Application Note

支持 SimpleLink™ Wi-Fi® 的电子智能锁

Benjamin Moore, SimpleLink Wi-Fi Applications Team

摘要

本应用报告介绍了支持 Wi-Fi® 的电子智能锁（电子锁）的开发，具体而言，阐述了在电子锁设计中增加 Wi-Fi 的优势。

文中介绍了不同的 Wi-Fi 用例，并估算了两个主要用例中的系统电池寿命。本应用报告演示了 SimpleLink™ Wi-Fi 可实现电池供电的电子锁设计，从而使用户能够通过云端安全地对电子锁进行监控。

本文引用了使用 4 芯 AA 电池并可实现 5 年以上电池使用寿命的智能锁参考设计 [1]，它可作为一个*智能锁参考设计*。有关支持文档和其他资源的列表，请参阅节 8。

内容

商标

1 引言

锁具的历史由来已久，而且数千年来经过不断演变，门锁已成为具有电子控制和无线接口的更加复杂的系统。作为安防系统的第一道防线，锁控制着可以进入住宅和楼宇的人员。

这些新型锁通常被称为*电子智能锁*（电子锁）。电子锁正在改变我们对门锁的认知以及交互方式。标牌、钥匙卡、PIN 码甚至移动设备都可用作锁门或将门锁打开的钥匙。对于很多住宅应用，用户使用电子锁则无需携带实体钥匙。而且，改变开门所用钥匙的形式帮助解决了传统锁面临的一个主要问题，即提供了一种快速创建和管理进入密钥的方法。

在电子锁系统中使用 Wi-Fi 连接，用户就可以随时轻松创建和管理进入密钥。Wi-Fi 连接还可实现一些新功能，例如远程监控电子锁。而且，将 Wi-Fi 直接集成到电子锁中，用户无需使用网桥就可将电子锁连接到互联网。集成式设计提供了可降低总体 BOM 成本的一体化产品，并支持需要电子锁直接处理大量信息的应用。本文档讨论了在电子智能锁设计中集成 Wi-Fi 的多个用例及其优势，以及对具有 Wi-Fi 连接功能的电子锁的一些关键要求。具体而言，本指南介绍了 SimpleLink Wi-Fi 如何支持电池供电类电子锁的开发，从而使用户可以通过云端安全地对电子锁进行监控。

2 术语

本文中使用了以下术语。

非对称密钥 非对称密钥对用于算法中，其中一方使用密钥执行加密操作，另一方则使用另一密钥执行相反操作。密钥对可定义为公共和私有密钥，最常用于数字签名和对称密钥分配。

真实性 真实性确保资产或实体是真实的，且已获得执行某一任务的授权，或者可按预期使用。验证过程通常涉及加密算法，该算法用于检查实体的真实身份与宣称的身份是否相符。某些预定义的信任机制始终属于验证机制的一部分。

证书 证书是标准格式文件。其中通常包含使用者公共密钥，以及头文件和公共密钥的 CA 签名。可提供 CA 公共密钥（若是证书链，则为子 CA）的任何人都能够验证使用者的身份。

机密性 机密性可确保资产不会供未获授权的实体使用，也不会向此类实体披露。在大多数情况下，机密性涉及加密，而在其他情况下，则使用混淆技术来保持机密性。

完整性 完整性是描述对象与原始版本相比保持完好无损的属性。

密钥 密钥用于数据加密、密钥建立和数字签名。密钥长度和类型取决于所使用的算法、具体用途和安全级别。

安全措施 旨在为某些资产提供预期保护以抵御某些威胁的措施。

3 电子智能锁（电子锁）

根据使用场合，电子锁通常可以分为两种类型：

- 商用锁（酒店、办公室、购物中心等）
- 住宅锁（家庭或公寓）

根据是否使用锁来保护住宅或商业楼宇，系统设计的注意事项有所不同。

3.1 住宅级

住宅锁设计用于房屋外部，通常安装在大门上。用于住宅的电子锁通常由电池供电，至少使用一年才需要更换电池。门和室内路由器之间的距离存在差异，因此有必要为住宅应用选择具备可靠连接功能的 Wi-Fi 器件。其他低功耗射频技术通常用于支持钥匙（钥匙卡或移动设备）和住宅电子锁之间的点对点连接。

