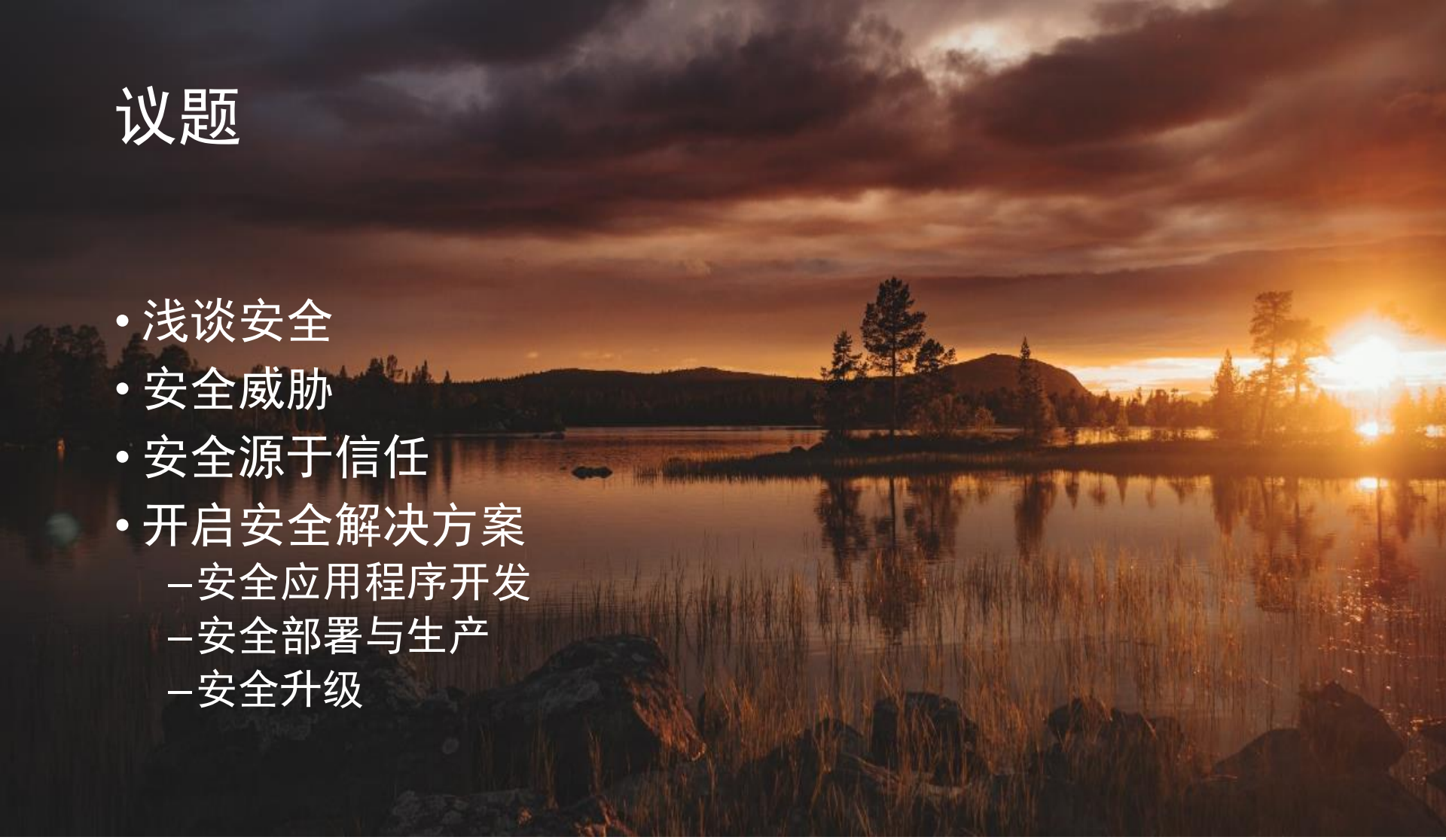
开启物联网安全应用软件解决方案

Cynthia Hu
IAR Systems (China)

