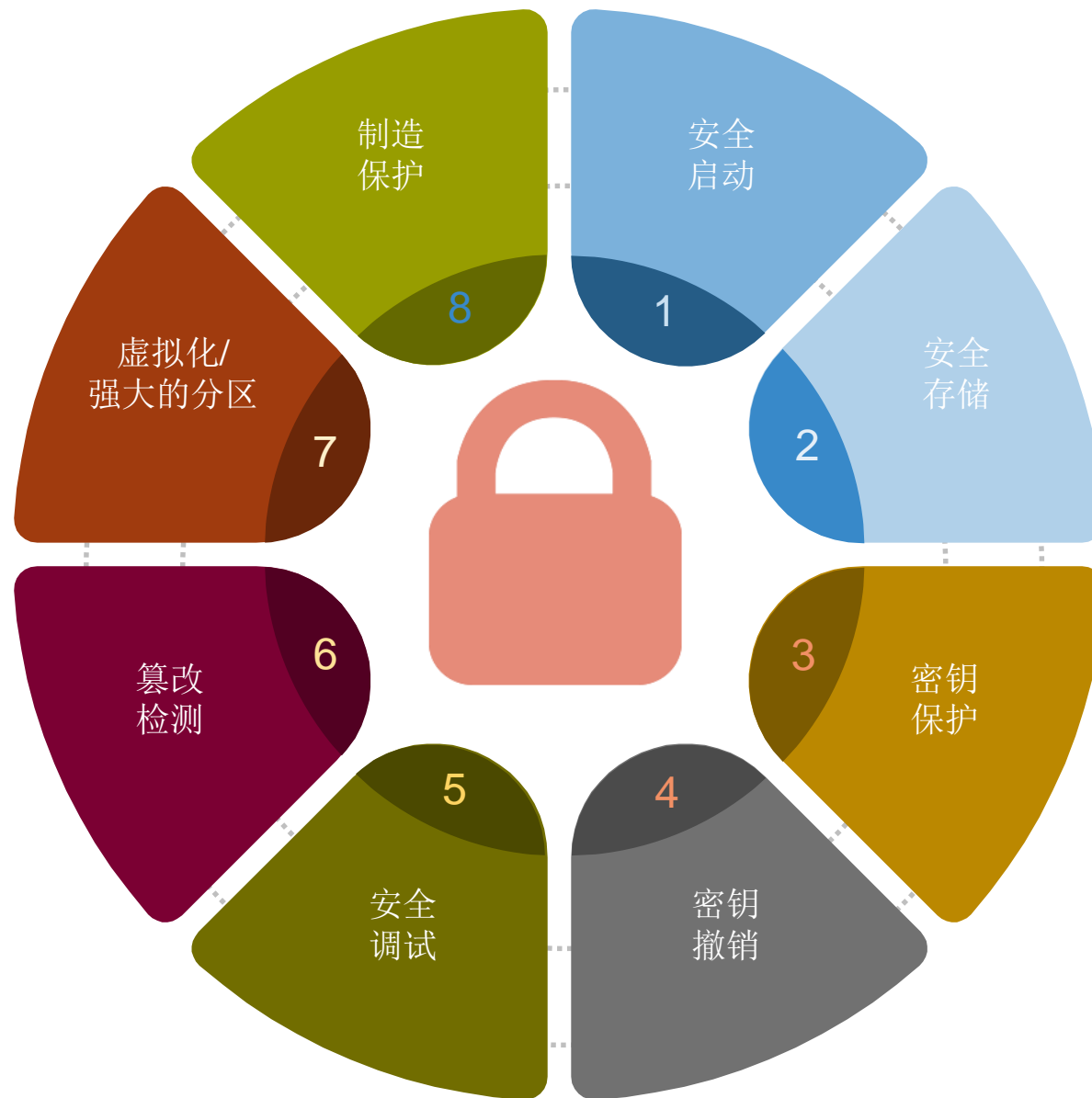
验证终端节点并检测不良设备

保护关键数据



可信架构

- 基于硬件的安全功能，可简化可信系统开发流程
- 所有QorIQ SoC支持可信架构



利用篡改检测阻止物理攻击

- 检测篡改

- 安全调试控制器

- 挑战 - 响应

- 篡改引脚

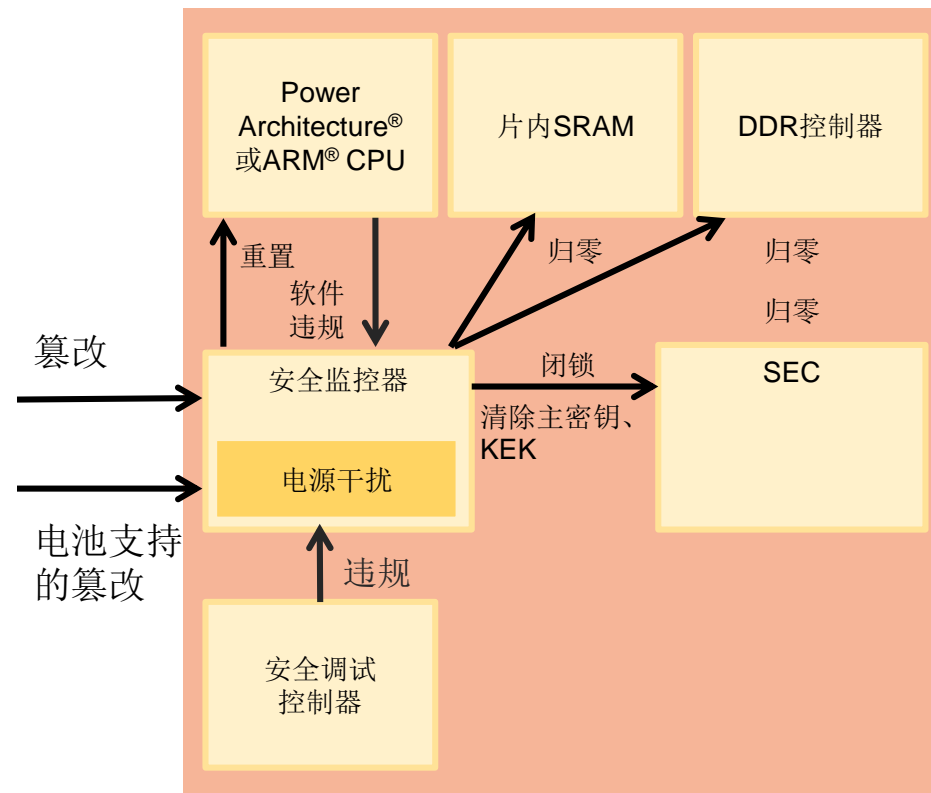
- 连接至外部传感器

- 电源干扰

- 保护系统

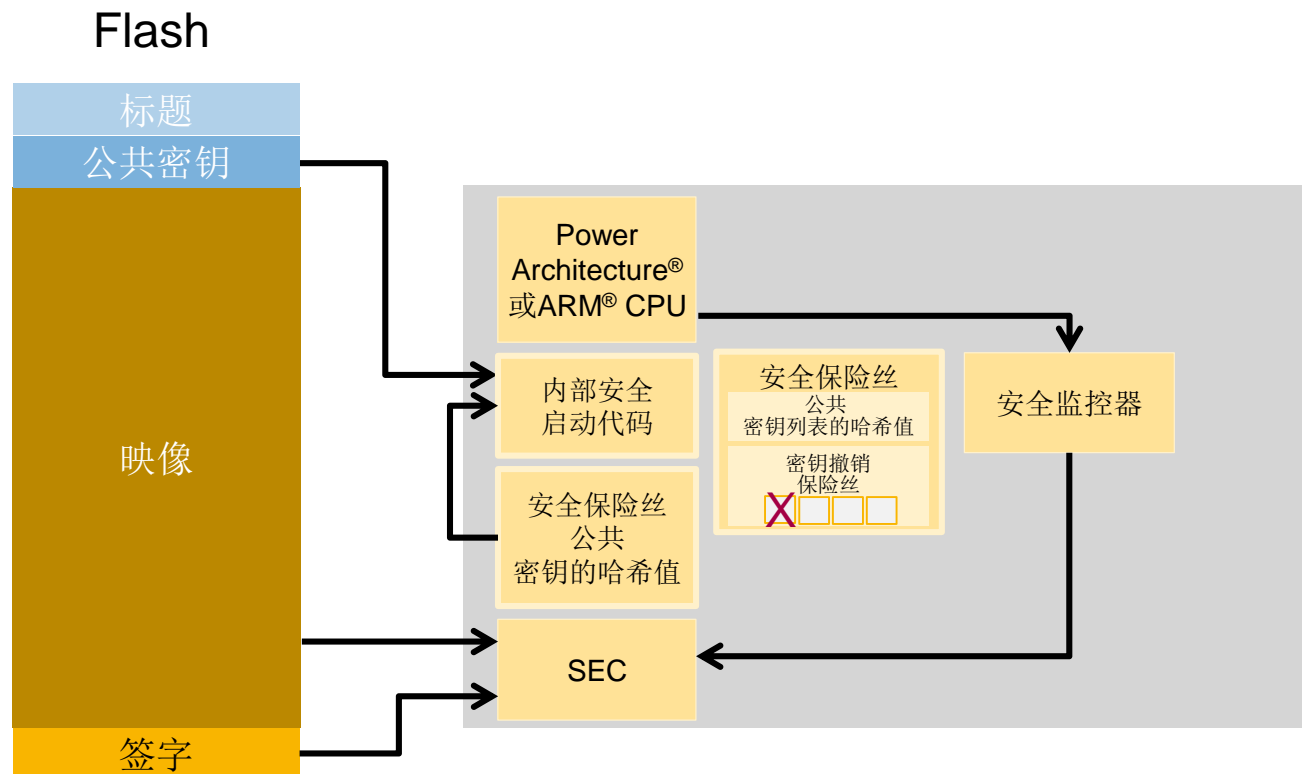
- 过渡到故障防护状态

- 对片内SRAM、DDR、主密钥进行归零



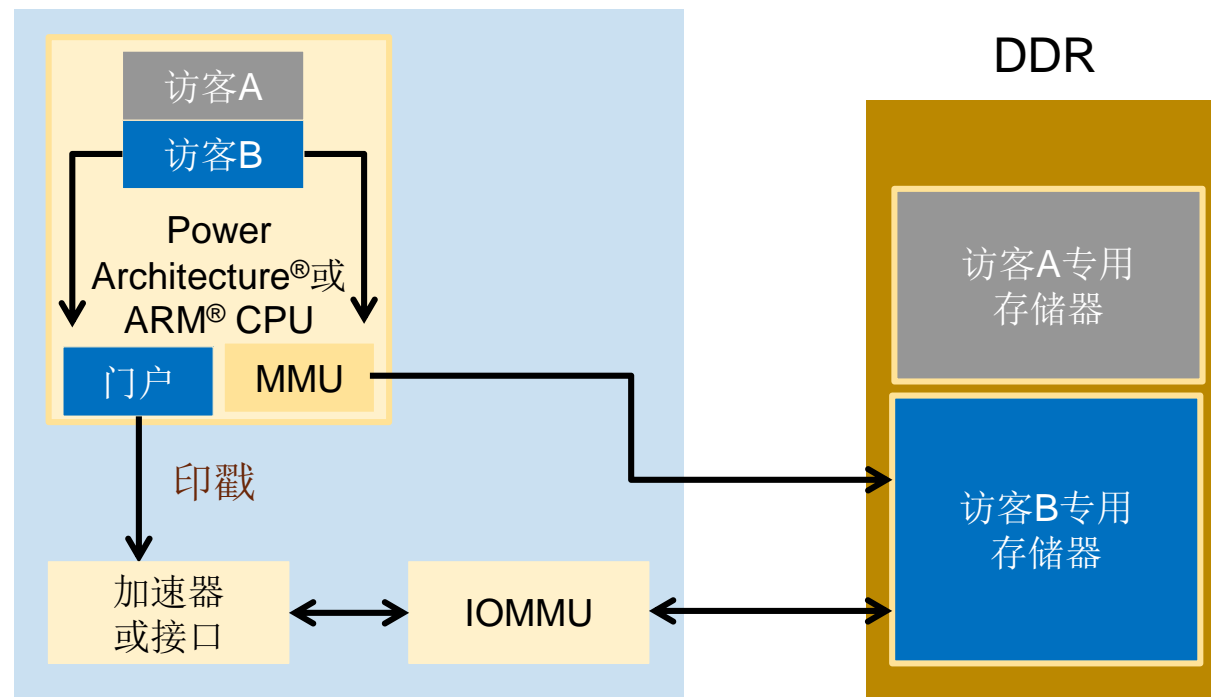
防止未经授权的固件映像

- 安全启动仅确保经签字的映像将在SoC上运行