图 3-1 显示了住宅电子锁系统中的典型无线连接示意图。

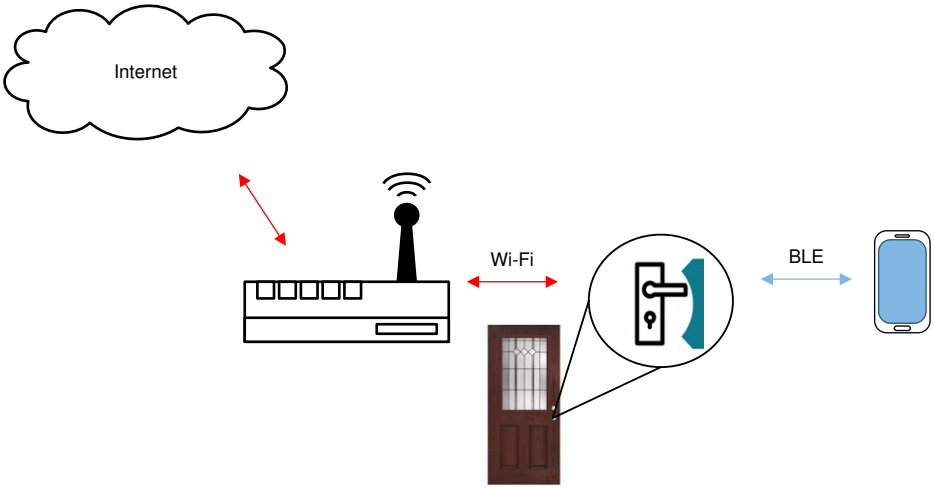

图 3-1. 住宅电子锁系统

3.2 商用级

商用锁可安装在楼宇外部，控制人员首次进入；楼宇内部安装商用锁可控制人员进入仅限特定人员进入的区域。一些商用锁设计为线路供电，但很多则采用电池供电。电池供电的商用锁通常会大量部署，因此面临严格的功耗限制。由电池供电的锁必须定期更换电池，因此在楼宇内大规模使用时，会导致大量的维护工作和成本。因此，具有超低功耗模式和极短唤醒时间的 Wi-Fi 解决方案对于商用电子锁应用至关重要。

4 Wi-Fi 用例和优势

与不提供直接互联网连接的其他低功耗射频技术相比，在电子智能锁设计中集成 Wi-Fi 的做法具有明显的优势。将家庭接入点 (AP) 直接连接 Wi-Fi 可实现以下功能：

- 通过互联网连接随时随地锁门或开锁
- 在每次锁门或开锁时收到通知
- 随时随地执行快速无线 (OTA) 更新
- 通过云端轻松添加或删除授权用户并进行身份验证
- 通过直接连接到云端的单个门锁解决方案，降低系统成本并提升最终客户的易用性

4.1 随时随地上锁或开锁

将电子门锁直接连接到家庭 AP，就可以通过互联网随时随地对门锁进行操作。将门锁连接到 AP 之后，就可以创建与远程云服务器的连接。然后，用户就可以使用另一连接互联网的设备（如智能手机、平板电脑或 PC）通过云服务器与门锁进行通信。

用户可以随时了解门锁的开关状态，从云连接中受益。如果门锁意外打开，用户无需回家，就可以快速检查门锁的状态，然后通过移动设备上锁。同样，拥有门锁遥控装置的主人可以随时选择让某人进入家里。如果有人丢了钥匙，或者不需要长期来访（例如修理人员、邮递员等），按需控制非常有用。

4.2 了解何时有人对锁进行操作

将 Wi-Fi 集成到电子智能锁中的另一优势是当有人对锁进行操作时，用户可收到通知。当锁的状态改变时，它会将该信息推送到云服务器，然后服务器会将通知消息转发给用户。

借助即时通知，锁的主人就可以方便地获得有人到达他/她家的信息。例如，当孩子从学校回家，或保洁人员来清理房屋时，就会生成通知。同样，如果有人试图撬开电子锁或破门而入，系统也会向主人发送通知。

4.3 执行快速 OTA 更新

对于连接互联网的产品（如支持 Wi-Fi 的电子锁），需要更新系统文件和软件。随着时间的推移必须替换的文件示例包括设备证书和密钥，云端使用这些证书和密钥来确定并建立与门锁的安全连接。可能还需要更新软件来实现新功能，修复现有问题或安全漏洞。电子锁通常安装在门上，因此如果让用户从门上拆下锁并使用物理连接来执行更新，这种做法并不现实。实行无线更新机制（也被称为“无线 (OTA) 更新”）提供了一种简便的方法让系统保持最新状态。