议题



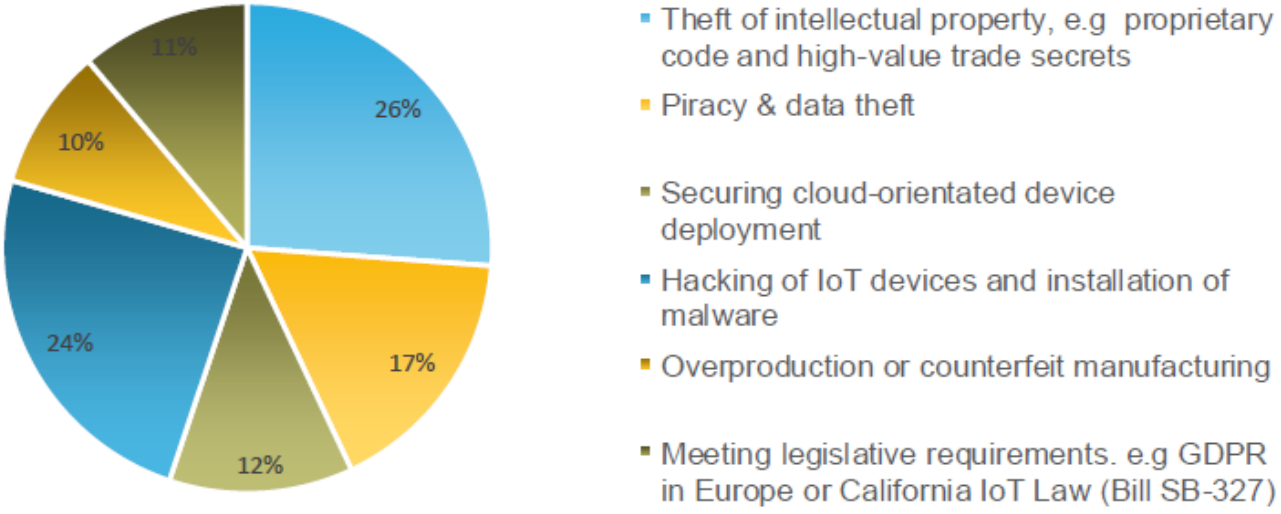
- 浅谈安全
- 安全威胁
- 安全源于信任
- 开启安全解决方案
  - 安全应用程序开发
  - 安全部署与生产
  - 安全升级

浅谈安全

安全需求的市场调查

Which is your #1 security concern?

We asked our customers this question in September 2019, and this is the answers we got.



调查结果中最关注的安全问题有：

- 知识产权的窃取
- 隐私和数据窃取
- 安全云端部署
- 黑客入侵IoT设备并安装恶意软件
- 过量生产和仿冒生产
- 符合法律法规，例如欧盟的GDPR或者加利福尼亚IoT法案（Bill SB-327）

“好”的安全很“难”实现

- 不同的人对于安全的理解以及需求不同
- 成本，研发进度，上市时间等因素优先于安全实施
- 安全的程度很难量化
- 不知道从何处着手在产品中添加安全功能
- 安全方案的考量：
  - 目前为止，还没有令所有人满意，或者说绝对安全的解决方案
  - 安全开发必须从一种专属技能转变为主流开发流程
  - 安全设计必须贯穿整个项目始末以及产品生命周期

安全基本原则（CIA/IIA）

身份鉴定与保密性（Identify & Confidentiality）

- 往往与加密相混淆—实际上保密具有更多的含义
- 核心是根信任（Root Of Trust) = 身份ID (一组密钥与证书)
- 验证设备的身份是否与其宣称的一致
- 身份ID是建立加密路径的基础

完整性（Integrity）

- 可依赖的框架确保设备授权和恢复到已知状态的稳健性。
- 尤其是处理恶意攻击以及通过升级来修正缺陷的能力
- 依赖于原始的身份ID来实现安全启动流程

可用性（Availability ）

- 一旦系统遭到破坏，访问将遭到限制
- 需要通过硬件相关技术的协助得以实现，比如Trust Zone ， Secure Enclaves 以及 Functional Separation 等

安全威胁

攻击向量– 信任锚点

- Rich OS/RTOS以及和通信协议栈中所提供的安全服务是依赖于较低层的信任锚和服务，原因是：
  - 第二层次之上的攻击面急剧增加
  - 代码的行数越多，OS/服务协议就越复杂，漏洞就越多
- 硬件信任根（RoT, Root of Trust）
  - 通常不容易受到软件攻击
  - 针对软件漏洞的定制化攻击几乎是不可能奏效的
  - 具有防篡改功能使得加密信息得到有效保护
- 安全启动服务
  - 一小段软件代码，具有最小的暴露水平
  - 具备恢复管理功能
  - 升级和修补功能可以帮助系统在受到攻击时保留弹性

攻击向量类型

在物联网环境中，通常会出现以下攻击类型:

