

STM32安全的概念与系统分析方法

STM32 Security

MCU China 2019



Safety & Security

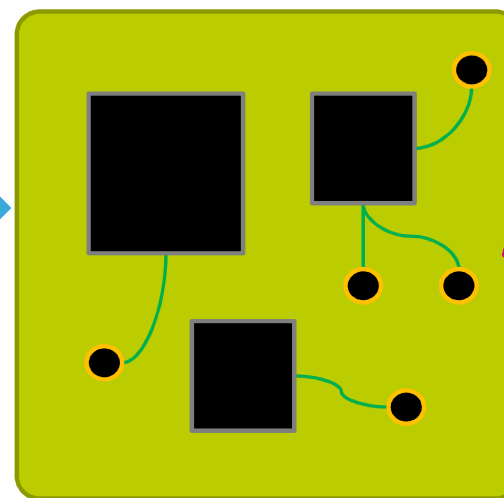
2

随机
故障



功能安全
Safety

安全?



恶意
攻击



信息安全
Security

STM32 功能安全Safety资源

3

	SIL Ready		ASIL Ready		ClassB Ready	
MCU						
功能安全标准	IEC 61508		ISO 26262		IEC, UL, CSA 60335-1 60730-1	IEC 60335-1
认证						
软件包内容	• Safety 文档 • 自测试软件库 (X-CUBE-STL)		Safety 文档		• Safety 文档 • 自测试软件库 (X-CUBE-CLASSB)	• Safety 文档 • 自测试软件库 for STM32 SPL • Safety 文档 • 自测试软件库
软件包名称	<u>X-CUBE-STL</u>		<u>STM8A-SafeASIL</u>		<u>X-CUBE-CLASSB</u>	<u>STM32-CLASSB-SPL</u> <u>STM8-SafeCLASSB</u>

Security的定义

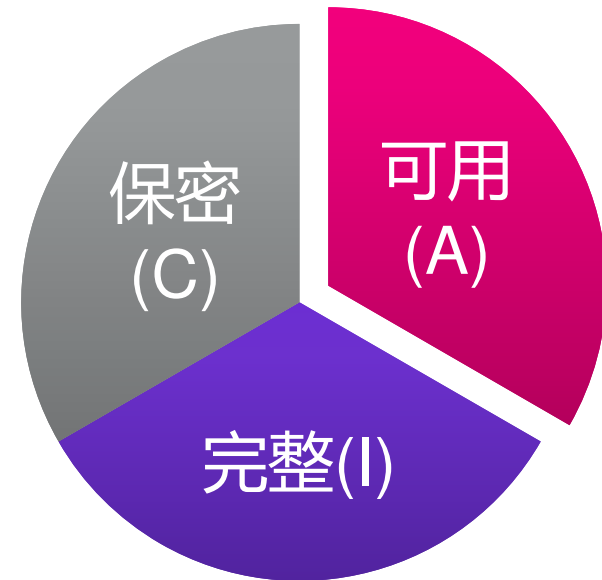
4

- 安全 (Security) 是保护资产，也就是有价值的对象，免受威胁的破坏
 - 威胁
 - 特定场景或者特定操作
 - 弱点
 - 对象总会存在弱点
 - 攻击者则利用弱点
- 信息安全 (Information Security) 则是保护完整可靠的数据仅被授权访问

