飞思卡尔 微控制器
瞄准安全可靠的物联网未来

Sun Dong, Senior Marketing Manager

Sept.24,2015

freescale™

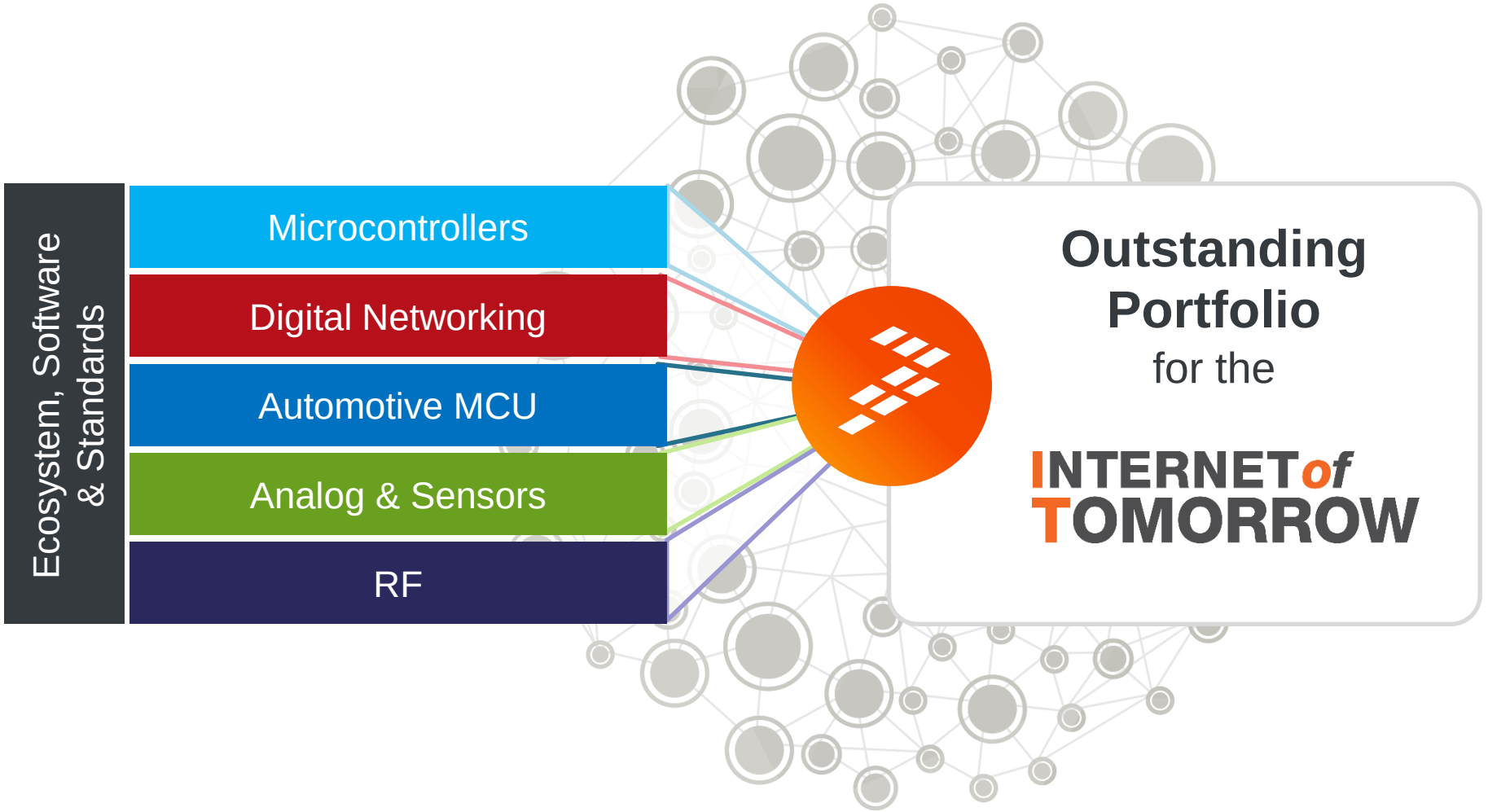
External Use