- 中间人攻击（MITM，Man in the Middle）
  - 攻击者或黑客拦截两个系统之间的通信。攻击者冒充原始发送者，因此非常危险。攻击者欺骗接收者以为他们正在接收合法通信。
- 黑客攻击
  - 黑客攻击是指黑客在线执行软件攻击的一种方式。比如植入病毒和恶意软件，这些病毒和恶意软件是通过物理或无线连接下载到设备的。
- 窃听
  - 监听以太网流量
- 棚屋攻击（Shack Attack）
  - 低预算的硬件攻击，使用的设备可以在街边商店就可以购买（比如无线电设备）。攻击者与设备发生物理接触，但没有足够的设备或专业知识来攻击集成电路封装的内部。
- 实验室攻击Lab Attack
  - 实验室攻击向量是最全面和最具侵入性的。如果攻击者可以使用电子显微镜等实验室设备，则他们可以对设备进行不受限制的反向工程。这类攻击者具备可以对晶体管级别的任何敏感部分设计进行反向工程的能力（包括逻辑和存储器）进行反向工程晶体管级细节。
  - .
- DoS攻击
  - 拒绝服务攻击

安全源于信任

如何实现“信任”

- 我们需要一种不可伪造的方式来进行身份验证
  - OEM是否与由他所生产的设备进行通信吗？
  - 在设备上运行的是否是合法固件？
  - 设备如何知道它正在与OEM交流？
  - 设备如何知道固件升级版本是由OEM发布的？

- 如何实现身份验证
  - 每个设备需要有一个唯一的身份标识（Unique ID）
  - 通过可靠的加解密技术来随机生成密钥对，可以确保其唯一性

- 设备固件中的可信任部分不能被更改
  - 通常为一段Boot loader程序
  - 需要将Boot loader程序存储在一段被保护的存储区域中（不可访问，不可改写或者擦除）

信任根（Root of Trust）

- 信任根定义
  - “平台中可绝对信任的软件，硬件和数据的最小集合...”

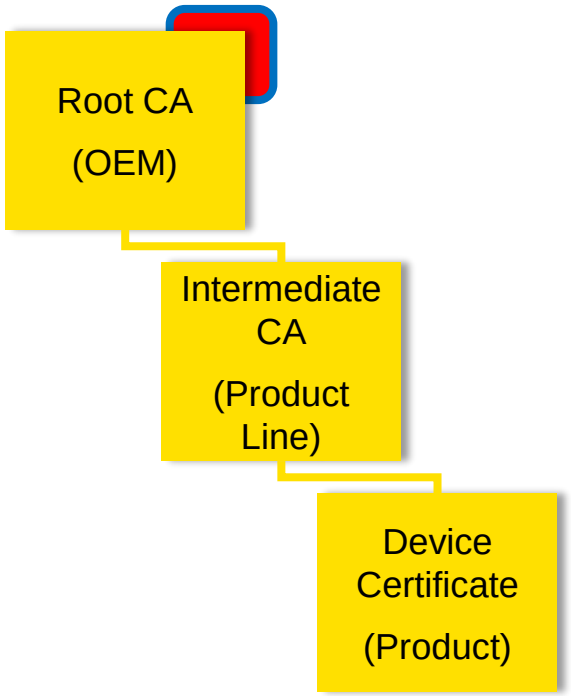
- 安全MCU/硬件必须具备:
  - 唯一标识 (芯片序列号)
  - 用于存储证书和密钥的受保护的存储区域
  - 用于软件安全下载与保护的安全存储管理
  - 硬件加解密单元（可选）

- 安全启动管理
  - 不可变更的引导路径，不能被调试接口中断
  - 确保加载到不安全内存中的软件已被正确签名（身份验证）并在烧写之前进行解密
  - 在执行应用代码之前进行验证 (签名检查，哈希算法)

