# 智慧生活，安全连接

– 恩智浦一站式解决方案为嵌入式系统安全保驾护航

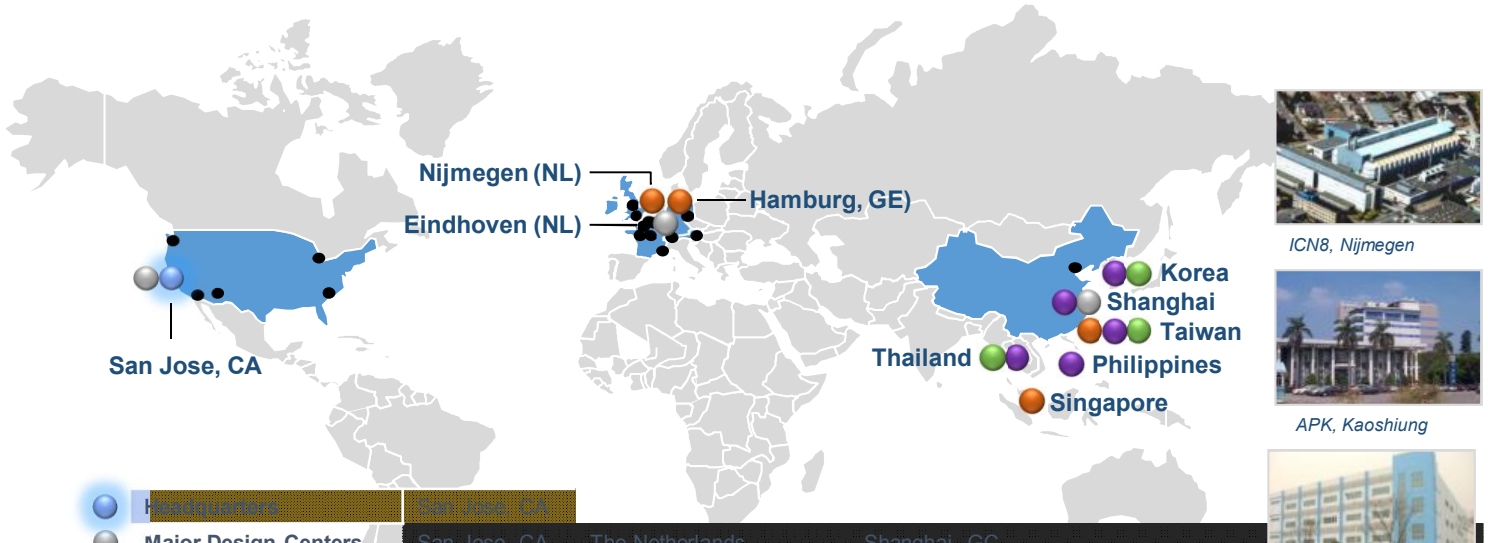
SECURE CONNECTIONS
FOR A SMARTER WORLD

**恩智浦半导体 | Nov 2015**

# 智慧生活，安全连接


- 四项改变社会的重大趋势正推动着电子产业的发展： 能源效率、设备互联、安全与健康。
- 紧随趋势：恩智浦半导体专为互联汽车，网络安全，便携和可穿戴式应用，以及物联网打造强大解决方案：帮助人们实现“智慧生活，安全连结”。

# LPC MCU恩智浦微处理器 — 来自美国硅谷






*ICN8, Nijmegen*



*APK, Kaoshiung*



*ASEN (J.V.) Suzhou*

| | | | | |
|---|---|---|---|---|
| Headquarters | San Jose, CA | | | |
| Major Design Centers | San Jose, CA | The Netherlands | Shanghai, GC | |
| Wafer Fab | | NXP (Hamburg, Germ.)<br>NXP IC8N (Nijmegen, NE) | SSMC (Singapore)<br>UMC (Singapore) | ASMC (China)<br>TSMC (Taiwan) |
| Assembly | | | ASE-K (Korea)<br>SPIL (Taiwan)<br>AMKOR (Philippines)<br>ATK (Korea) | ASEN (Shanghai)<br>UTAC (Thailand)<br>NXP (Thailand) |
| Test | | | AMKOR (Korea)<br>NXP APB (Thailand)<br>NXP APK (Taiwan) | KYEC (Taiwan)<br>ASE<br>TSMC (Taiwan) |

# 恩智浦微控制器 -- 风雨同舟，我们一路共同走来

## 40年的微控制器创新史 | 25年与ARM的深度合作

**Signetics**
- **Launched first 8-bit microcontroller* (1975)**
- *Acquired 1975*

**CodeRed**
- **Renown for 32-bit ARM MCU development tools (incl. LPCXpresso IDE)**

**Quintic**
- **Leader in BTLE SoCs for Wearables**
- *Acquired by NXP (2014)*

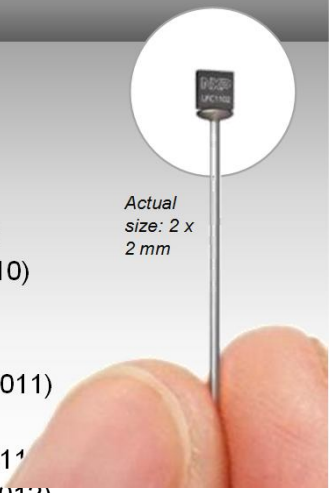
**Royal Philips Electronics (Philips Semiconductors)**
- **Founding investor in ARM and first ARM licensee** (1990)**
- *Acquired 1999*

