選對片上NVM存储器，改造SOC成忠实的保密者。
Choosing an exact on-chip NVM Memory, making SOC a faithful securer.

陈建良（Nick Chen）
现场应用工程师经理
2017年3月23日

概述

主题：您的SoC可以保护秘密吗？

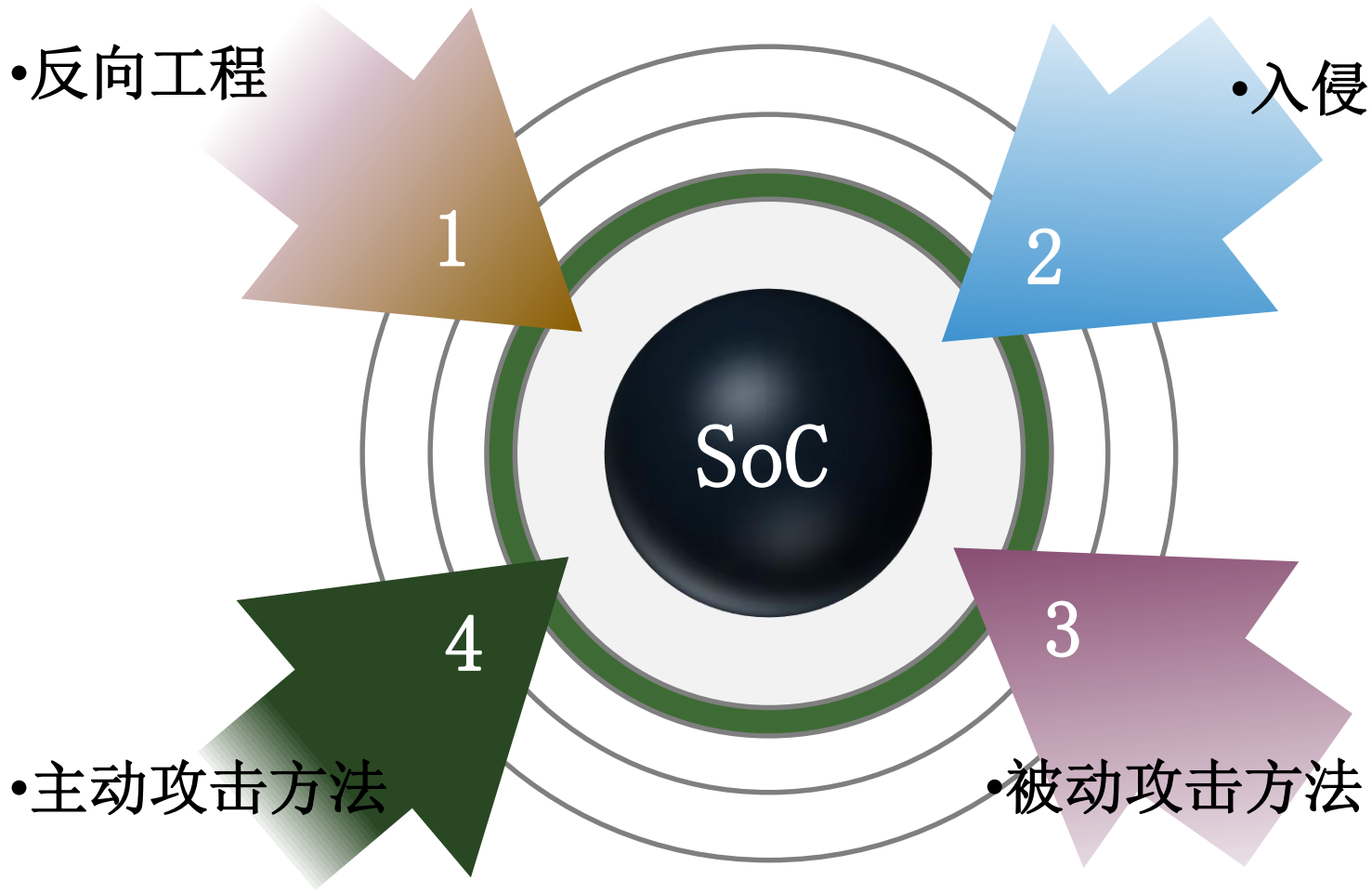
当今高端SoC，除了不断增加的复杂性外（例如：逻辑门数量與越来越多的IP内核使用等），对联网（特别是物联网）使用环境下的SoC安全性要求也越来越高。物联网设备已被证明是更容易遭到恶意攻击的目标。

最近非常出名的安全漏洞（最近网站的中断（DDoS,DoS）,DT大量路由器的中断，目标信用卡漏洞等）充分表明了联网设备的脆弱性，因此对安全的非易失性存储器的需求也非常明显。本次演讲主要介绍使用片上IP安全存储敏感数据和密钥的一些可用设置选项。让大家選對片上NVM存储器，改造SOC成忠实的保密者。

主要内容

- SoC安全威胁
  - 威胁术语和目标
  - 攻击术语和方法
- 针对联网设备的SoC安全性
  - 物联网市场预测和要求
  - 安全性是首要考虑因素
- 嵌入式存储器——安全的SoC实现的关键部件
  - 可用选项
  - 反熔丝的关键特性
- Kilopass产品
- 总结