- 信任链的构建始于信任根

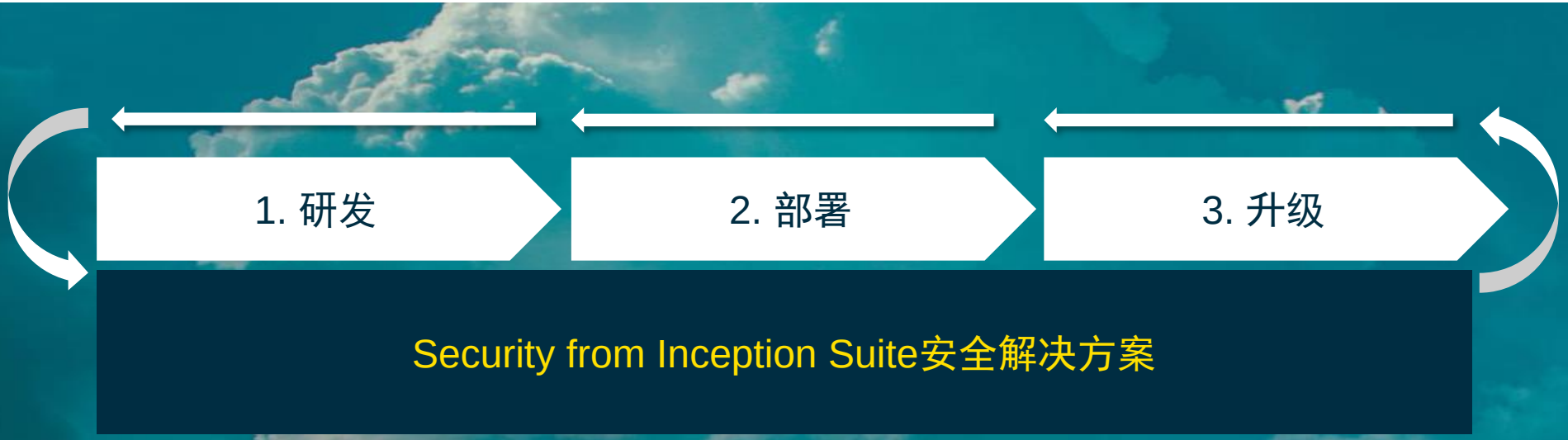
信任链---多级证书管理

- **传统互联网证书架构**
  - X.509, CRL, CSR等.
  - 依赖第三方CA
- **许多OEM选择自我认证**
  - 独特的证书结构和模板
  - 最简洁的X.509类型证书
  - 确保长期有效的所有权
  - 利用第三方CA（DigiCert，GlobalSign等）
- **定制符合物联网需求的层次化证书管理系统**
  - 根证书/中间证书/设备证书
  - 基于PC或者HSM
  - 灵活的证书配置：研发证书/量产证书