**VLSI Technology**

**NXP Semiconductors**

### Driving industry firsts

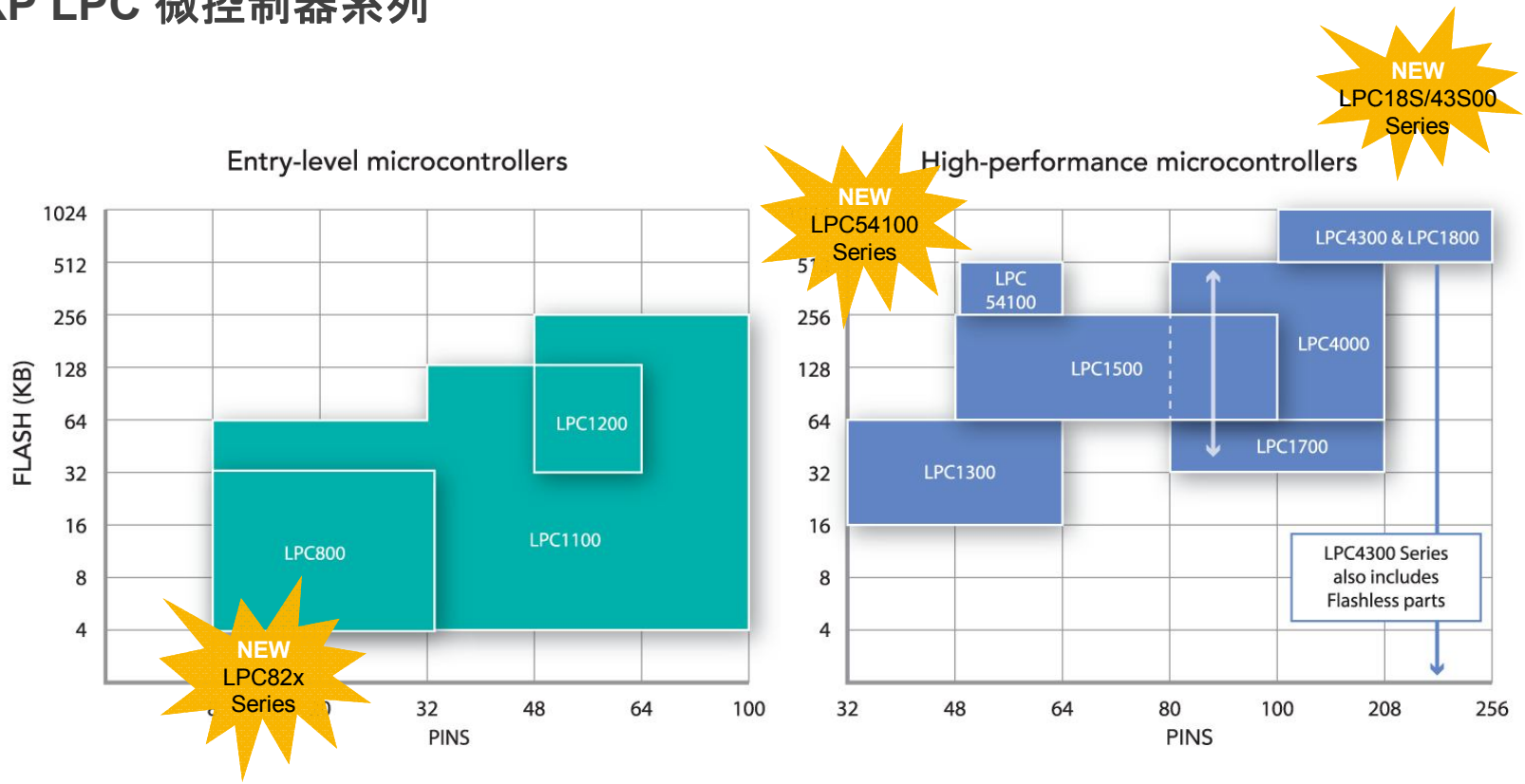
- First ARM7 MCUs with dual high-speed bus (2006)
- First 180 MHz Cortex-M3 (2008)
- First ARM Partner to license new Cortex-M0 (2009)
- One of the first ARM partners to license Cortex-M4 (2010)
- First asymmetrical dual-core MCUs (Cortex-M4F/M0) (2010)
- First 204 MHz Cortex-M4 (2011)
- First low-pin-count Cortex-M0 (2011)
- First Cortex-M0 MCU with integrated USB class drivers (2011)
- First dual-supply voltage ARM Cortex-M0 MCUs (2012)
- First seamless high-speed SPI Flash interface (SPIFI) (2011)
- First 32-bit ARM MCUs (2 x 2 mm) in WLCSP package (2012)