SOC安全威胁



威胁术语和目标——反向工程

反向工程 | 入侵 | 被动攻击方法 | 主动攻击方法

反向工程是非法获得机密或秘密SoC产品信息以开发竞争性产品或为恶意攻击作准备的第一步：

- 识别内部配置设置
- 识别内部微调设置
- 识别算法开关和从属性
- 识别启动顺序和从属性
- 获得身份和安全密钥
- 获得微代码

威胁术语和目标——入侵

反向工程 | 入侵 | 被动攻击方法 | 主动攻击方法

入侵是恶意攻击SoC、通过使系统瘫痪或劫持SoC以达到破坏系统功能或非授权使用系统目的的第二步：

- 通过配置设置关闭整个SoC或某些功能
- 通过错误微调关闭SoC的模拟功能
- 激活未授权的SoC功能/模式
- 劫持SoC（擅用错误身份）以闯入网络
- 改变身份和安全性来获得未授权/未付费的服务
- 改变身份和安全性来完成未授权的金融交易

攻击术语和方法——被动攻击方法

反向工程 | 入侵 | 被动攻击方法 | 主动攻击方法

被动攻击方法是通过测量或测试以下指标，观察SoC在系统中运行时的参数：

- 功耗
- 电磁辐射
- 发热
- 发光
- 电源毛刺

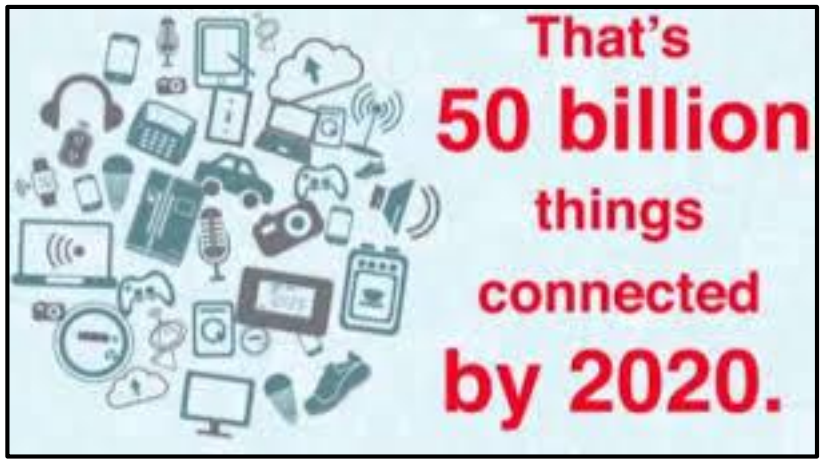
攻击术语和方法——主动攻击方法

反向工程 | 入侵 | 被动攻击方法 | 主动攻击方法

主动攻击方法是一种物理方法，通过避实就虚的方式在电路级别分析或改变SoC：

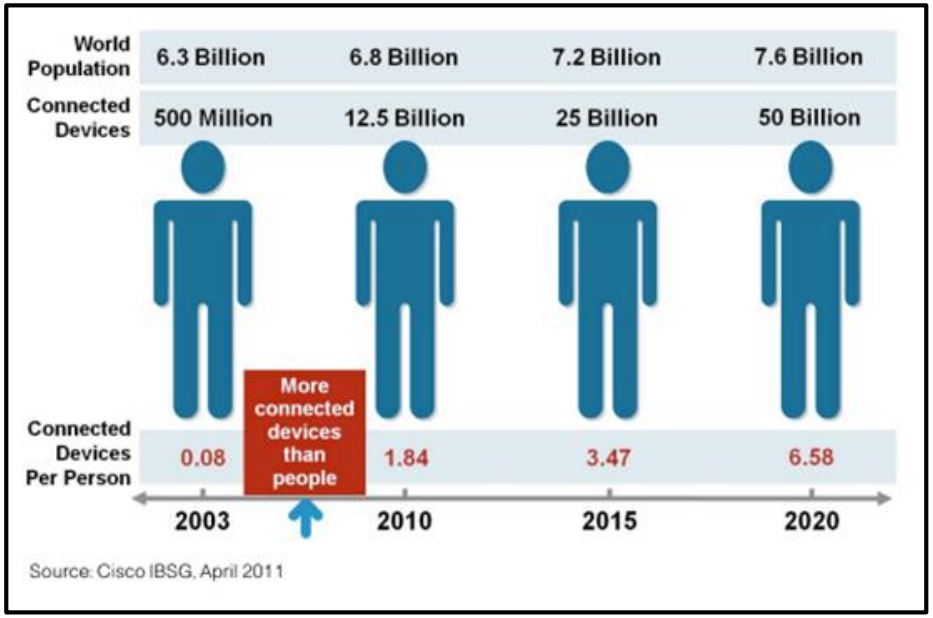
- 显微镜（SEM/TEM）
- 纳米/皮米探测
- 聚焦离子束/电子束/激光/紫外线
- 电压对比
- 磁力扫描
- 逆向工艺处理/剥层
- 横截面