SECURE EMBEDDED PROCESSING SOLUTIONS

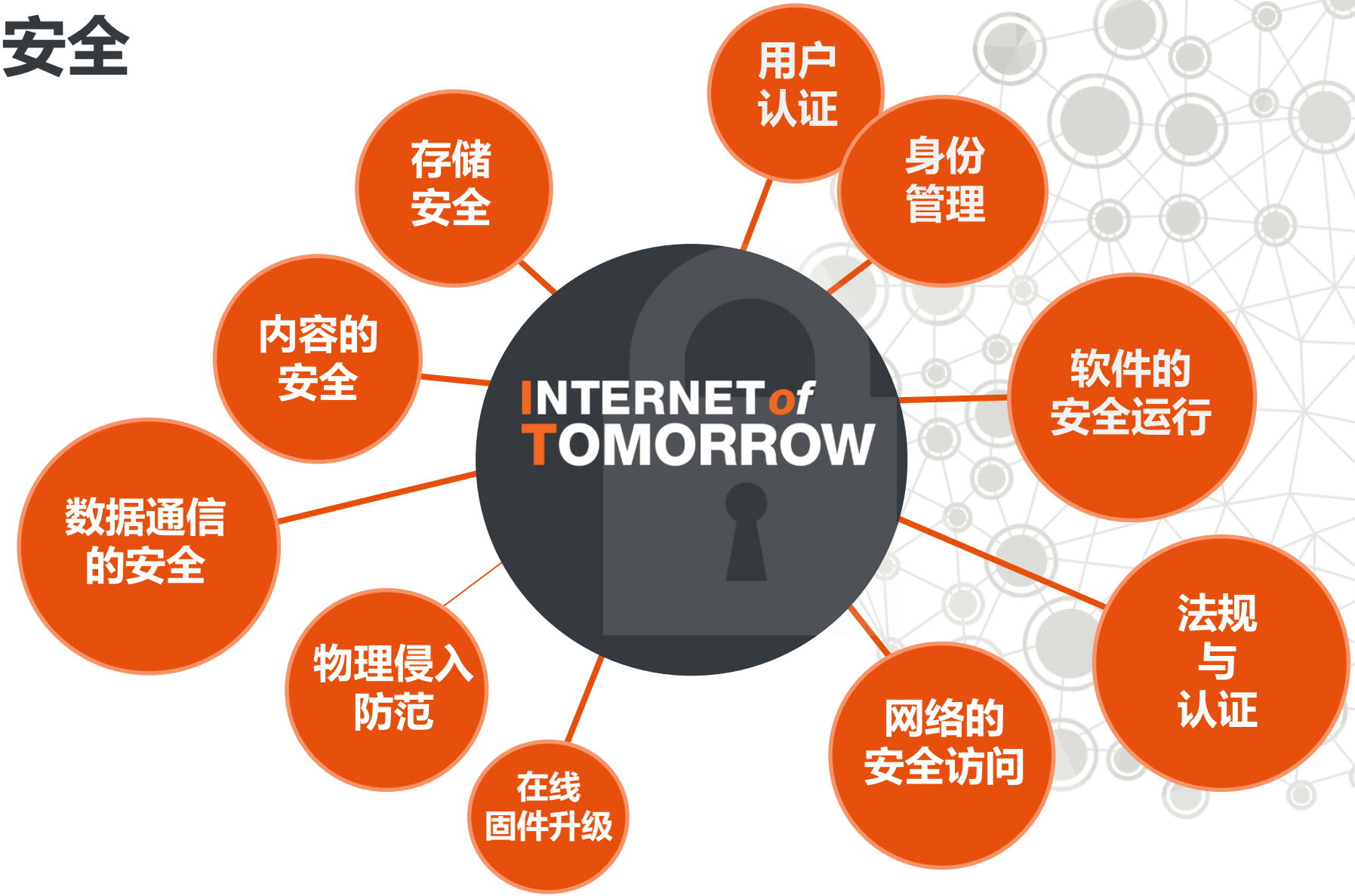
for the

INTERNET *of* TOMORROW