*2650 NMOS 8-bit microcontroller

** http://www.arm.com/about/company-profile/milestones.php

# NXP LPC 微控制器系列



# 恩智浦微控制器始终聚焦在快速增长的市场热点应用

# 恩智浦提供各种安全机制 为您的产品保驾护航

✓ 安全的四大方面

- 密钥的产生与存储
- Flash内容防盗
- 安全地建立连接
- 安全地传输数据


✓ LPC MCU的基本安全保护

- 代码读取保护(CRP)
- 唯一识别码(UID)
- 软件实现的安全算法

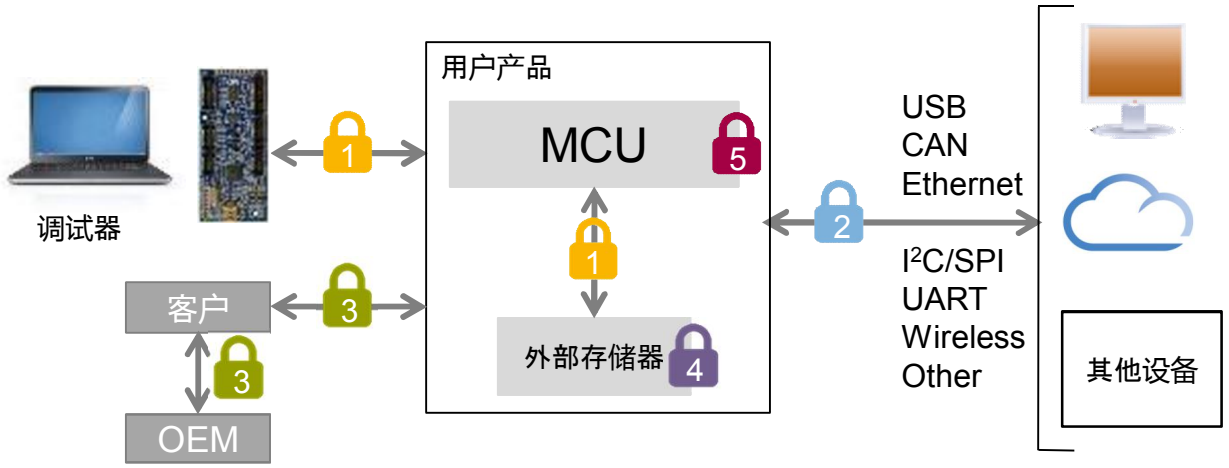
✓ 雪中送炭

- LPC18Sxx/43Sxx MCU
- 硬件随机数发生器（RNG)
- 加密的OTP存储器
- 安全启动机制
- 硬件加速的AES与认证

✓ 锦上添花

- MCU + A7x安全伴侣芯片
- 通过认证的硬件RNG
- 银行级闪存内容保护
- 防拆解设计
- 安全固件升级机制
- 安全连接建立机制

# 保护嵌入式系统




1 防止程序的复制，篡改及反向工程

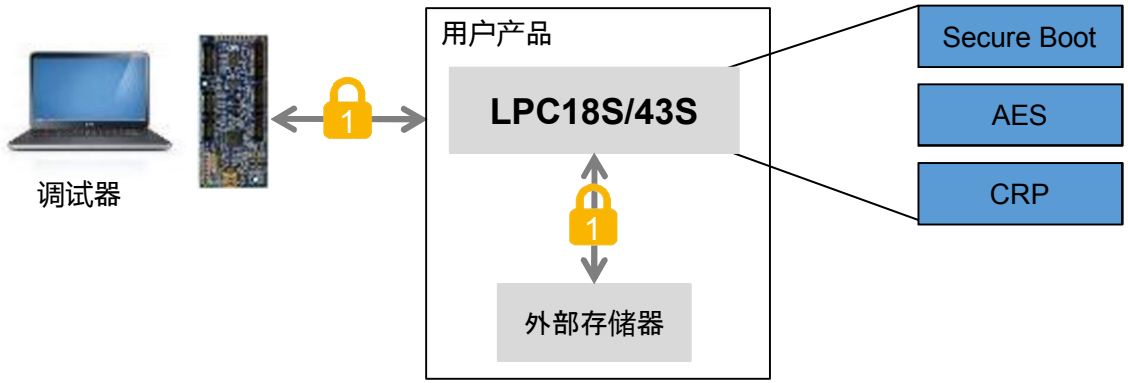
2 防止数据的窃听和篡改

3 防止未授权的仿造产品

4 保护外部存储器的安全可靠性

5 安全的固件升级

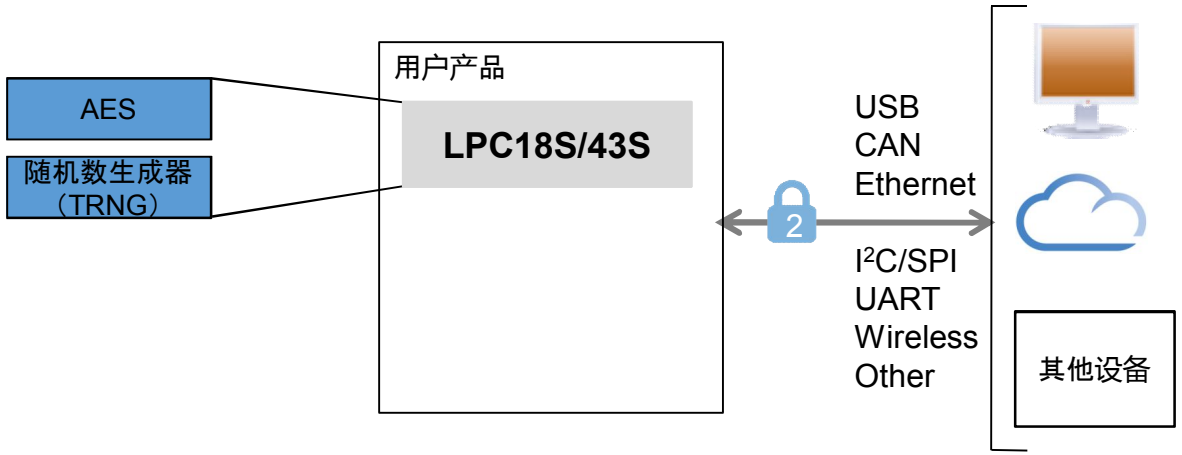
# 防止程序的复制，篡改及反向工程




- ✓ 从片内存储器启动MCU
  - 通过CRP禁用JTAG/SWD和ISP接口
- ✓ 从外部存储器启动MCU
  - 通过CRP禁用JTAG/SWD和ISP接口
  - Secure boot (加密程序的安全启动) 保证执行程序的可靠性，完整性

- ✓ 代码读保护
  - 不同级别的保护等级设置
  - SWD/JTAG 调试口锁定
  - 基于应用的用户配置
  - 支持系统和应用的编程设置
- ✓ 每颗芯片唯一的ID号
  - 通过ISP/IAP 命令读取
  - 128-bit 位宽