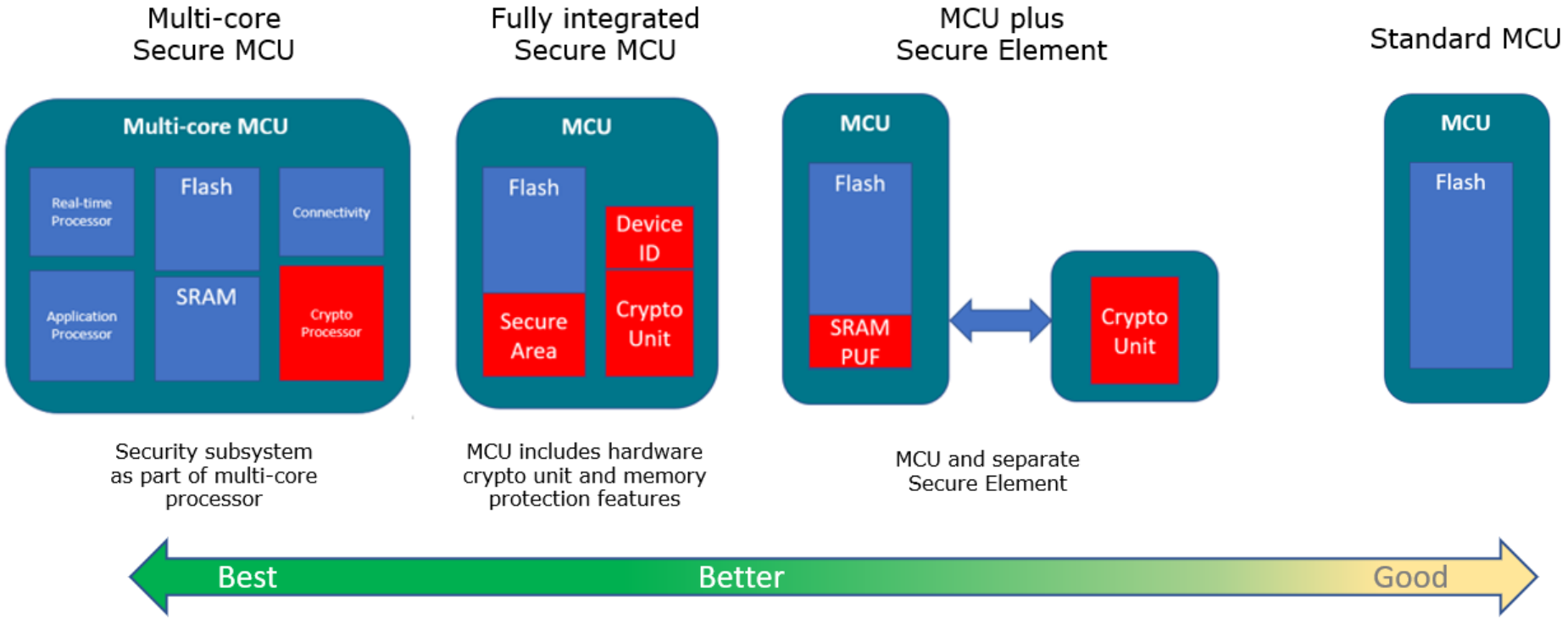
开启安全解决方案

贯穿物联网产品整个生命周期的安全解决方案



1. 安全研发流程包括制定安全策略，保护应用软件IP
2. 安全部署包括预配置与安全生产
3. 安全升级为产品的持续安全性保驾护航

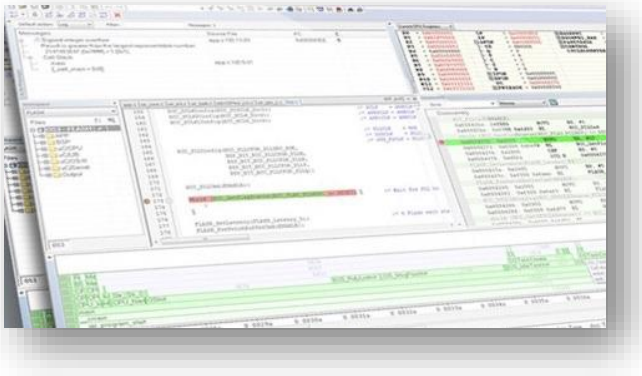
选择安全MCU架构


Multi-core
Secure MCU
Fully integrated
Secure MCU
MCU plus
Secure Element
Standard MCU
Multi-core MCU
Real-time Processor
Flash
Connectivity
Application Processor
SRAM
Crypto Processor
MCU
Flash
Device ID
Secure Area
Crypto Unit
MCU
Flash
SRAM PUF
Crypto Unit
MCU
Flash
Security subsystem as part of multi-core processor
MCU includes hardware crypto unit and memory protection features
MCU and separate Secure Element
Best
Better
Good

传统软件开发流程

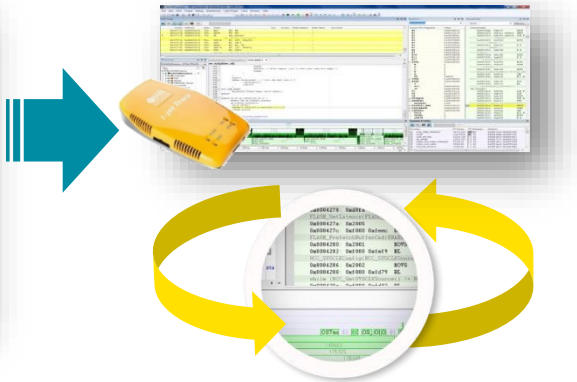
开发应用程序 → 测试 → 发布 → 生产 → 管理

设计和开发应用代码



使用静态代码工具发现代码缺陷

编译调试应用程序



发现并修正运行时错误

发布用于生产的映像文件

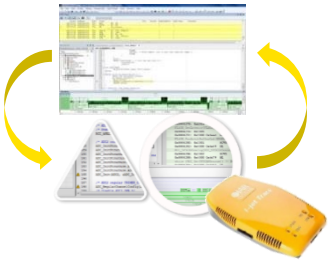
安全软件开发流程

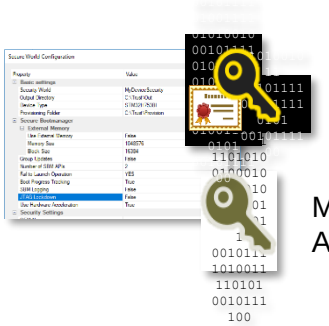
开发安全上下文 → 编译SBM，预配置芯片 → 开发应用程序 → 测试 → 部署 → 生产 → 管理