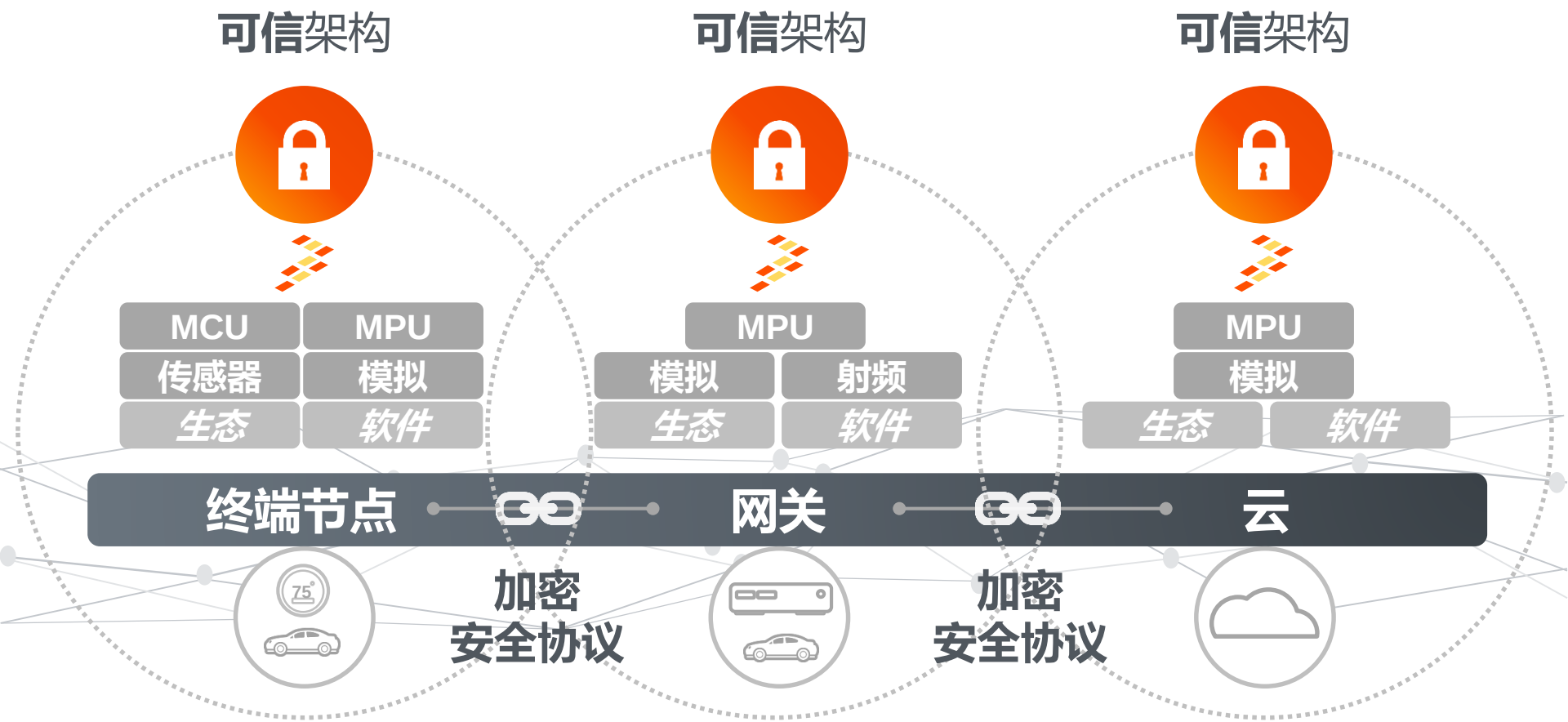
全球领先的安全嵌入式方案供应商



安全


INTERNET of TOMORROW
用户认证
身份管理
存储安全
内容的安全
软件的安全运行
数据通信的安全
法规与认证
物理侵入防范
网络的安全访问
在线固件升级