# 防止数据的窃听和篡改

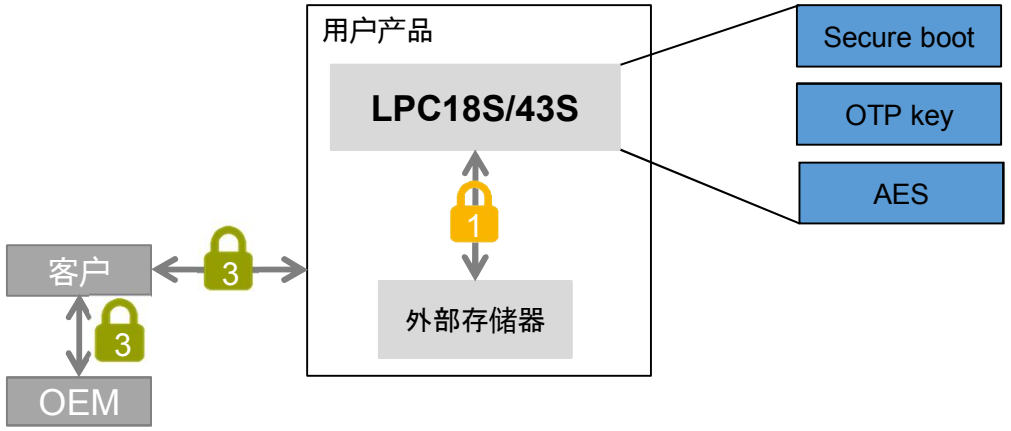



- ✓ AES 加密
  - 低复杂度（较public key 算法）
  - 扩展性较差（不易分布系统key）

或

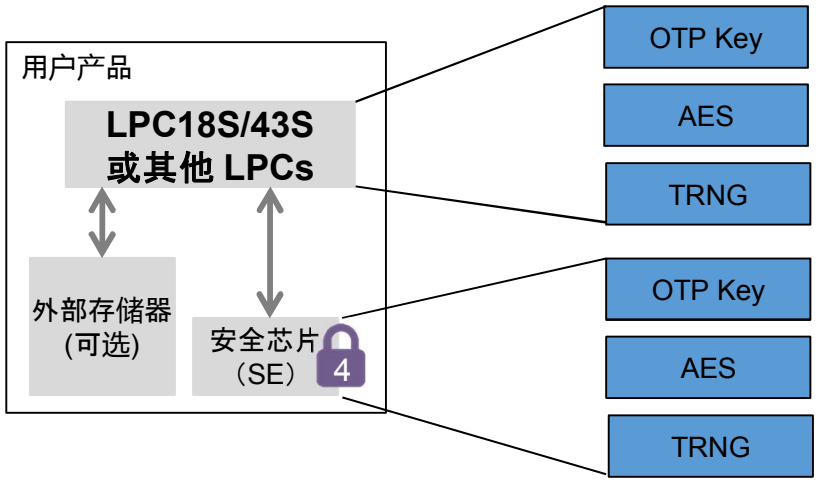
- ✓ 非对称加密算法 public key/private key（较高复杂度，扩展性强）
  - AES 实现块加密/解密算法
  - 随机数生成器（TRNG）产生随机会话密钥（session key）

# 防止未授权的仿造产品



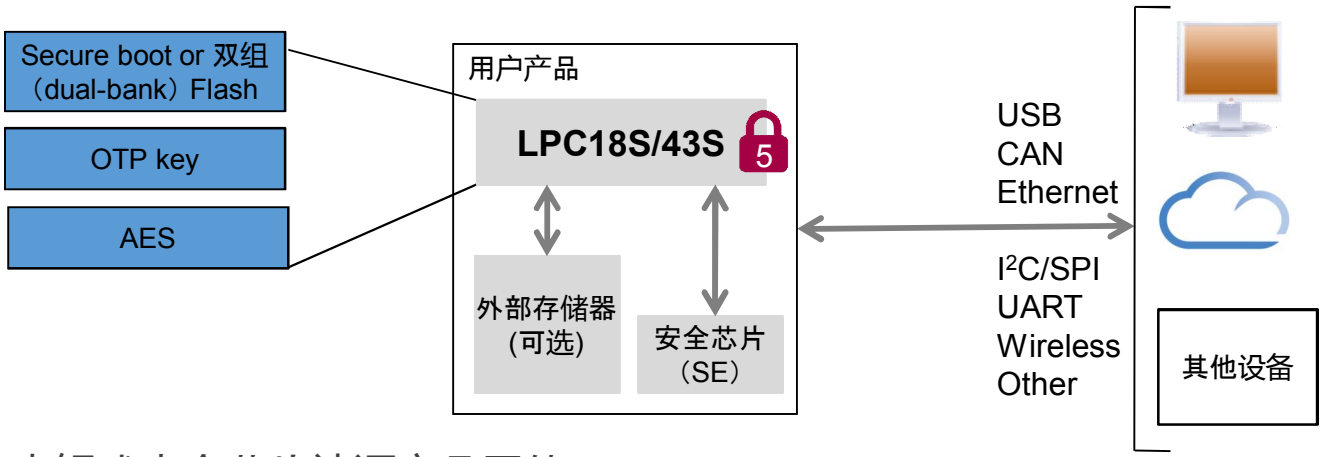

- MCU使用外部存储器应用“安全启动”技术(Secure boot)
- “安全启动”技术解密、认证保存在外部存储器中的固件
  - OTP 密钥存储保证KEY的安全性
- 提供客户预编程的MCU（带OTP）和加密的固件

# 保护外部存储器的安全可靠性




- 在系统中存储密钥，防范攻击
- 密钥存储解决方案
  - 存储密钥于FLASH存储器中（容易被攻击）
  - 存储密钥于LPC18S/43S MCUs OTP中 – 密钥不可更改
  - 存储密钥于NXP A7x 安全芯片– 经安全认证的FLASH存储