创建安全上下文，编译安全启动管理程序（SBM）并将这些安全相关的内容预配置入芯片受保护的内存中

使用开发密钥来开发和测试应用程序

先使用生产密钥来构建程序，然后再部署生产





SBM

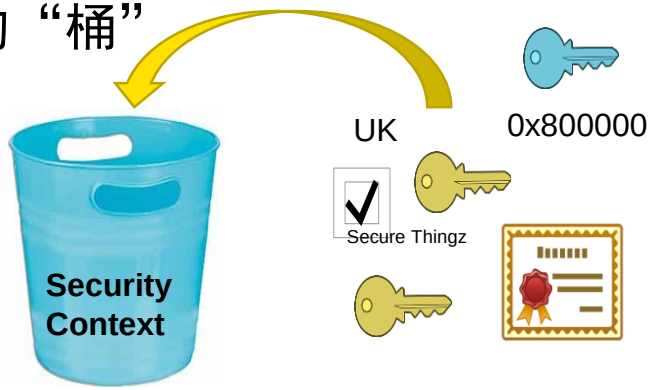
Mastered Application

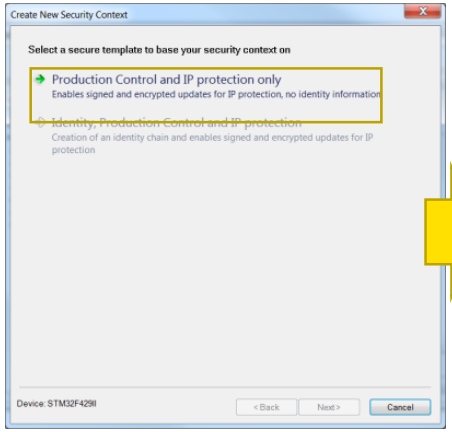
SECURE THINGZ

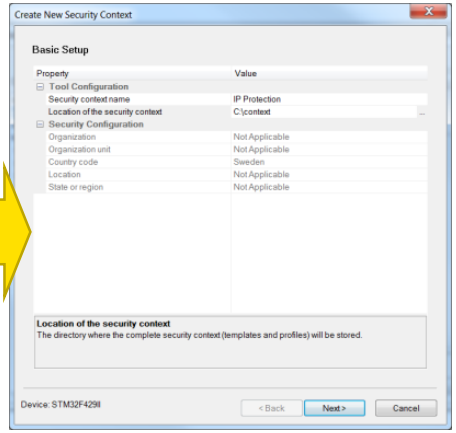
IAR SYSTEMS

安全上下文（Security Context）

- 一个包含了所有安全设置（规则和数据）的“桶”
- 根据这些安全设置可以生成：
  - 预配置信息(provisioning)
  - 制作生产文件 (mastering)
  - 安全启动管理器的选项标志 (SBM代码生成)
- 内容
  - 密钥，证书和身份标识(导入和生成)
  - 生成设备身份和原始数据规则
  - 软件升级和上电检测规则
  - 版本管理规则
  - 内存布局与SBM配置
- 初始化向导(快速设置) 和编辑器

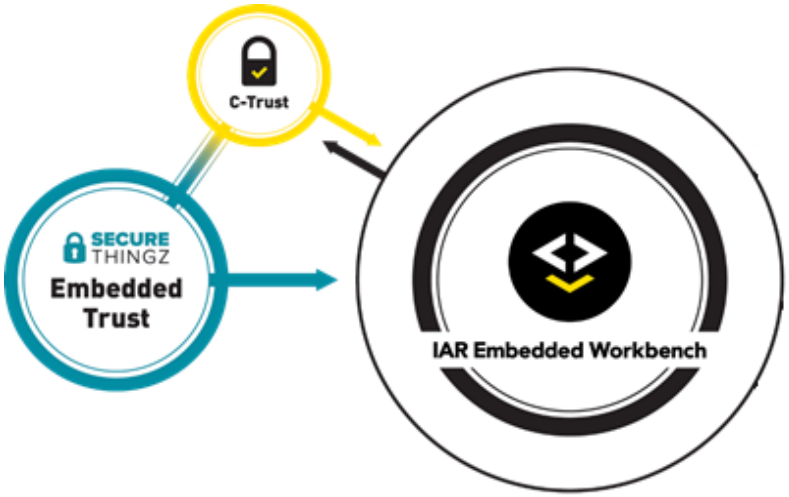


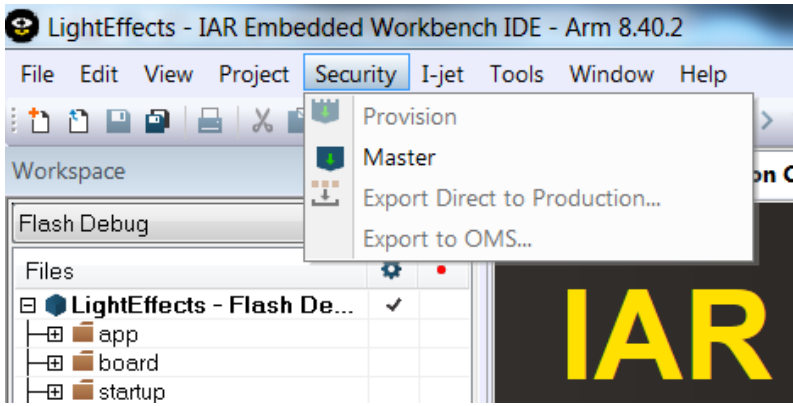




Embedded Trust和C-Trust

- 无缝融入日常研发流程
- 由安全架构师创建制定安全策略
- 支持密钥证书创建与管理
- 预配置安全策略与SBM
- 应用开发团队一键导入安全策略
- 自动交付经过AES加密的映像文件，防止IP窃取
- 支持量产文件制作与导出