联网设备和物联网——爆发式增长



- 到2023年，除了蜂窝电话和平板电脑外将达到340亿

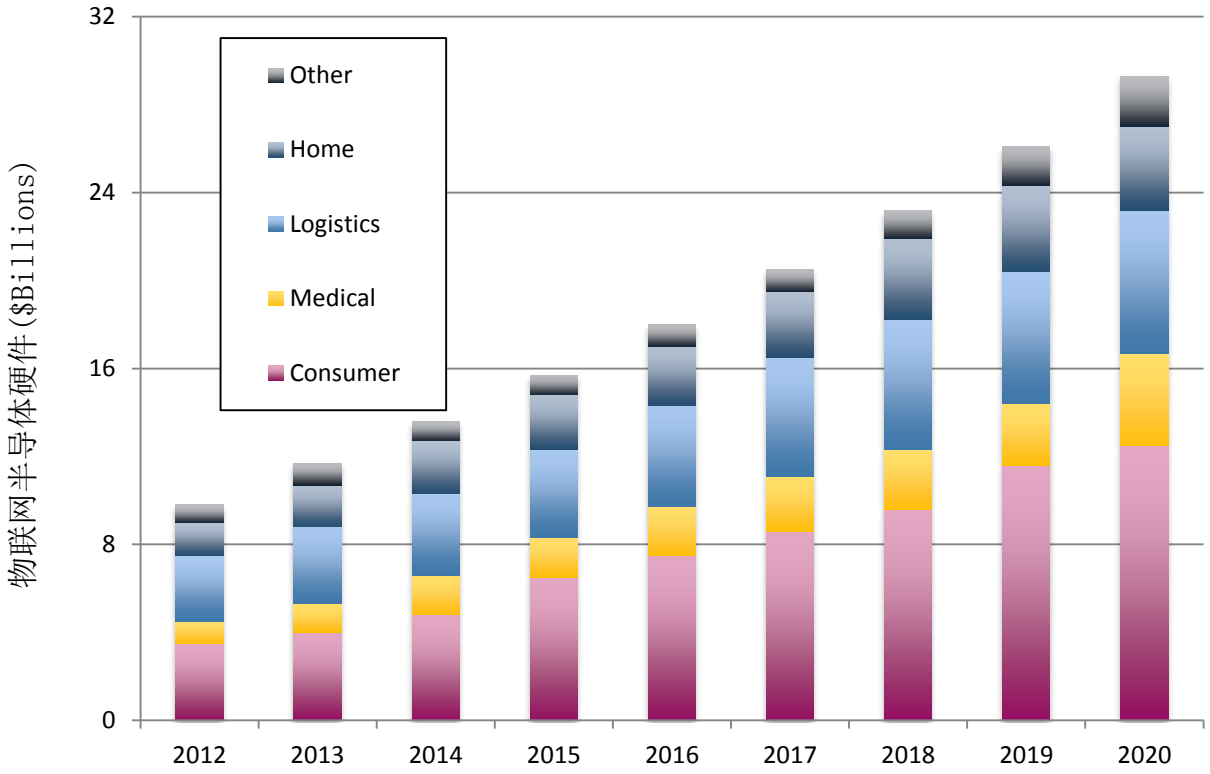
- 增长速度远超我们的人口增长率



Kilopass

物联网半导体硬件市场

- 市场很大，但高度细分
- 还没有公司开发出销售达10亿的器件
- 大量独特的SoC



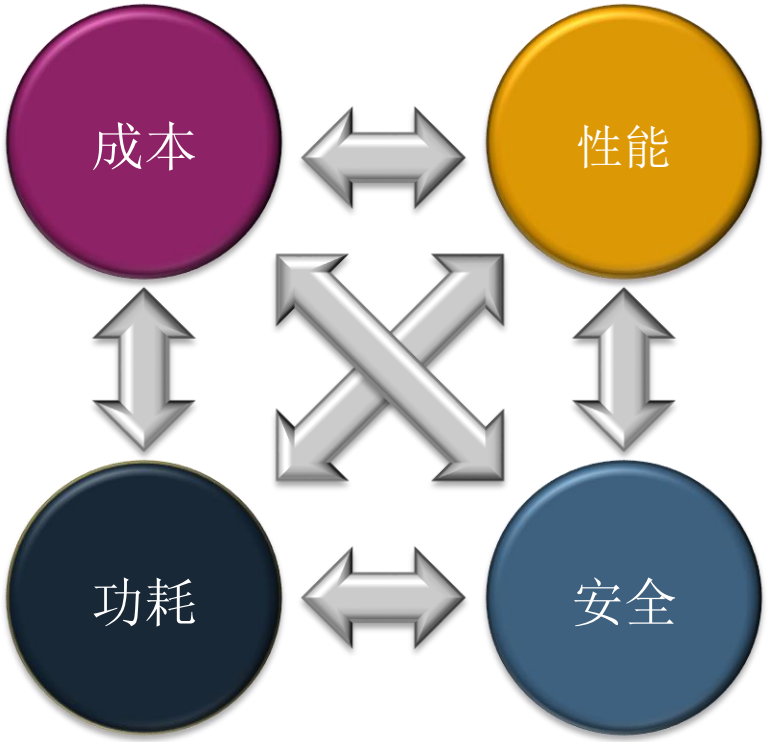
来源：IBS - 2014

Kilopass

物联网对SoC的要求

要求：系统成本低于10美元

方案：使用低成本的CMOS工艺实现高集成度



要求：可容纳新功能的可扩展性能（比如语音命令）

方案：增强CPU功能

要求：长达数年的工作寿命

方案：改为更小的几何尺寸

要求：在任务关键应用中受到充分信任

