

防范安全漏洞、保护产品全生命周期安全， IAR端到端安全解决方案助您一步到位！

Late-Stage Security

IAR Embedded Secure IP

在开发过程的后期阶段中实现安全功能，为您的制造过程提供加密，有助于防止伪造。

Advanced Security

IAR Embedded Trust

从产品开发周期之初，就考虑将端到端安全性构建到产品设计和开发全流程中。

产品
开发
周期

功能亮点

与设备无关

将当前框架移植到新的MCU

重用代码

无需从头开发，应用代码可复用并快速完成移植到新MCU设备上

安全生产

使用HSM和加密机制安全地提供产品的授权生产

概念



Authentication 认证

- 安全启动
- 确保正版固件
- 确保产品完整性



未经授权的软件



Anti-cloning 防克隆

- 防止制造过程中的假冒和过度生产
- 防止收益损失
- 设备证书绑定设备唯一身份信息



Active IP Protection 主动IP保护

- 加密软件二进制代码
- 每个设备拥有唯一密钥
- 通过二进制代码加密来防止逆向工程



内存攻击
设备访问



Anti-rollback 防回滚

- 包括软件安全更新过程，防止软件版本降级
- 减轻已知安全漏洞的危险

产品已经完成

安全设计



Anti-cloning 防克隆

- 防止制造过程中的假冒和过度生产
- 防止收益损失
- 设备证书绑定设备唯一身份信息



Active IP Protection 主动IP保护

- 加密软件二进制代码
- 每个设备拥有唯一密钥
- 通过二进制代码加密来防止逆向工程



安全部署原型 (SDP)

- 加密生产包并提供授权设备
- 主要用于样品原型制作和小批量生产



安全部署原型 (SDP)

- 加密生产包并提供授权设备
- 主要用于样品原型制作和小批量生产

增加安全性

安全制造



安全部署制造 (SDM)

- 将加密生产包安全地传输到设备烧录服务商
- 生成唯一的设备证书和密钥以防止设备在生产过程中被伪造
- 通常用于大批量生产



安全部署制造 (SDM)

- 将加密生产包安全地传输到设备烧录服务商
- 生成唯一的设备证书和密钥以防止设备在生产过程中被伪造
- 通常用于大批量生产



IP窃取

生产
及发布



版本篡改

现场升级

了解更多