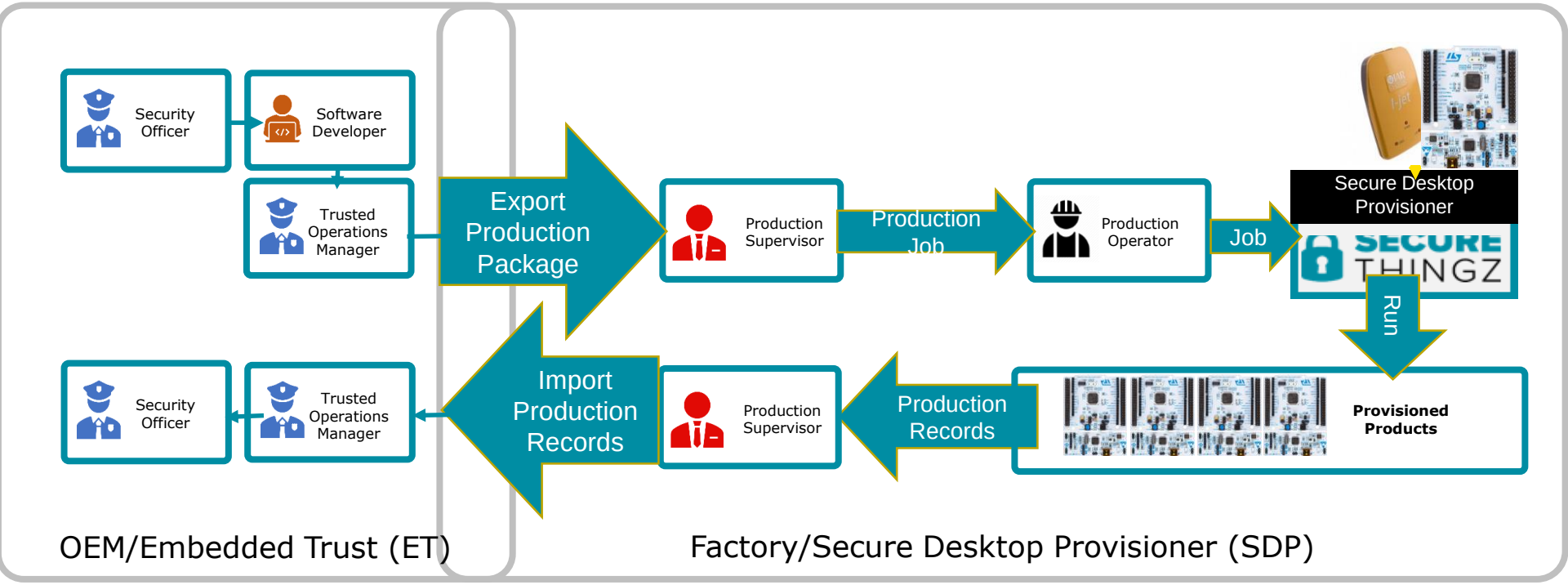




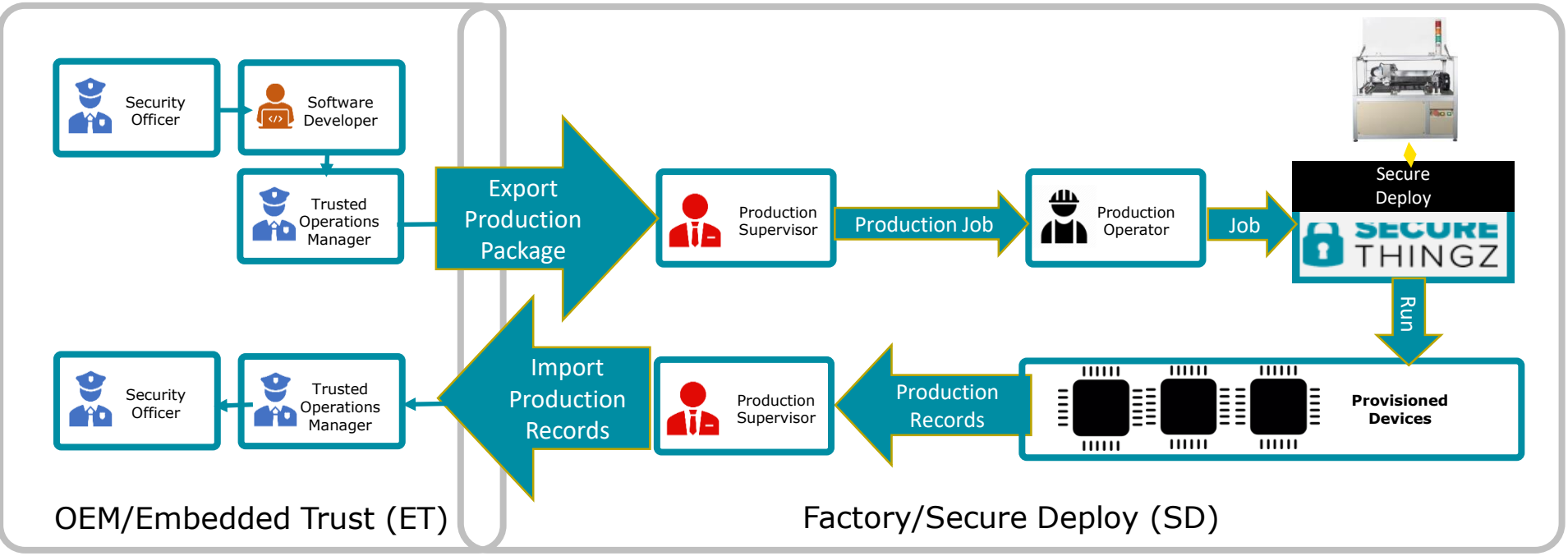
安全生产


All the news is about attacks here i.e. IoT devices in service
But attacks can also occur here …
Silicon Platform Vendor
Software Application Developer
IoT Device OEM
Programming Centre
Contract Manufacturer
End User
… and here

安全桌面烧写流程

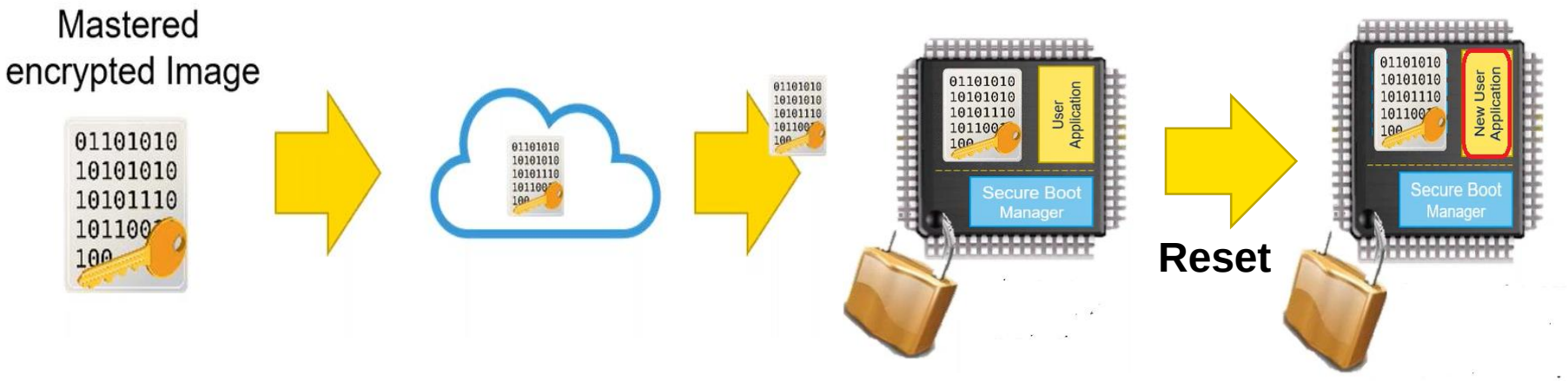

Security Officer
Software Developer
Trusted Operations Manager
Export Production Package
Production Supervisor
Production Job
Production Operator
Job
Secure Desktop Provisioner
SECURE THINGZ
Run
Provisioned Products
Production Records
Production Supervisor
Import Production Records
Security Officer
Trusted Operations Manager
OEM/Embedded Trust (ET)
Factory/Secure Desktop Provisioner (SDP)

安全部署流程


Security Officer
Software Developer