- 密钥撤销可防止攻击者运行较旧的固件映像
 - OEM可撤销写入模块中的保险丝密钥，以防止较旧映像启动



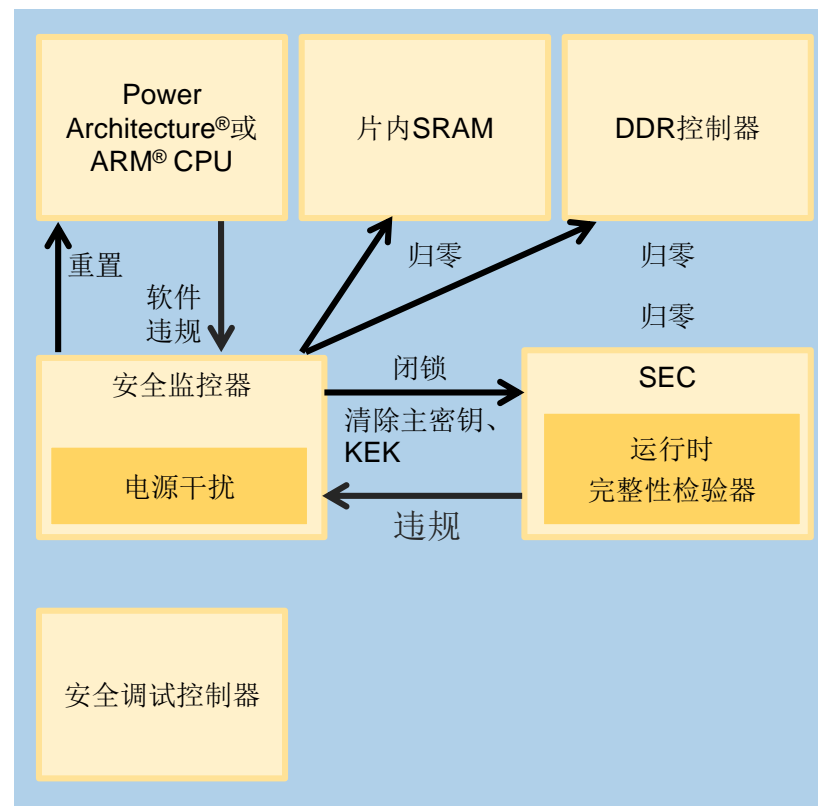
防范遭破坏的应用程序

- 虚拟化具有强大分区
- SoC保护每个VM的存储器和IO
- 单个VM中遭破坏的应用程序无法访问其他VM中的信息或资源

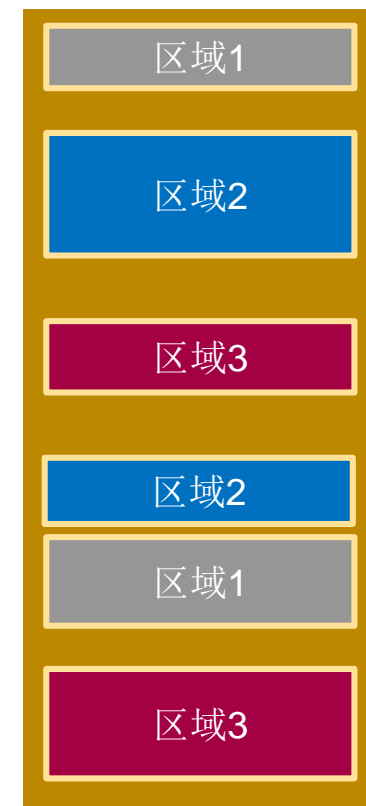


防止尝试覆盖存储器

- SEC引擎针对哈希值验证存储器的定义区域
- 故障产生篡改事件

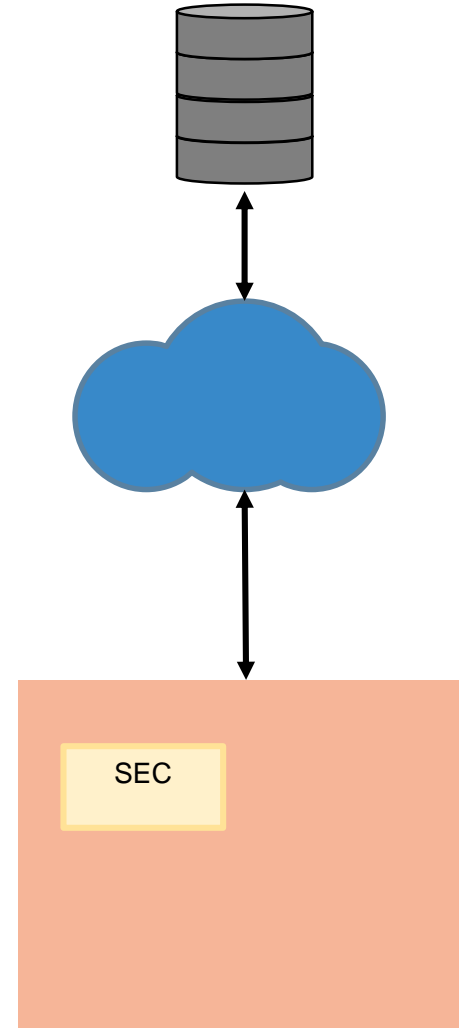


存储器映射



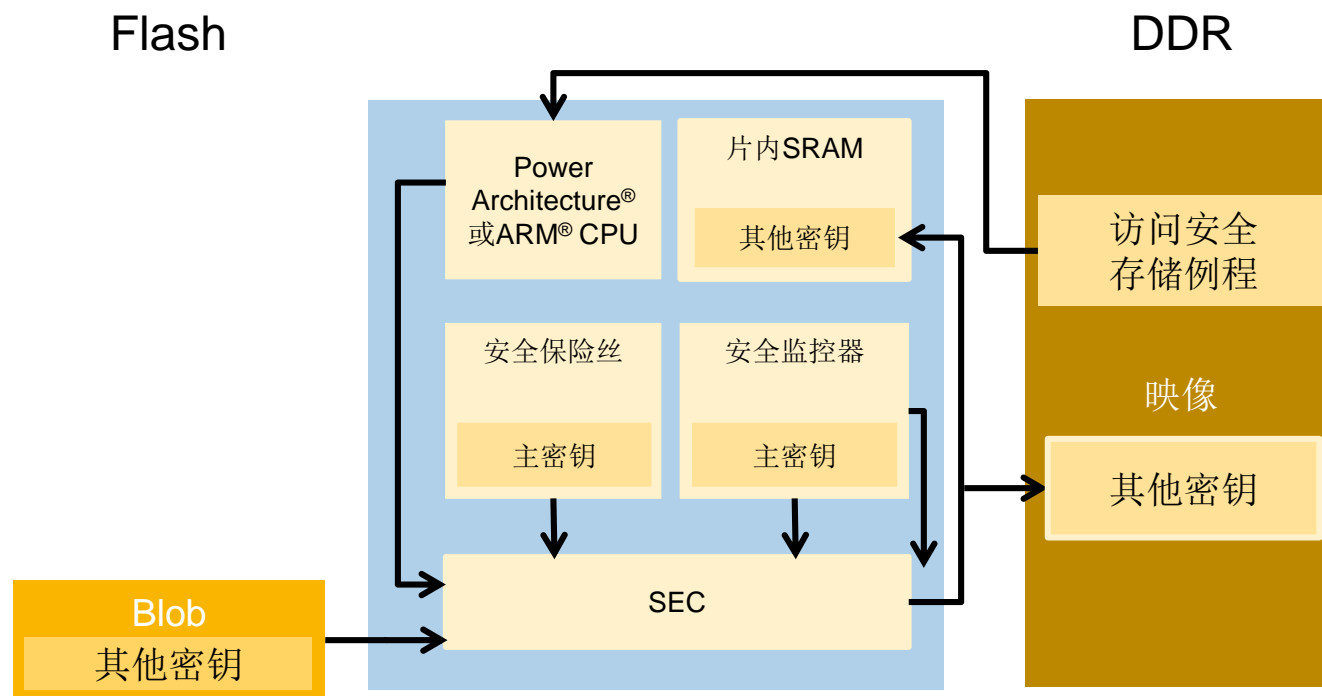
通过端到端加密保护用户数据

