# 为安全智能的工业物联网护航

## ——如何守住工业物联网的安全防线？

工业物联网（IIoT）作为推动数字经济与实体经济深度融合的关键路径，现已成为全球主要经济体促进经济高质量发展的共同选择。据麦肯锡调研报告显示，工业物联网在 2025 年之前每年将产生高达 11.1 万亿美元的收入。全球知名咨询公司埃森哲也给出了积极预测，称到 2030 年，工业物联网能够为全球带来 14.2 万亿美元的经济增长。

在今年的全国两会上，“工业物联网”这一关键词被第四次写入政府工作报告中，充分体现出国家对工业物联网在推动制造业高质量发展方面发挥更大作用的高度重视。中国信息通信研究院发布的《工业物联网产业经济发展报告（2020 年）》显示，2020 年，中国工业物联网产业经济规模达 3.1 万亿元，占 GDP 比重为 2.9%，带动约 255 万个新增就业岗位。

### 安全威胁是真实存在的

面对正在快速发展的工业物联网，保障其安全性至关重要。因为安全威胁是真实存在的，设备、连接、网络、数据中心、设备管理，物联网的每一个环节都有可能遭到攻击。那么，用户在部署工业物联网方案时，会遇到哪些关键性的安全挑战？

### 企业新旧设备优化

工业物联网需要面对各种各样的设备。有的是使用多年的旧设备和系统，有的是在进入物联网时代后全新推出的设备，它们可能会遍布各地，黑客可以直接对设备发起攻击，传统防火墙、IPS 等网关类防护设备用处不大。

同时，物联网的通信协议，诸如 ZigBee®、蓝牙、NB-IOT、2/3/4/5G 等在传统互联网应用上并没有使用到，互联网安全策略也无法覆盖到这些协议，因而带来了新的安全风险。

### IT 与 OT 融合的焦虑

物联网转型让工业设备变得更加智能且集成度更高，从而提高了生产制造的效率。随着数十亿设备通过物联网连接起来，信息技术（IT）和操作技术（OT）融合的时代已经到来。

但工业物联网对实时性、可靠性和产品监控质量的要求极高。作为工业自动化的骨干系统之一，控制系统如何在保障安全的同时，进行数字化升级，是行业用户和方案供应商面临的焦点问题之一。

### 标准

设备一旦进入网络，就会面临各种安全性威胁。目前，网络攻击已从针对远程企业 IT 云服务器和数

据中心转向传感器、边缘节点和网关等本地设施，攻击媒介也不仅限于 TCP/IP 网络和端口。

考虑到在工业物联网中存在大量有线和无线的标准，所以安全设计不但应该从设计之初贯彻到量产，还需要在系统内部建立多层独立安全等级（Multiple Independent Levels of Security, MILS）的设计理念——在确保系统灵活性的前提下，针对一个系统的不同层级都提供安全性。

## 坚决贯彻，而非仓惶补救

如何充分利用芯片级的安全性，实现全面的系统保护？如何在最初的开发环节就把安全要素考虑进去，并贯穿其整个生命周期？在 Microchip，我们也对此思考了很多，例如：

- 可信平台

随着越来越多的设备连接到互联网，主要的云供应商现在都鼓励用户使用安全元件来保护密钥。Microchip 为 CryptoAuthentication™ 系列推出的可信平台提供了一套软件和硬件开发工具，该平台结合了 Microchip 的安全元件和内部的安全密钥配置服务。Microchip 的配置服务仅在其半导体供应链工厂内“装载”密钥，这样一来就消除了密钥暴露给合同制造商或任何第三方的机会。这种方法也提升了 Microchip 一直希望达到的加密密钥、固件和人之间的“空气间隙”（air gap）隔离。

作为第一个为大众市场提供随时可用的安全身份验证解决方案，可信平台由三层组成，提供开箱即用的预配置安全元件或可完全量身定制的安全元件，开发人员可根据个人设计灵活选择。