飞思卡尔 IoT 安全方案



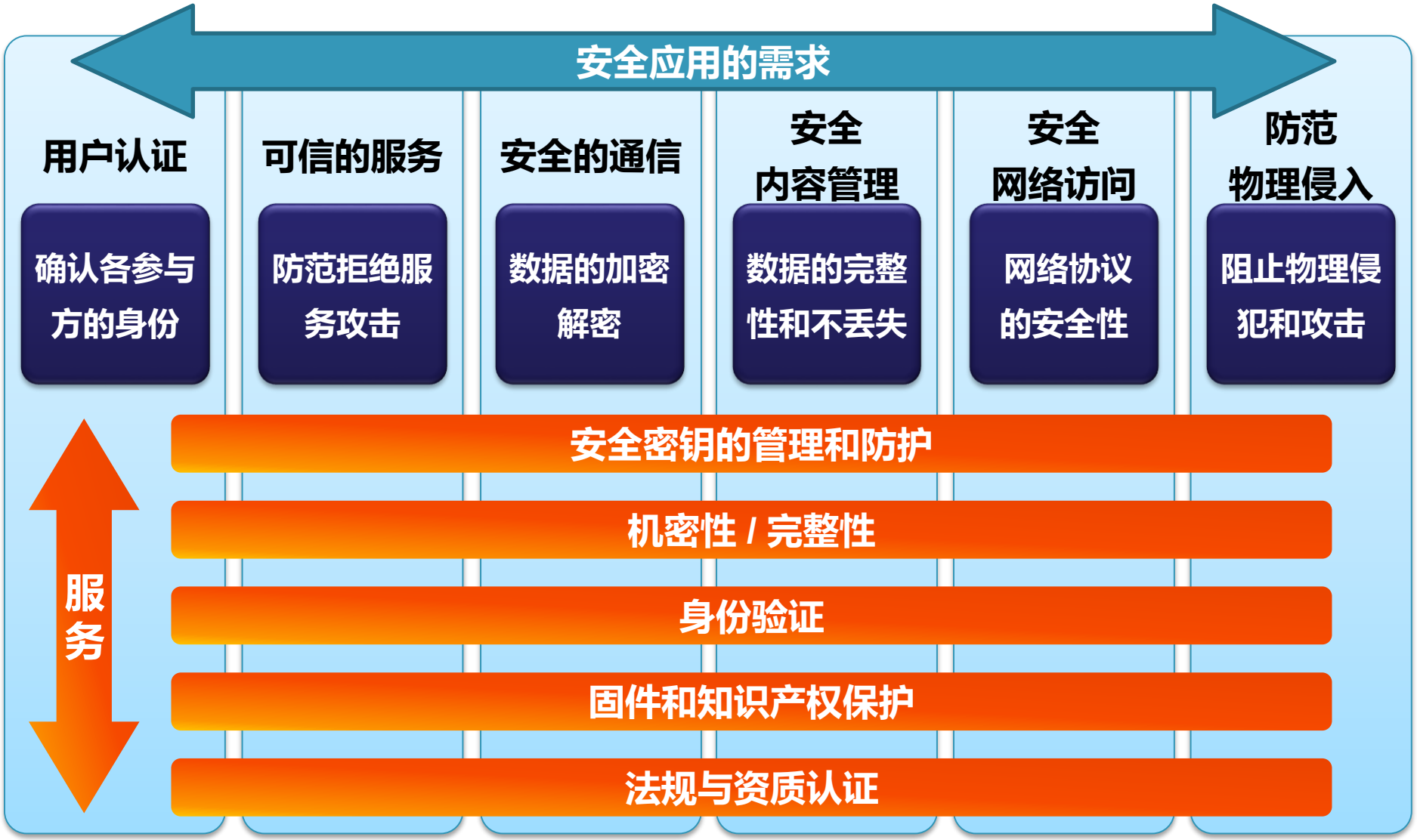
嵌入式应用在安全方面的需求

嵌入式应用在安全方面的需求

安全应用的需求

用户认证	可信的服务	安全的通信	安全 内容管理	安全 网络访问	防范 物理侵入
确认各参与方的身份	防范拒绝服务攻击	数据的加密解密	数据的完整性和不丢失	网络协议的安全性	阻止物理侵犯和攻击