方案：增加复杂的软硬件层

- 极具挑战性的设计环境，有差异化的机会
- 向半导体行业开放新的市场

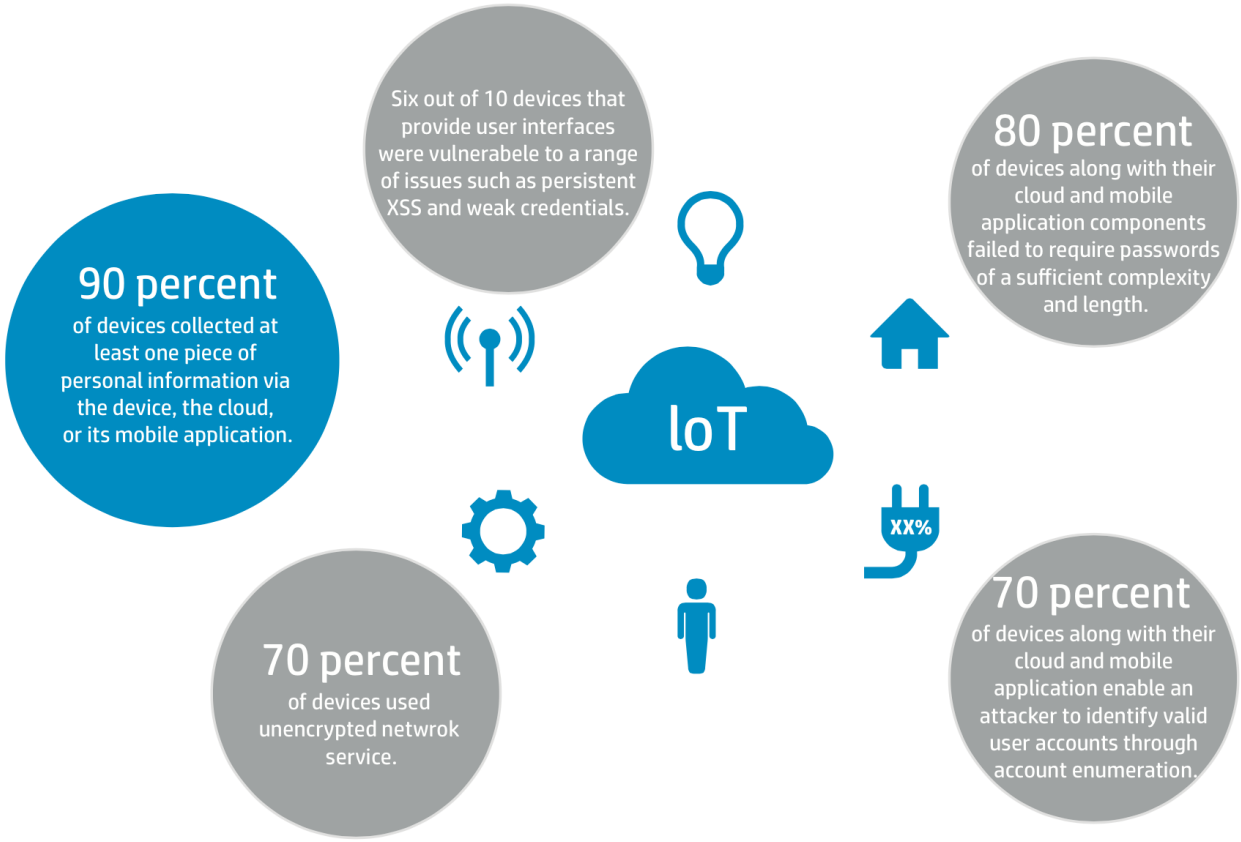
Kilopass

安全性挑战：
创建物联网产品的SoC设计师不是安全方面的专家

Kilopass

物联网：安全性挑战

惠普调查表明，70%的物联网设备易受到攻击



反熔丝非易失性存储器能够很好地用来保护代码和密钥

Kilopass

损害案例1

一个导致4000万条信用卡记录被盗的目标商店的漏洞来自**暖通空调系统**：
黑客利用从暖通空调公司偷来的登录证书从许多入口侵入这家零售家的网络。暖通空调公司为了执行诸如远程监视各家商店的能耗和温度等任务而拥有访问目标网络的权限。攻击者利用这个权限以不被检测到的方式登录目标网络，并向公司的销售点系统上载恶意软件。