# 安全的固件升级

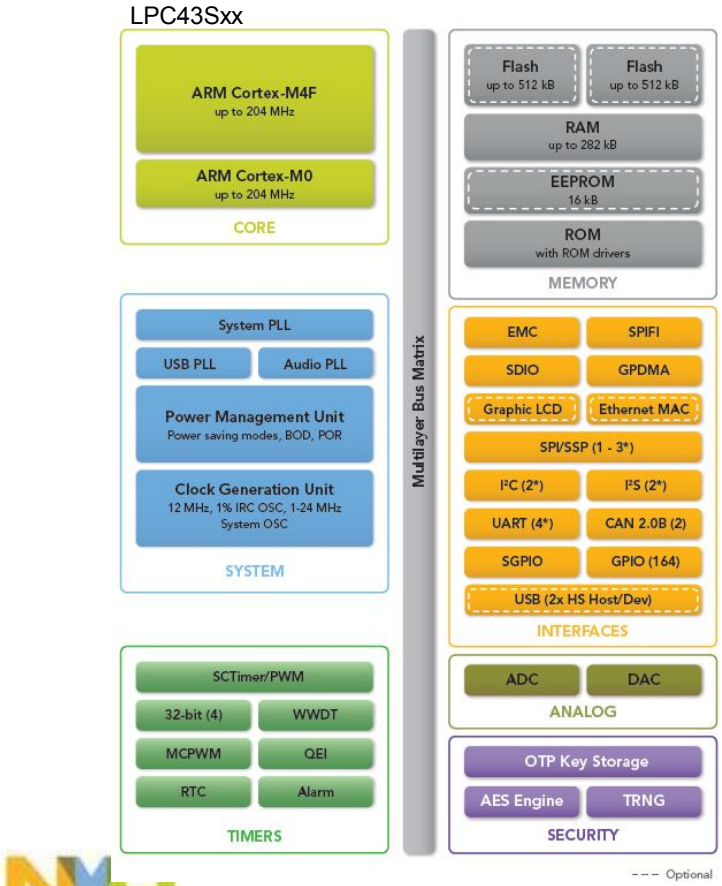



1. 通过OTP密钥或安全芯片认证产品固件
2. 下载固件
   - **对称加解密算法**: 运用OTP密钥加解密
   - **非对称加解密算法**: 运用公钥设施（PKI）产生临时密钥加解密
3. 烧写固件到存储器
   - **带有片内FLASH的MCU**: 烧写解密固件到FLASH并激活
   - **使用外部FLASH的MCU**: 使用OTP密钥加密固件, 烧写外部FLASH 并切换到2nd bootloader

# 全方位的数据保护 – 代码, 数据, 传输…


| | | **MCUs** for embedded applications | **LPC18Sxx/LPC43Sxx MCUs** | |
|---|---|---|---|---|
| | | | **+ security software** | **+ security hardware** | **+ A7 secure element** |
| **Handles AES keys** | Generation | | • Software RNG | • True RNG | • Certified True RNG |
| | Storage | | • Flash | • Encrypted in OTP unique per device<br>• Not software readable | • Extraction proof using banking-grade security |
| **Prevents software tampering** (software integrity) | | • Code read protection | • Code read protection | • Code read protection<br>• Secure boot | • Secure boot with FW signatures verification<br>• Secure firmware update |
| **Establishes secure connection** (message confidentiality) | | | • Software authentication | • Software authentication | • Hardware-accelerated tamper proof authentication and setup of session keys |
| **Secures bulk message transfers** | | | • AES software encryption | • AES hardware-accelerated encryption | • AES hardware-accelerated encryption with tamper protection |

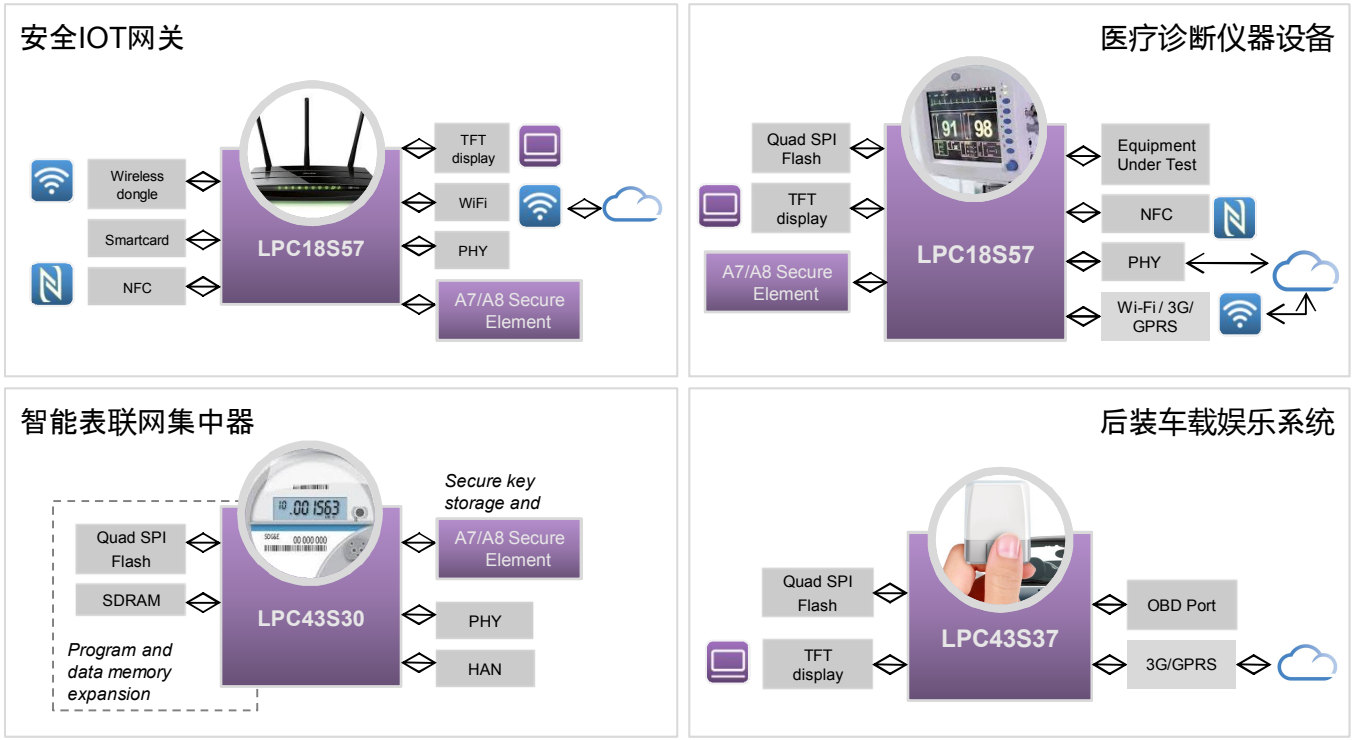
# LPC18Sxx and LPC43Sxx 集成安全模块的MCU系列




- **与LPC18xx & LPC43xx 系列具有相同的特性**
  - 高性能Cortex-M 内核:
  - 大容量内部存储器,支持外部内存扩展
  - 丰富的外设, 支持多种高速连接和显示