嵌入式应用在安全方面的需求



Freescale的解决方案

安全密钥的管理和防护
OTP Key space, HW Crypto Accelerators, Flash and chip security

机密性 / 完整性
AES, DES, ECDSA, ECDH acceleration
Software crypto libraries (WolfSSL), mbed SSL, KSDK crypto drivers

身份验证
ROM routines for creating secure firmware updates.

固件和知识产权保护
Flash Security, Flash Access control

法规与资质认证
NIST compliant RNG, CAVP certifications

对嵌入式系统的攻击种类

- 电子攻击
  - 过/欠电压
  - 功耗分析
  - 频率分析
  - 静电放电
  - 电路探针探测
  - 电磁分析
- 软件攻击
  - 插入间谍软件
  - 流程分析
  - 特鲁伊木马
  - 病毒
- 物理攻击
  - 温差 (趋于极限)
  - 温度分析
  - 磨片
  - 盗窃
  - 部分解构
  - 硬件的叠加/删减
- **分类**
  - 投资(设备)
  - 时间
  - 专门知识或技能
- **类型**
  - 侵入性或半侵入性
  - 非侵入式或侧面攻击
  - 软件

硬件助力安全防范

- **减少开发时间**
  - 硬件加速取代软件算法
  - 芯片硬件保护取代外部防护措施和器件
- **加密算法的硬件加速，有效提高功耗效率**
- **降低系统成本**
  - 减少外部器件
  - 降低生产复杂度
  - 抵御安全攻击的长效防护，保障设备的唯一身份