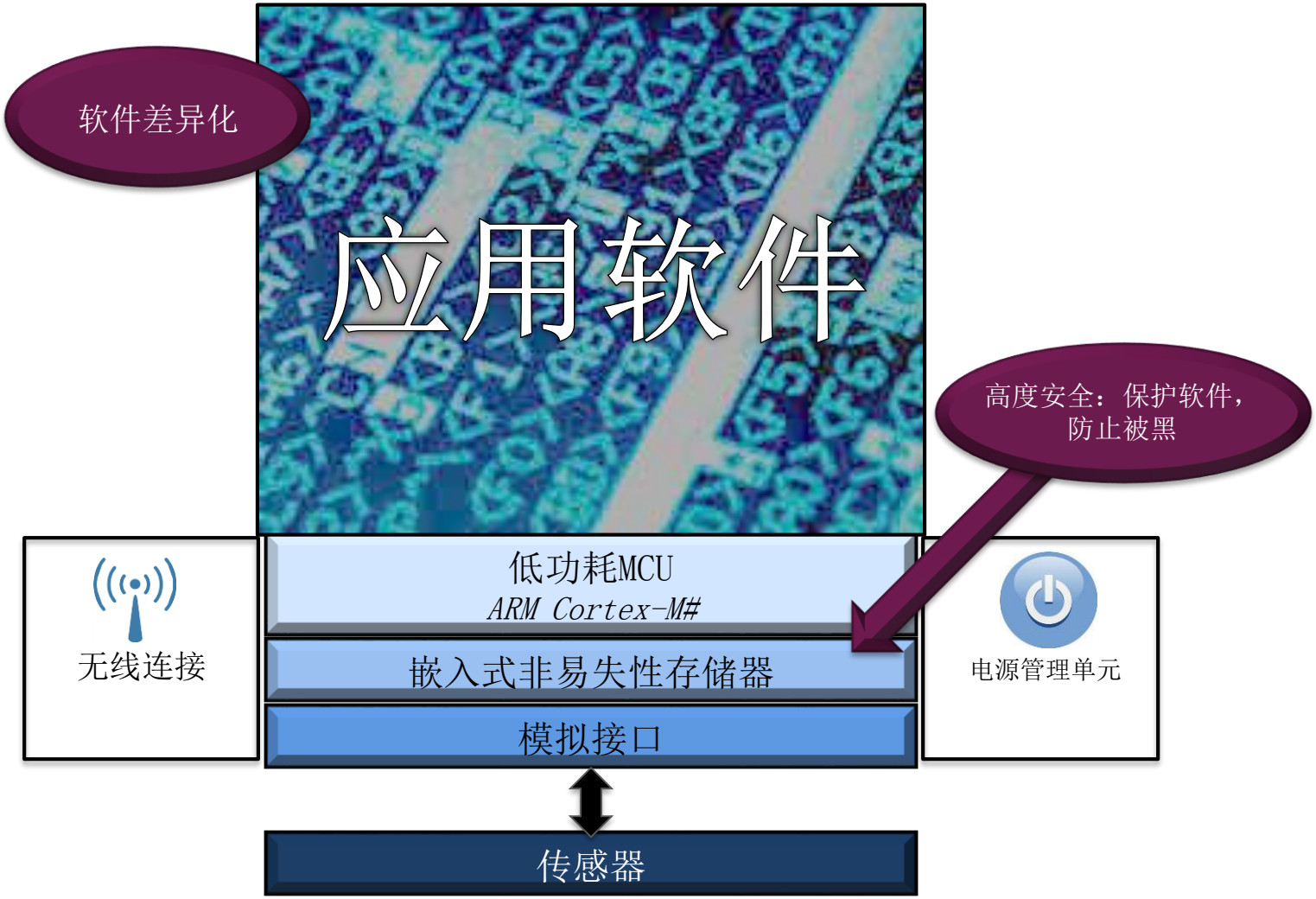
这种漏洞被攻破的影响是巨大的：
- 与数据泄漏有关的成本达2亿美元
- 由于业务受损导致475人下岗
- 技术升级花了1亿美元
- 首席信息官（CIO）被撤换

损害案例2

在2014年披露的一次更为严重的侵害事件中，黑客侵入德国的一家钢厂并大肆破坏其控制系统，使得厂内的一台高炉不能正常关闭，进而导致“大面积”受损。黑客利用网络钓鱼手法获得了进入钢厂办公网络的安全证书才得以进入其控制系统的。据德国联邦安全信息技术局透露，黑客进去后就闯入了高炉控制系统。

黑客入侵德国一家钢厂的控制系统造成大面积受损

针对物联网的SoC构建模块



Kilopass

目前嵌入式非易失性存储器技术综览

	ROM	“e-Fuse”	EEPROM/ e-FLASH	Antifuse OTP
技术	一种独特掩模	熔断导线或poly	浮栅	氧化物击穿/反熔丝
附加工艺层和步骤	0	0 - 5	0 - 15, 紫外，烘烤	0
位单元尺寸	0.3	30 - 100	5 - 10	1
写次数	1	1	许多次	1
读次数	无限	有限	无限	无限
设计灵活性	无!!	有些	最大	较大
安全性	低	低	低	高
备注	从20世纪70年代开始就有了，但不能满足今天对灵活性的需求	无法扩展到16kb以上，不能防止反向工程	最灵活，但非常昂贵，不能适应先进工艺	可以适应先进的工艺，并提供卓越的安全性