- 使用IPSec、TLS、DTLS通过网络传输私人数据
- SEC引擎可以加密数据并保存CPU周期进行分析



保护本地用户数据

- 加密存储在闪存中的敏感数据



小结

- 物联网系统必须以安全性为设计理念
- 可信架构提供基于硅芯片的平台以确保网关是安全的
- 安全网关能有助于保护传感器免受外部网络威胁



软件产品和服务

开发工具

- CodeWarrior

运行时间产品

- VortiQa软件解决方案

CodeWarrior
QorIQ

VortiQa



解决方案参考

- 物联网网关
- OpenWRT+

集成服务

- 安全咨询
- 强化Linux

Linux®服务

- 商业支持

- 性能调谐



加快客户产品上市时间



提供商用软件、支持、服务和解决方案



简化恩智浦软件开发流程



创造成功!



其他资源

[可信系统技术](#)

[可信架构：飞思卡尔用于工业控制系统的安全解决方案](#)

联系人

Jeffrey.Steinheider@nxp.com



SECURE CONNECTIONS
FOR A SMARTER WORLD

版权声明

恩智浦、恩智浦徽标、恩智浦“智慧生活，安全连结”、CoolFlux、EMBRACE、GREENCHIP、HITAG、I2C BUS、ICODE、JCOP、LIFE VIBES、MIFARE、MIFARE Classic、MIFARE DESFire、MIFARE Plus、MIFARE Flex、MANTIS、MIFARE ULTRALIGHT、MIFARE4MOBILE、MIGLO、NTAG、ROADLINK、SMARTLX、SMARTMX、STARPLUG、TOPFET、TrenchMOS、UCODE、飞思卡尔、飞思卡尔徽标、AltiVec、C 