该平台第一层为 Trust&GO，提供零接触预配置安全元件，设备证书已在 ATECC608B 中预先编程、装载和锁定，用于自动云登录或 LoRaWAN®登录时的身份验证。与此同时，相应的证书和公钥以“清单”文件的形式交付，文件可从 Microchip 直销网站和授权分销商处下载。除了节省长达数月的开发时间外，新解决方案还大幅省去其它繁琐事项，帮助大众市场客户轻松进行边缘设备保护及管理，无需第三方配置服务或证书颁发机构的额外费用。

目前，Microchip 已与业界多家云供应商合作，帮助其以更经济的方式轻松实现基于硬件的安全性，消除之前配置设备时的各种障碍。如需了解更多信息，请访问 **Microchip Trust&GO 平台**。

如果客户有更多定制需求，第二层 TrustFLEX 不但可灵活地使用客户选择的证书颁发机构，同时还可使用预先配置中的使用案例，包括基线安全措施，如传输层安全协议（TLS）增强身份验证（用于使用任何证书链连接到任何基于 IP 的网络）、LoRaWAN 身份验证、安全启动、无线（OTA）更新、IP 保护、用户数据保护和密钥轮换，从而减少了设备定制的复杂性，缩短定制时间，同时无需定制的部件号。针对只需要定制设计的客户，该平台的第三层—TrustCUSTOM —可为客户提供特定的配置功能和自定义凭据设置。

- 守卫无线 MCU 的安全

随着物联网从家庭自动化领域拓展到如暖通空调（HVAC）、车库门和电风扇等家庭控制领域，以及在建筑和工业自动化领域的加速应用，市场对高度集成、可靠和安全的工业物联网连接性的需求前所未有地增加。

WFI32E01PC 是 Microchip 采用自有 Trust&GO 技术的业界首款 Wi-Fi®单片机模块，用以实现独特的身份验证功能。其使用的新技术包括顶尖的 PIC32 单片机内核、丰富的外设支持和成熟的硬件安全平

台。例如 Trust&GO 平台采用安全元件技术，为云身份验证进行预先配置和设置，简化了网络身份验证的过程；模块符合 Wi-Fi 联盟（WFA）规范，并获得美国联邦通信委员会（FCC）、加拿大工业部（IC）和欧洲无线电设备指令（RED）三家世界级监管机构的全面认证。

凭借自身的安全专业知识，Microchip 为客户提供设计的安全性，并消除客户对建立昂贵的内部安全能力的需求。从安全加密到可信执行环境，Microchip 通过广泛的安全解决方案支持并满足客户独特的安全实施需求，以合理的价格提供适当的保护级别。

## 结语

其实对包括工业物联网在内的所有物联网产品和应用而言，通常就包含三个核心要素：处理器或单片机（“智能”元素）、网络控制器（“连接”元素）以及确保与云安全通信的方法（“安全”元素），而 Microchip 的优势就在于有能力横跨“云”-“管”-“端”三重领域，为用户提供完整的解决方案。

换句话说，Microchip 既可提供具备高级安全功能的集成方案，也能提供诸如 ATECC608B 这样的独立方案。Microchip 的一系列单片机均内置了硬件保护功能，以实现牢不可破的安全性。Microchip 强大的安全解决方案使物联网应用开发人员能够实现各种安全用例，例如安全启动，确保仅执行真正的应用程序固件；安全固件升级；通过相互认证实现安全的云连接；安全通信实现消息认证和加密和 IP 保护等。

除安全芯片外，Microchip 还提供软件示例和配置服务，方便客户能够通过软硬件协同配合，在其嵌入式系统中轻松、顺畅地实现安全防护。

安全是物联网应用的一个重要组成部分。每种物联网解决方案应该都含有安全相关模块——特别是在需要确保系统身份安全和传输数据安全时。确保物联网安全不仅要靠相关法规，更重要的是在实践中从根本上采取负责任的做法，而且应该从产品概念设计阶段就把安全纳入考虑之中，而不应该是事后的亡羊补牢。

如需了解更多信息，请访问 **Microchip CryptoAuthentication™系列推出的可信平台**。