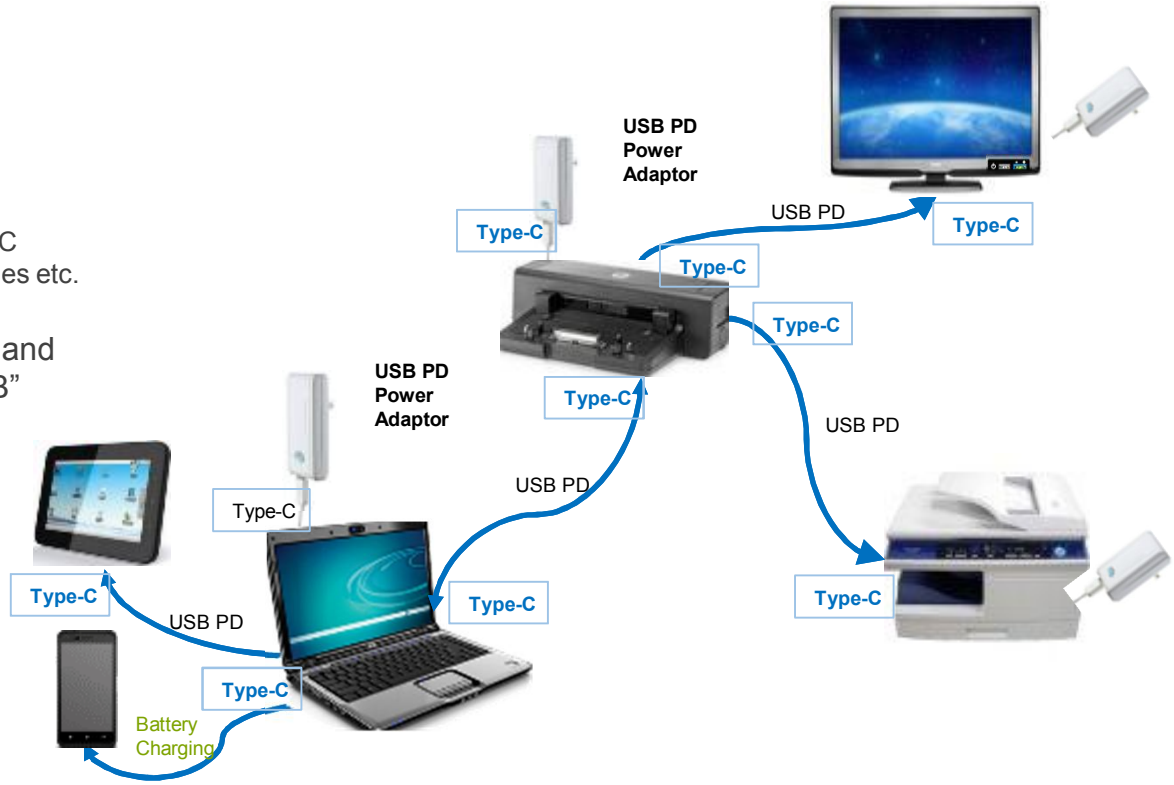
- **安全模块: 保护数据通信和应用代码**
  - 硬件加速的AES-128加密引擎
  - 两组128位OTP存储控制器
  - 真随机数产生器
  - Boot ROM 驱动程序支持授权的安全启动,加密烧录得固件
  - CRP代码读保护

# 典型应用示例


安全IOT网关
Wireless dongle
Smartcard
NFC
LPC18S57
TFT display
WiFi
PHY
A7/A8 Secure Element
医疗诊断仪器设备
Quad SPI Flash
TFT display
A7/A8 Secure Element
LPC18S57
Equipment Under Test
NFC
PHY
Wi-Fi / 3G/ GPRS
智能表联网集中器
Quad SPI Flash
SDRAM
Program and data memory expansion
LPC43S30
Secure key storage and
A7/A8 Secure Element
PHY
HAN
后装车载娱乐系统
Quad SPI Flash
TFT display
LPC43S37
OBD Port
3G/GPRS

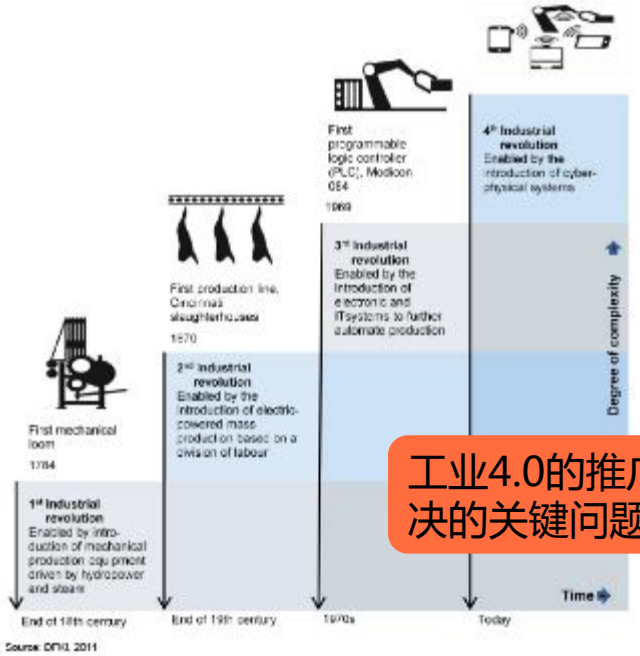
# 在USB Type-C PD(Power Supply)系统中的安全和认证

- 恩智浦提供USB Type-C 的解决方案
  - Systems
  - Cable and dongle adaptors
  - AC/DC power adaptors
- 为什么Type-C需要安全认证
  - Tamper resistant highly secure authentication IC solutions to verify that Type-C peripherals, cables etc. can be trusted
  - Enabling reliable and safe connections and preventing counterfeiting and “Bad USB”
- 恩智浦完整的安全认证方案
  - Secure Hardware (A7101…)
  - Secure Crypto Library
  - Secure Java Card Operating System (JCOP)
  - Proven Development Tools
  - Secure Manufacturing Facilities
  - Secure Key Insertion
  - Host Library Reference Code
  - Industry leading security experts