5、CodeTEST、CodeWarrior、ColdFire、ColdFire+、C Ware、高效解决方案徽标、Kinetis、Layerscape、MagniV、mobileGT、PEG、PowerQUICC、Processor Expert、QorIQ、QorIQ Qonverge、Ready Play、SafeAssure、SafeAssure徽标、StarCore、Symphony、VortiQa、Vybrid、Airfast、BeeKit、BeeStack、CoreNet、Flexis、MXC、Platform in a Package、QUICC Engine、SMARTMOS、Tower、TurboLink和UMEMS是NXP B.V.的商标。所有其他产品或服务名称均为其各自所有者的财产。ARM、AMBA、ARM Powered、Artisan、Cortex、Jazelle、Keil、SecurCore、Thumb、TrustZone和 μ Vision是ARM Limited（或其子公司）在欧盟和/或其他地区的注册商标。ARM7、ARM9、ARM11、big.LITTLE、CoreLink、CoreSight、DesignStart、Mali、mbed、NEON、POP、Sensinode、Socrates、ULINK和Versatile是ARM Limited（或其子公司）在欧盟和/或其他地区的商标。保留所有权利。Oracle和Java是Oracle和/或其关联公司的注册商标。Power Architecture和Power.org文字标记、Power和Power.org徽标及相关标记是Power.org的授权商标和服务标记。© 2015–2016 NXP B.V.