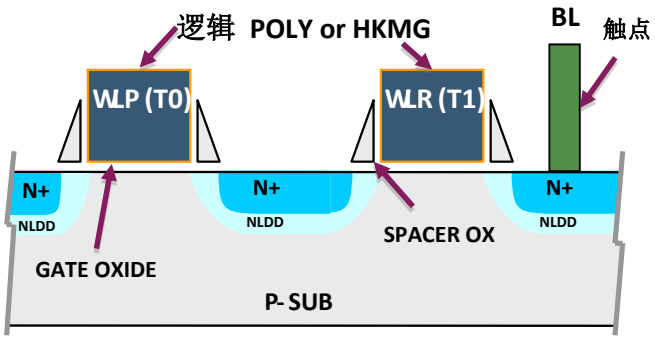
- 对下一代存储器的巨大投资将主要放在标准存储器元件方面
  - MRAM、RRAM依赖于电容的堆叠，不适合单片SoC工艺

反熔丝位单元与浮栅位单元的比较

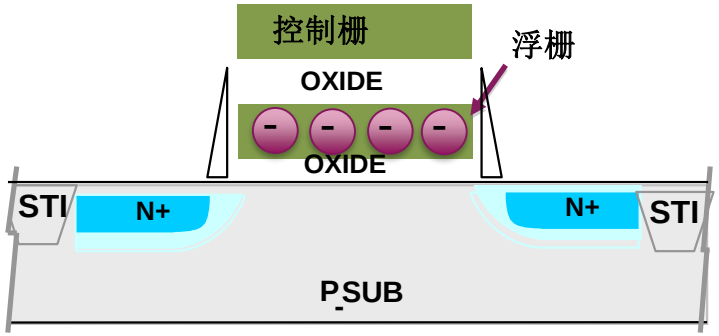
- **反熔丝位单元:**
- 标准CMOS工艺
  - 标准NMOS晶体管
  - 遵循**标准**DRC/DFM设计规则
  - 无需额外的晶圆处理:
    - 不用晶圆烘烤
    - 不用紫外线擦除
- 可靠性和良率
  - 与标准CMOS基准逻辑工艺技术相同

- **浮栅位单元:**
- 非标准CMOS工艺
  - **要求额外工艺层的**复杂的定制晶体管
  - 违反**标准**DRC/DFM设计规则
  - 要求额外的晶圆处理:
    - 晶圆烘烤
    - 紫外线擦除
- 可靠性和良率
  - 落后于标准工艺

2T传统标准CMOS



浮栅——晶体管非标准逻辑器件



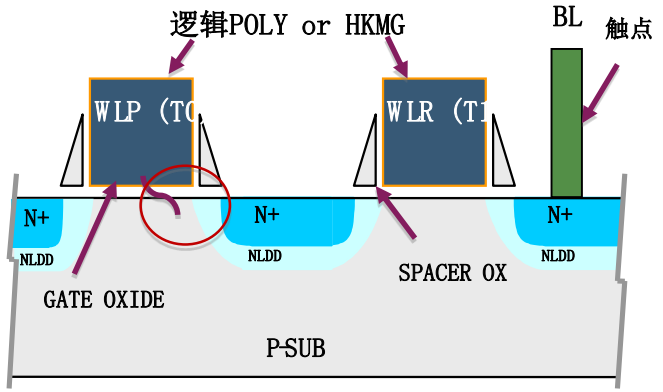
Kilopass

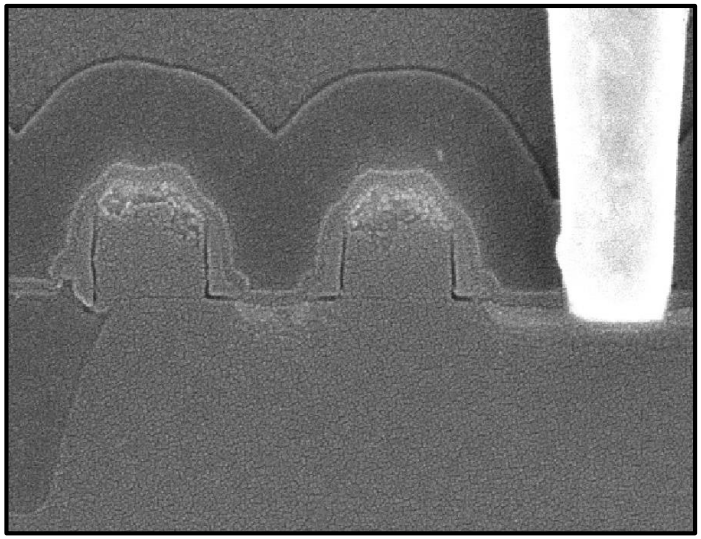
Kilopass公司介绍

公司	eNVM OTP存储器领域中的先驱	丰富的器件物理专业知识	扩展到新的内存技术
成立于2001年 总部位于圣何塞 雇员人数75 2008年到2017年增长了10倍	70多个专利 被250多家IDM及无晶圆厂公司集成 Kilopass OTP交付的器件数量超过100亿个 台积电<10nm 基础OTP-IP	80个端口小至10nm BiCMOS, BCD, SOI, FD-SOI HKMG, FinFET HV, DRAM	VLT（基于晶闸管） SRAM & DRAM 1/10待机功耗 ½成本 无需刷新 经硅片验证的位单元