# 面向工业物联网的安全连接

## 工业革命的历史进程

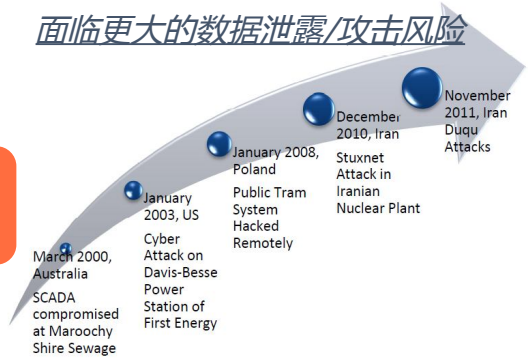



工业4.0的推广，必须要解决的关键问题是网络安全！

## 工业4.0*

- 工厂级别的M2M (Machine to Machine)
- 流水线上的部件可通过电子标签进行智能识别
- 设备通过无线传感器网络互联
- 其他表述: 智能工业或者工业物联网

*面临更大的数据泄露/攻击风险*




•* source: Siemens website
•** source: Frost and Sullivan, Schneider

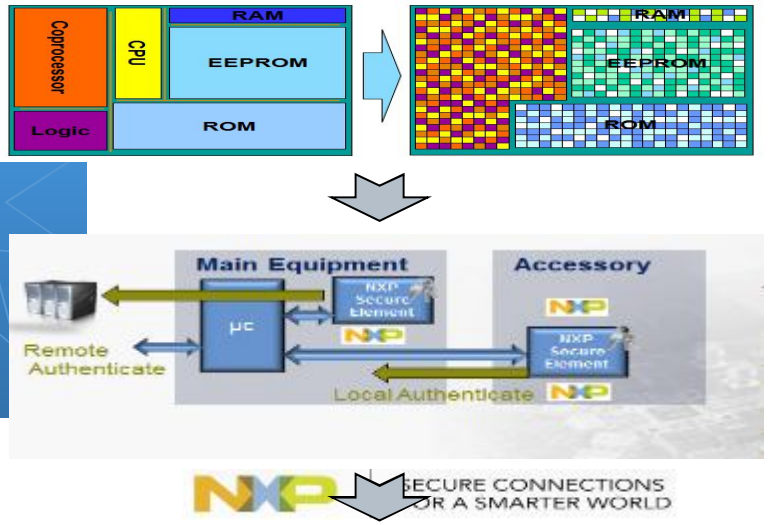
# NXP的安全技术，为无线传感器网络保驾护航

网络安全
解决方案

无线传感器网络
解决方案

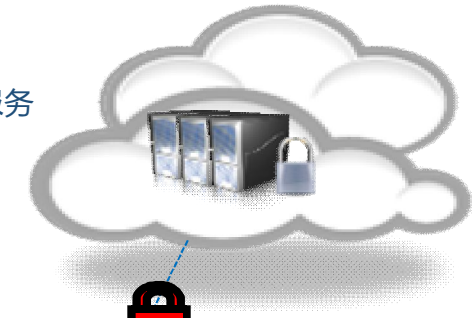
基于RFID的智
能物流和智能
制造解决方案

NXP的安全单元(SE)为工业互联网中的节点提供芯片银行卡级别的安全保护

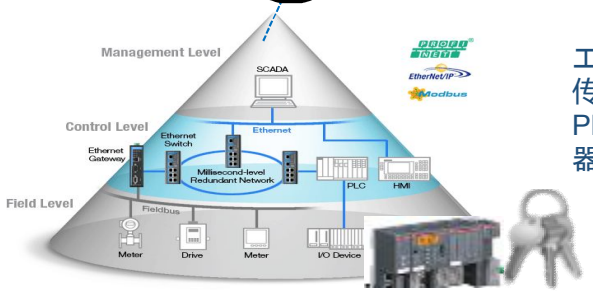



端到端的系统安全性

工业IoT云服务



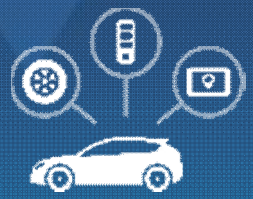
工业IoT/工业4.0网关




工业设备 (工业传感器节点，PLC，工业控制器等)