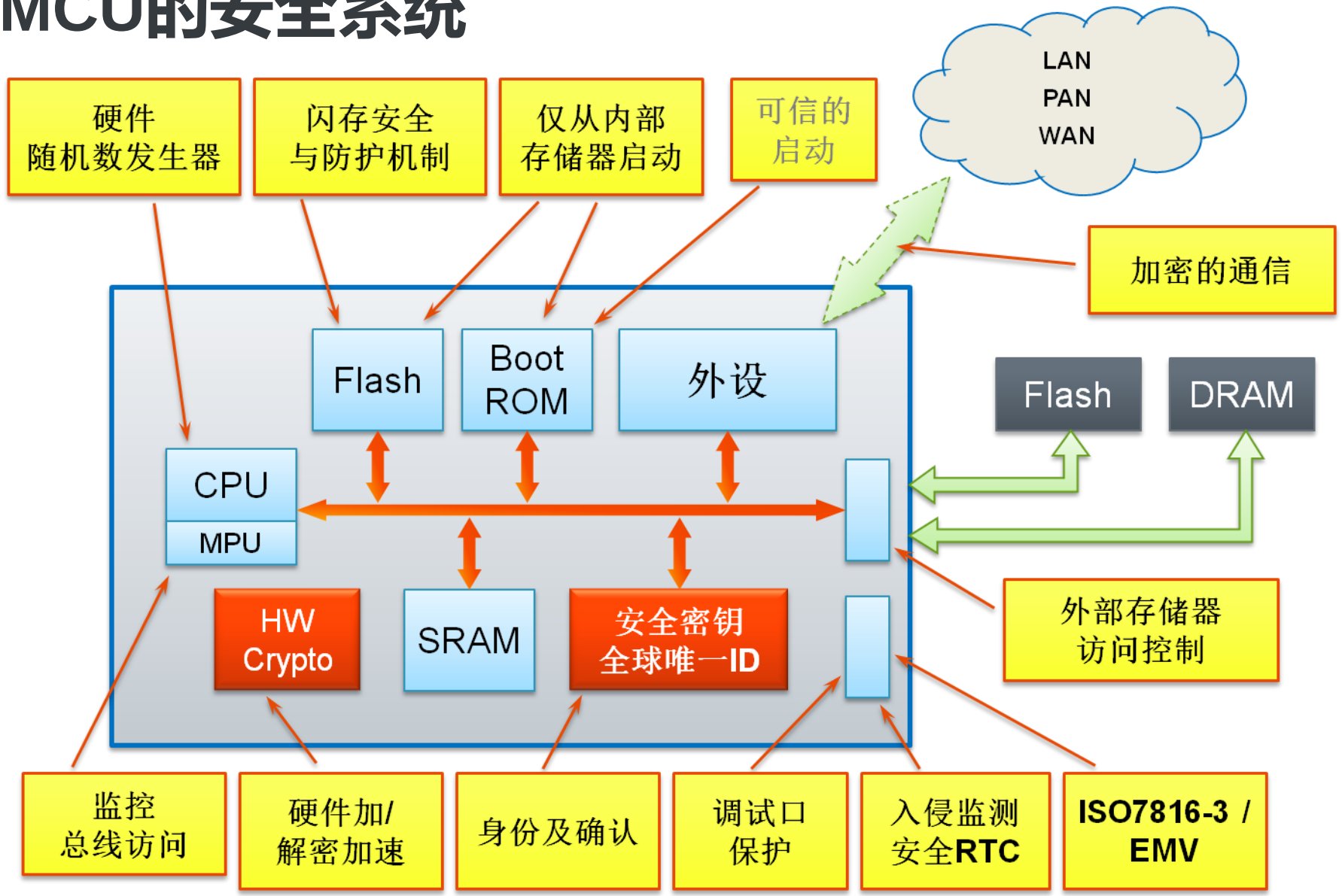
硬件安全是现今嵌入式设计必不可少的基本要素

Kinetis MCU安全特性

Kinetis MCU系列产品中拥有很多优异的安全功能

功能	描述	器件
闪存安全与防护	对外部访问的防护 对内部意外擦写的保护	所有Kinetis MCU器件
入侵检测和安全RTC	入侵检测引脚监视信号的扰动和对系统的入侵	部分Kinetis MCU产品。通常是Kx1系列。 例如：K20没有，但K21具有该功能 。
加解密加速	实现对称算法和哈希算法加速的硬件模块	部分Kinetis MCU产品。通常带有入侵检测和/或以太网的产品具有此功能。
随机数发生器	硬件随机数发生器	部分Kinetis MCU产品。通常带有入侵检测和/或以太网的产品具有此功能。

MCU的安全系统


硬件
随机数发生器
闪存安全
与防护机制
仅从内部
存储器启动
可信的
启动
LAN
PAN
WAN
加密的通信
Flash
Boot
ROM
外设
Flash
DRAM
CPU
MPU
HW
Crypto
SRAM
安全密钥
全球唯一ID
外部存储器
访问控制
监控
总线访问
硬件加/
解密加速
身份及确认
调试口
保护
入侵监测
安全RTC
ISO7816-3 /
EMV