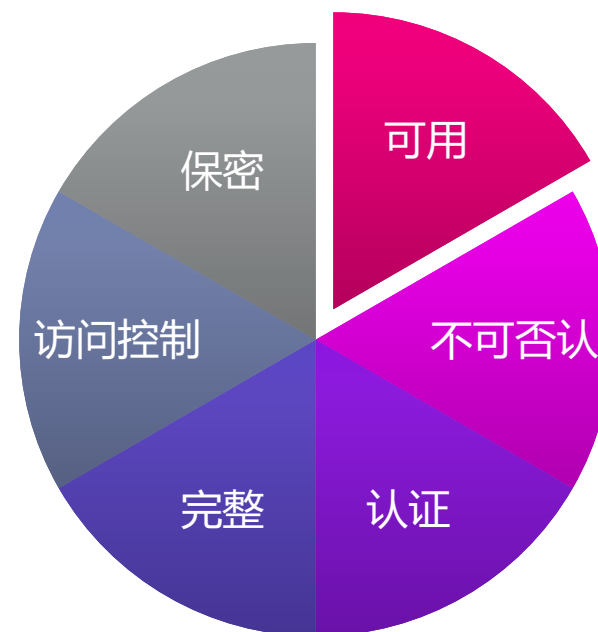
信息安全三要素

5

- 保密
 - 信息不能被未被授权的人得到
- 完整
 - 指信息未被破坏或者篡改
- 可用
 - 则指被授权的人总是需要时能得到它需要的信息



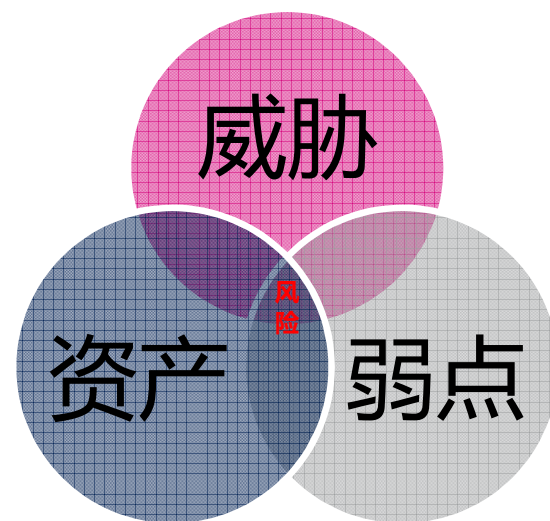
- 访问控制
 - 隔离
 - 权限
- 认证
 - 身份认证
- 不可否认
 - 消息认证