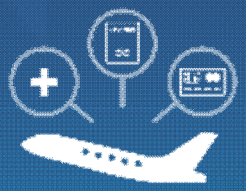
# 恩智浦半导体助力中国物联网与工业互联网(工业4.0)应用

- 安全的物联网节点
- 无线自组织网络
- 智能传感器
- 智能照明
- 工业4.0网关于云安全
- 低功耗微处理器

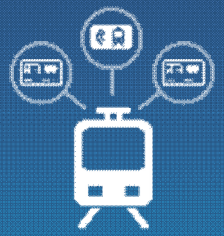


- 车载娱乐
- 车内通信系统
- 智能汽车与安全
- 车联网与汽车雷达

- 银行卡安全
- 移动支付
- RFID标签
- 智能供应链管理
- 近场无线通信



- 电子护照
- 智能识别
- 交通、医保卡

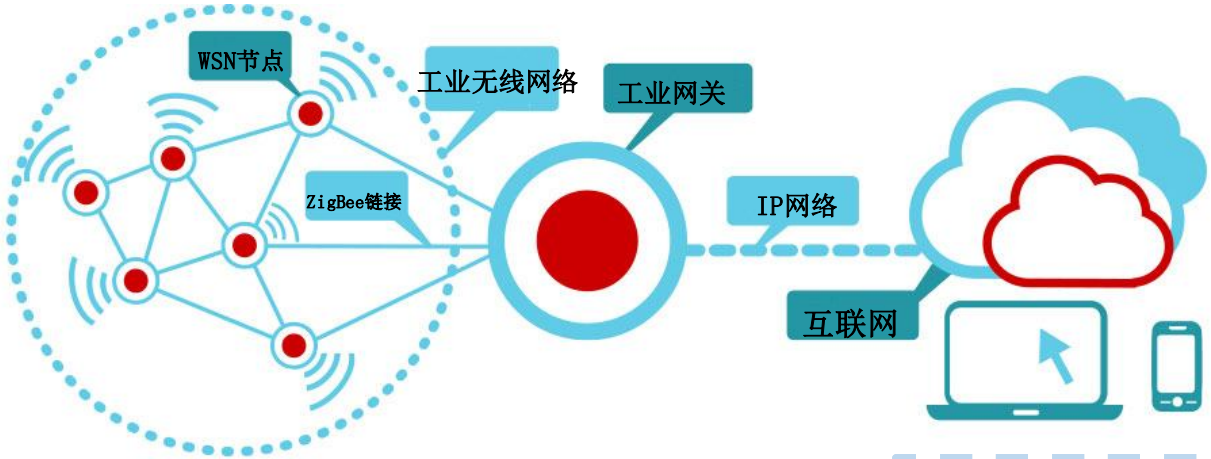


- 非接触式射频卡
- 存取控制
- 小额支付

# 智慧生活，安全连结

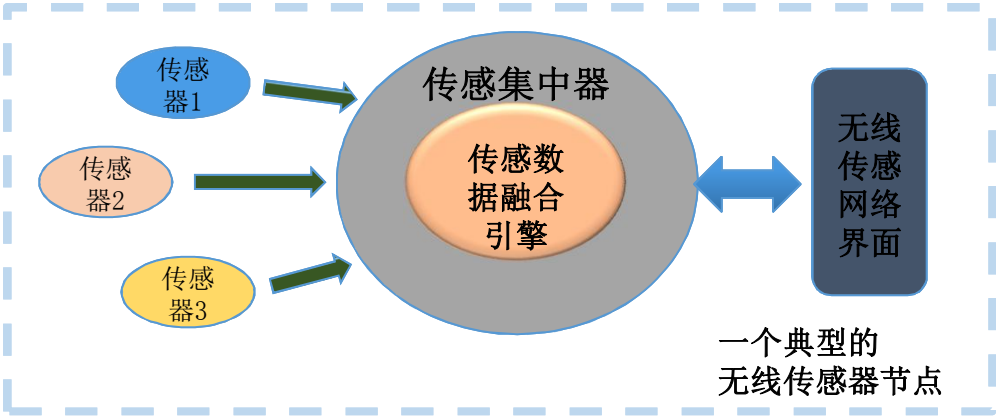
SECURE CONNECTIONS
FOR A SMARTER WORLD

# 物联网(IOT)架构：智能传感器-传感集中器-传感器网络

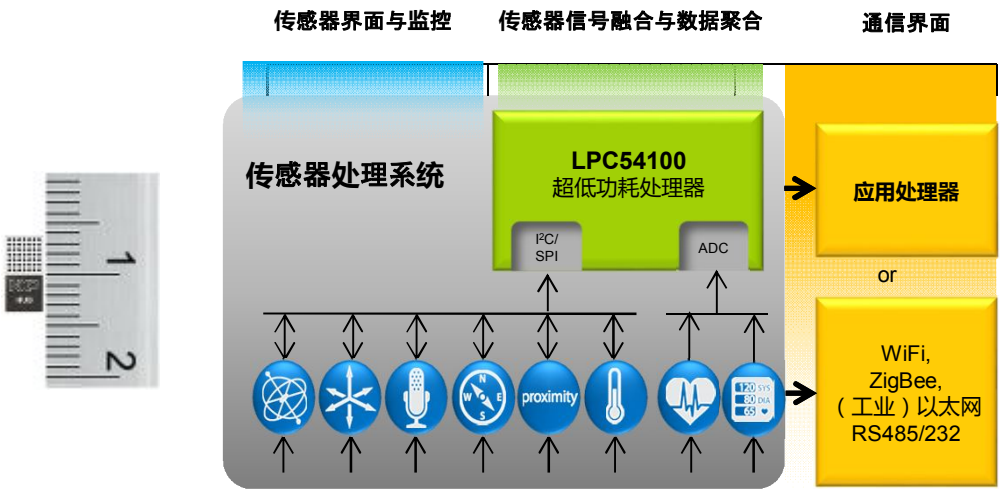


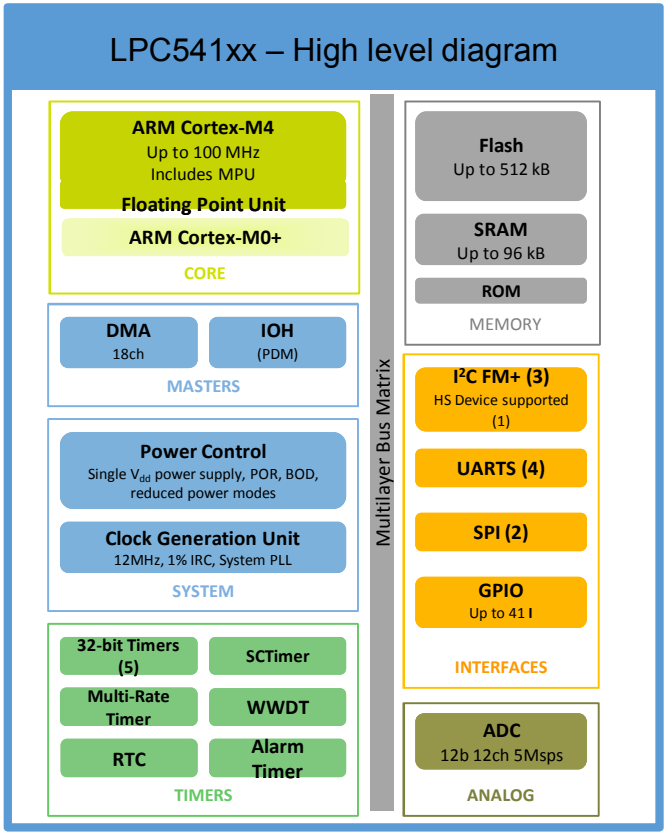

- 布线成本和柔性制造所需的灵活性
- 无线互联成为显著发展趋势；
- 大量的无线传感器需要电池供电以满足真正“无线”的需求；

- 复杂的工业环境下互联 提出了高可靠性需求；
- 单个网络的组网规模可能高达数百节点以上 - 可扩展性；
- 所有节点能够通过工业网关与云端互联



# 传感集中器(Sensor Hub) – 单节点上集成多种传感器输入和信号处理能力




- uA级别的低功耗模式：监听传感器数据并保持RAM存储器工作
- 高效的ADC: (12-bit, 4.8 Msps) at any voltage (1.62 to 3.6V)
- 多种传感器界面
- 传感数据融合：去除冗余信息，降低数据传输量，节约电能，提高网络性能
- 可搭配安全单元(Security Element)