Kinetis MCU: 宽广的ARM Cortex-M 产品线

Kinetis MCU：应用市场

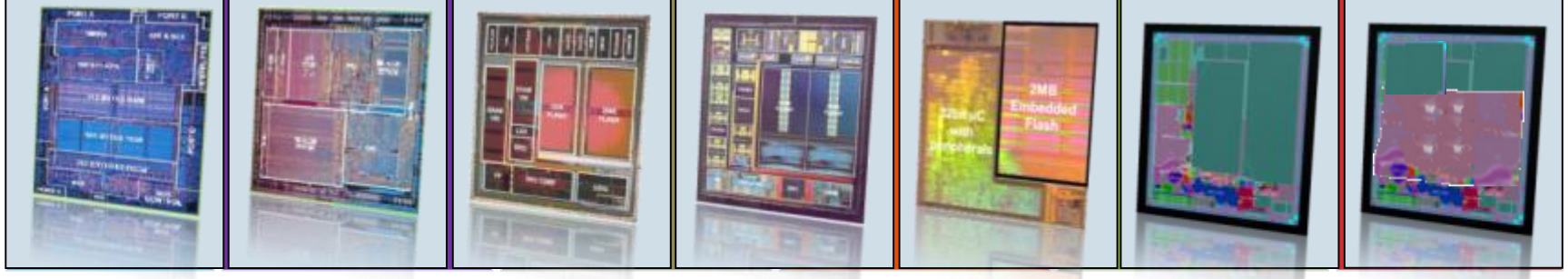
MCU的安全系统

i.MX拥有更丰富的安全资源

- ARM Trust Zone
- 安全存储器 up to 32KB
- 抵御DPA攻击
- 实时DRAM加解密
- 真随机数发生器
- 非对称：RSA, ECDSA (up to 4096)
- 对称：AES-128/256, DES, 3DES, ARC4, Hash & HMAC: MD5, SHA-1, SHA-224/256. 256-位 安全

i.MX 应用处理器

1995	2001	2003	2005	2009	2012	2014
Dragonball 1st FSL Apps Processor	**i.MX1** 1st FSL ARM9 Apps Processor	**i.MX2 Series** 90nm LP HW Video Accel Analog Integration	**i.MX3 Series** ARM11 GPU Integration	**i.MX5 Series** 65nm LP/GP ARM Cortex-A8 >1GHz	**i.MX 6 Series** 40nm LP ARM Cortex-A9 Multi-core family	**i.MX 7 Series** 28nmLP ARM Cortex-A7 Multi-core family



50+ 产品
>200M 出货

- **No.1** eReader 应用处理器(IDC)
- **No. 2** 车载娱乐 (Strategy Analytics)
- Freescale ARM SOC 的增长趋势:
  - 基于ARM的产品 (Kinetis, i.MX) >50% y/y
  - 在车载娱乐强势增长 (i.MX > 50% y/y)
  - 工业 & 消费类 MCU产品的两位数增长 y/y
  - i.MX产品在所有领域的两位数增长

i.MX 市场和应用

Automotive

- Infotainment
- Telematics
- Instrument Clusters
- Vision/Camera Systems

eReaders

- Monochrome eReader
- Color eReaders

Smart Devices

- Medical – Patient Monitoring
- Smart Energy
- Factory Automation
- HMI
- Digital Signage
- Smart Metering
- Point of Sale

- Medical tablets
- Industrial tablets
- Educational tablets
- IPTV/Streaming Media
- Smart Monitors
- Media / IP Phones
- Printers
- Smart Home Appliances
- Scanners

i.MX: 更多安全功能

	Kinetis	i.MX
Secure Boot	No	High Assurance Boot Authenticated + Encrypted Boot
Random Number Generator	Yes	TRNG
Secure Memory	32B + 128B	Yes
Secure RAM	No	2KB~32KB
No. of Tamper Pins	3~8	10
Frequency Tamper	Yes	Yes
Voltage Tamper	Yes	Yes
Temperature Tamper	Yes	Yes
Cryptographic Accelerators	AES, RCA/ECC, SHA, DES/3DES	Asymmetric: RSA, ECDSA (up to 4096) Symmetric: AES-128/256, DES, 3DES, ARC4, Hash & HMAC: MD5, SHA-1, SHA-224/256. 256-bit security
Protection on External Storage	No	On-The-Fly DRAM Encryption
ISO7816-3 / EMV	Yes	Yes
DPA Protection	No	Yes
ARM TrustZone	No	Yes

Note: Above features are available on selected devices.

安全性检查表

在考虑保护一个系统时需要回答这些问题：

- 需要保护什么？它的价值？
- 需要防范什么样的攻击？
- 可能的攻击点和手段？
- 需要什么级别的安全性？
- 你愿意为此支付的费用是多少？
- 安全与安全措施会如何影响整个系统？
- 你将如何升级/维护系统？

可以设想如何保护你的家

谢谢您！