Trusted Operations Manager
Export Production Package
Production Supervisor
Production Job
Production Operator
Job
Secure Deploy
SECURE THINGZ
Run
Provisioned Devices
Production Records
Production Supervisor
Import Production Records
Security Officer
Trusted Operations Manager
OEM/Embedded Trust (ET)
Factory/Secure Deploy (SD)

OTA升级

- 将升级软件程序加密并签名
- 通过网络下载到芯片的升级槽（Update slot）
- 重启芯片，SBM将对升级槽中的软件升级包进行验证，若验证成功，则对其进行解密，并将其更新到应用程序执行区域
- 执行升级后的应用程序



产品与服务

提供安全开发所需的所有产品：

- Embedded Trust安全开发环境
- IAR Embedded Workbench for Arm集成开发环境
- C-Trust for IAR Embedded Workbench安全开发工具
- C-STAT集成静态分析工具
- I-jet高速在线硬件调试器

提供培训课程以及咨询服务来帮助您分析和解决所面临的安全挑战：

- 威胁模型
- 关键资产和知识产权管理
- 安全法律法规对具体实施的影响
- 鉴定和证明
- 授权与认证
- 密钥最少化与系统简化
- 证书基础架构和安全的云连接
- 跨产品生命周期的升级与修复

Thank you for your attention!

iar.com

securethingz.com

SECURE THINGZ

IAR SYSTEMS