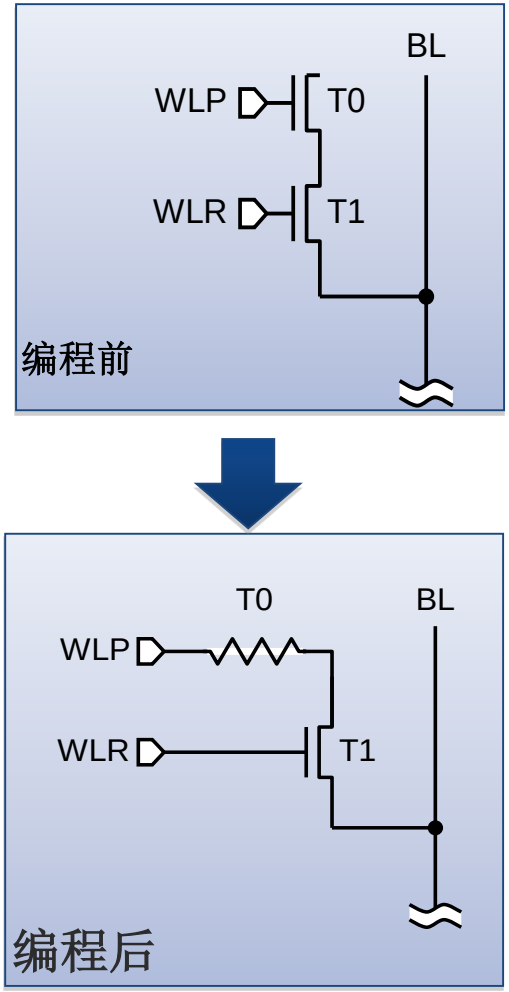
Kilopass反熔丝位单元：标准CMOS，经生产验证

单元横截面



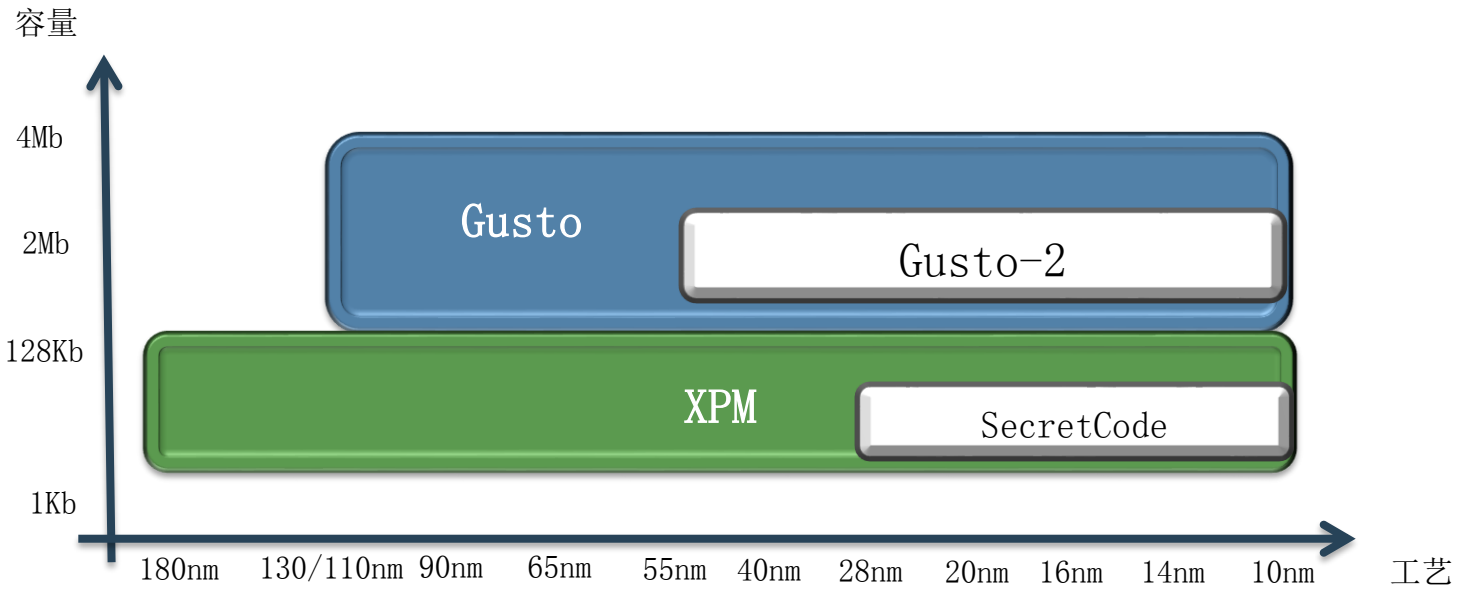


XPM单元原理图



Kilopass

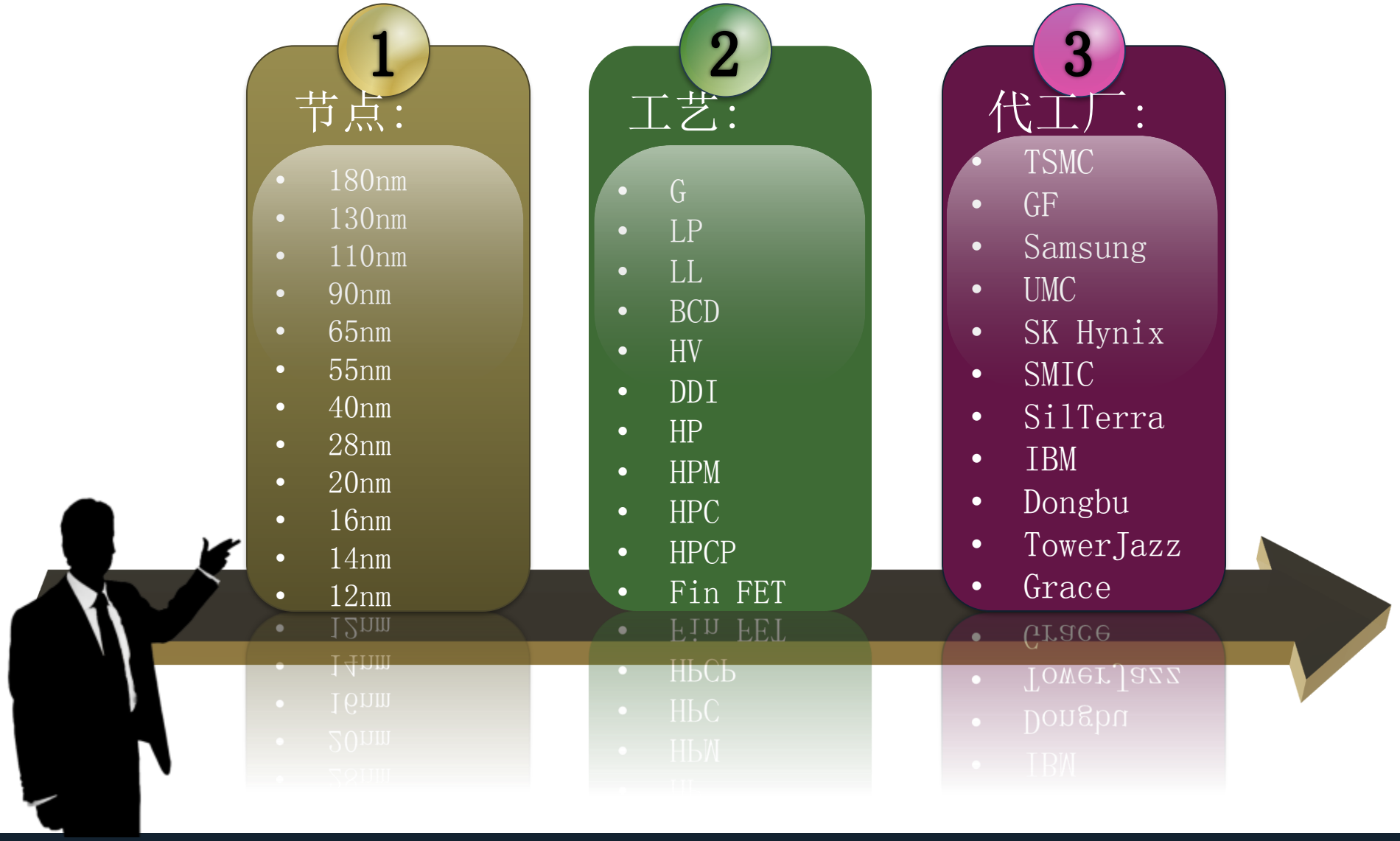
Kilopass反熔丝eNVM OTP产品



- XPM (eXtra Permanent Memory): **超绝**永久存储器
- SecretCode:绝密永久存储器
- Gusto-2: 新一代Gusto,适合低功耗连接应用
- 继续保持领先于安全性要求
- 将片上非易失性存储器扩展到先进工艺节点（HKMG,FinFET）

Kilopass

Kilopass eNVM OTP工艺规范/选项：



Kilopass

总结

- **Kilopass 反熔丝eNVM:**
- **具有一流的安全性能，能够防止**
  - 反向工程
    - 发现不了反熔丝链路
  - 入侵
    - 可在阵列或位等级防止编程数据被篡改
  - 被动攻击
    - 监视供电电压
    - 一致的电源分配
  - 主动攻击
    - 锁定功能防止被篡改
- **使用低成本的标准CMOS工艺**
- **适应宽范围的多家晶圆代工厂工艺**
- **可扩展到更先进的工艺**
- **方便系统/现场编程**

谢谢