系统安全分析模型

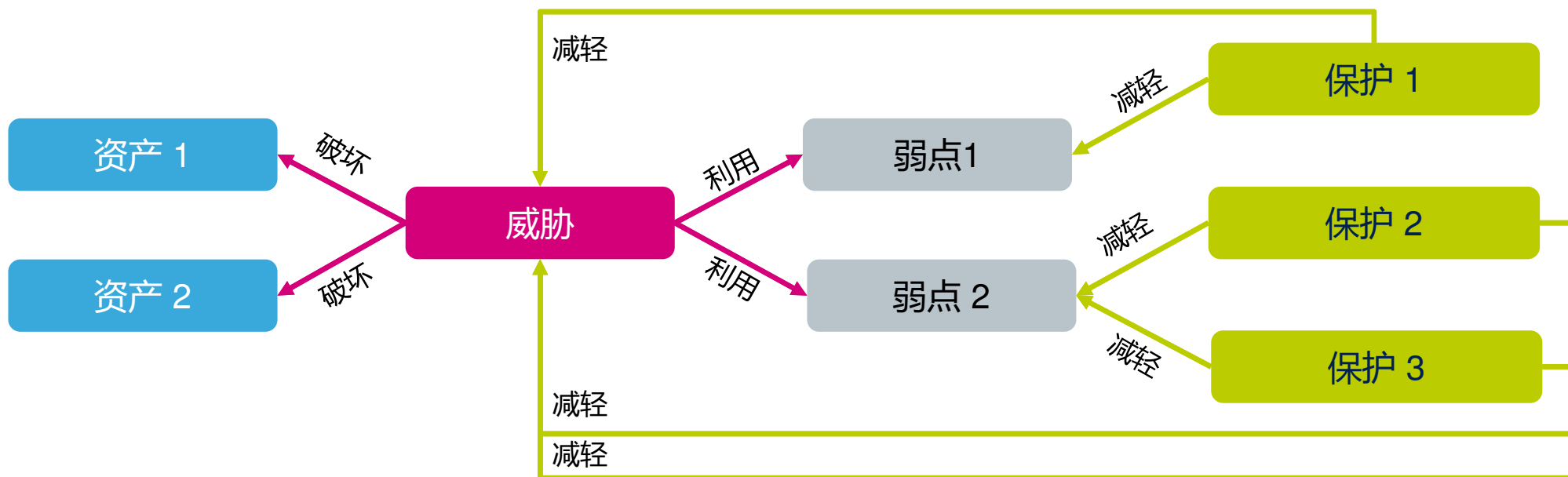
7

- 资产
 - 系统中有价值的对象
- 威胁
 - 利用系统弱点让资产价值损失，同时让恶意第三方获得利益的行为
- 弱点
 - 系统能够被外界非法利用的缺陷



系统安全分析流程

8



典型用户场景

9



- 列出所有资产
- 理解相关威胁
- 思考相关弱点

威胁分类

10

95%的攻击



成本上升, 时间增加



软件攻击

- 网络协议漏洞(不安全的算法, 密钥太短, 中间人)
- 软件设计/实现中的漏洞, 缓冲区溢出
- 调试接口, 管理员权限



板级攻击

- SPA / DPA, 辐射分析, 时间分析
- 故障注入: 故障, 激光, 光, UV, X-rays
- 内存探测



芯片级攻击

- 开盖, 电子线路逆向工程, 微探针
- 故障注入: FIB
- 高级显微镜

安全威胁应对

11

威胁

设备仿冒/破解

数据篡改

数据泄露



防护功能

安全通讯

安全启动

安全固件安装

安全升级

执行保护

代码保护

数据保护

保护资产的
安全属性



保密



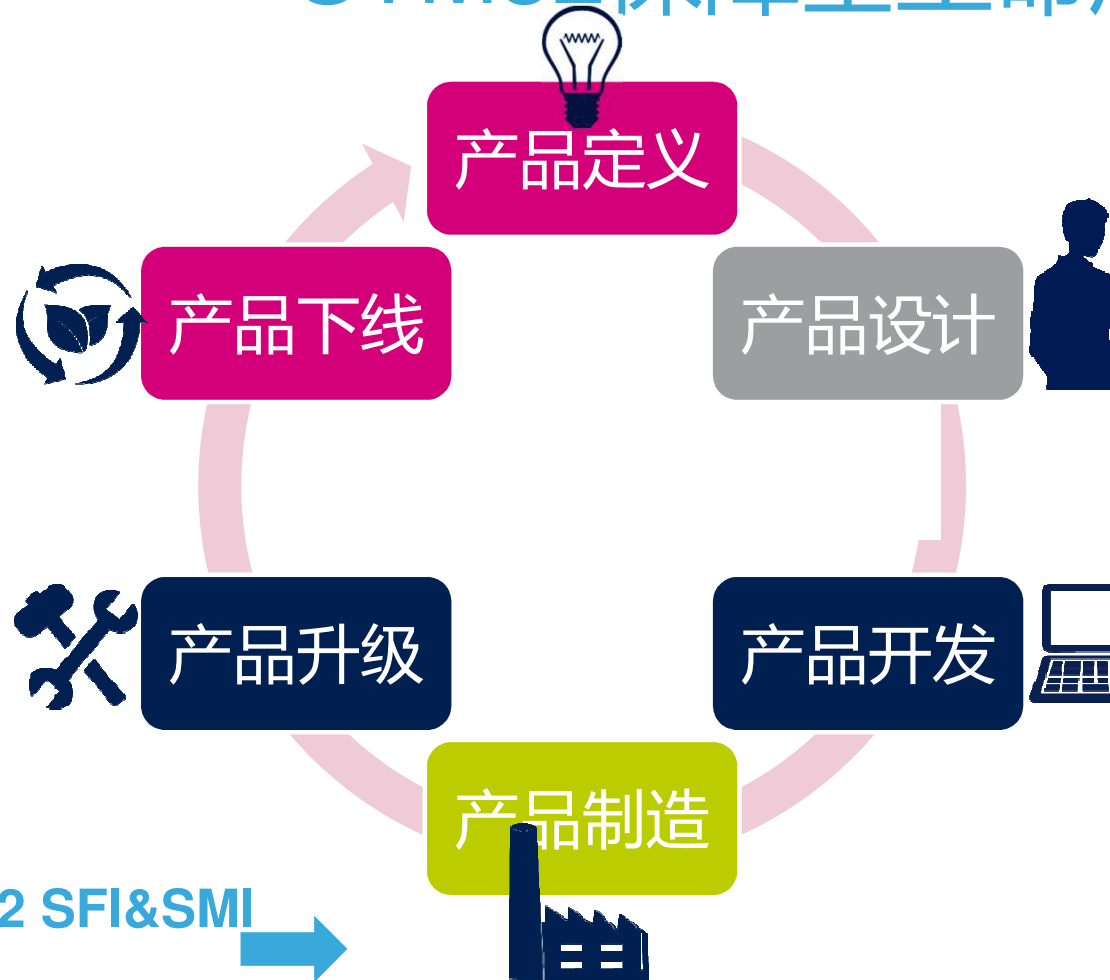
完整



可用

STM32保障全生命周期安全

12



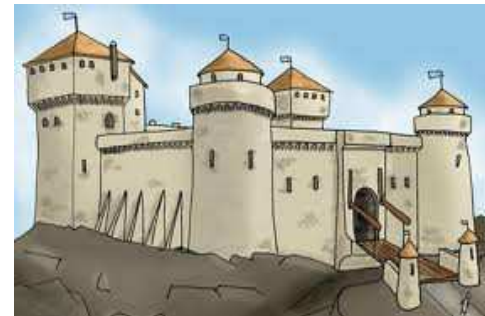
STM32 SBSFU

STM32
SBSFU

STM32 SFI&SMI

- 系统与局部---尽量避免系统级受攻击
 - 关闭STM32 JTAG
 - 使用STM32 UniqueID构成一机一密
 - 使用非对称密钥算法避免暴露私钥
- 内部与外部
 - 代码可信，重点在外部攻击
 - 有第三方代码，则内外兼防
- 长久与短暂---尽量避免长时间受攻击
 - 使用STM32看门狗
 - 加入报警机制

- 关闭调试使外部攻击无法发生
 - RDP
- 隔离控制使内部威胁无法构成破坏
 - STM32 Firewall/MPU/Secure User Memory/TrustZone
- 限制输入/限制输出避免暴露太多的弱点
 - STM32 DAP/RDP/DMA
- 多重防护保护最有价值的资产
 - STM32 WRP/PCROP
- 实时监控发现异常
 - STM32 IWDG/Tamper



- 安全的概念
 - 区分功能安全与信息安全
 - 理解信息安全三个服务原语及其扩展
 - 保密，完整与可用
- 系统分析技术
 - 理解资产是安全第一关注的对象
 - 理解安全风险来自资产、弱点、威胁的交集
 - 运用安全与资产、弱点、威胁的依赖关系
 - 分析STM32与专门安全芯片，或者两个STM32芯片之间的安全协作
 - 导出安全是一个整体的结论
 - 理解常见的攻击分类与防护
 - 理解基于产品生命周期的STM32安全技术