也可以借助其他低功耗射频技术实行 OTA 更新，但这些方法通常不切实际。例如，使用低功耗点对点技术需要用户在场才能进行更新。在这种情况下，通过用户的移动设备使用移动应用直接对门锁进行更新。而且，根据该技术提供的吞吐量，用户可能还需要等待几分钟才能完成更新。

另一方面，具有集成式 Wi-Fi 和互联网连接的电子锁可以通过 AP 自动更新，而无需用户在门锁旁操作。用户还可以利用更高的吞吐量来加快更新过程。对于商用电子锁应用，由于集成了 Wi-Fi，无需手动更新电子锁固件，从而可以显著节省成本和时间。

4.4 轻松地添加或删除用户

传统锁的主要限制是为用户配一把新钥匙所花的时间。配一把实体钥匙需要特殊的机器，并且需要花费较长的时间。甚至使用键盘或无线接口开锁后，用户要对锁进行实际操作来创建一个新 PIN 或数字钥匙也不方便。

在电子锁设计中增加 Wi-Fi 连接后，锁就可以在本地或云端存储身份验证列表。将使用白名单或受认可用户列表来确定是否为用户提供基于数字钥匙的访问权限。当所有者想要添加或删除用户时，过程非常简单，即所有者创建一个包含唯一钥匙和访问限制的新个人资料，然后新用户信息就会作为更新被推送到锁中或云端。

4.5 无需多余的网桥硬件

制造商可以创建一个在非 Wi-Fi 电子锁和家用 AP 之间建立链接的设备，从而在电子锁中增加 Wi-Fi 相关功能。这类被称为*网桥*的设备必须能将数据包转换为可由电子锁直接使用的协议（如低功耗 *Bluetooth*® 或 Sub-1GHz 协议），以将电子锁与本地 Wi-Fi 网络连接。

而网桥并不是理想的解决方案，因为它会增加整体系统设计的复杂性，还会增加最终用户的总体系统成本。增加网桥硬件并不可取，因为它通常需要壁式插头，并会占用更多空间。

与使用网桥相比，采用将 Wi-Fi 直接集成到锁中的方式，可以降低最终用户的成本，简化用户体验，并可帮助开发人员开发出依赖电子锁高数据处理量的新功能。

5 Wi-Fi 连接和功耗用例

可以通过很多不同的方法在电子智能锁（电子锁）中使用 Wi-Fi 连接功能。实现的功能数量和所需的功率预算取决于 Wi-Fi 连接功能的使用方式。下面列出了常用的 Wi-Fi 连接用例（按照从最低功耗到最高功耗的顺序排列）：

- 用于定期更新的 Wi-Fi 计划唤醒
- 通过传感器事件唤醒 Wi-Fi
- Wi-Fi 始终保持连接

仅在定期更新时开启 Wi-Fi 是功耗最低的用例。如果不通过 Wi-Fi 控制门锁，通常可以选择此用例（Wi-Fi 不总是激活状态）。通常，仅在定期更新时唤醒的系统将使用另一机制来接收访问凭证，例如键盘。例如，每天只需为办公楼或酒店客房更新一次或几次白名单。定期按计划唤醒可用于开启 Wi-Fi 和检查更新。同样，按计划唤醒可用于以 OTA 更新的形式向电子锁提供新软件。

另一个用例是通过传感器事件（例如按下按钮、被动红外传感器甚至低功耗蓝牙网络处理器等另一连接器件产生的中断）触发唤醒 Wi-Fi。触发唤醒有助于在降低功耗的同时，让系统能够响应用户。当用户靠近采用此 Wi-Fi 方案的门锁时，该锁使用传感器检测用户，然后连接到云端，从而对用户进行身份验证，或向主人发送推送通知。

Wi-Fi 解决方案必须缩短唤醒和连接周期，以便在触发唤醒时提供出色的用户体验。SimpleLink™ Wi-Fi 通过多个内置机制来缩短唤醒和连接时间，包括快速连接、快速 DHCP 更新和 TLS/SSL 握手的硬件加速。通过将这些机制搭配使用，SimpleLink Wi-Fi 大约需要 0.5 秒可从 4.5μA 的休眠模式中唤醒，建立与 AP 的 WPA2 安全连接，并创建与服务器的 TLS/SSL 连接。

当 Wi-Fi 保持连接时，Wi-Fi 用例支持更丰富的功能集。通过保持与云端的安全连接，可以按需访问门锁，并在发送数据时提供超低延迟。在始终连接的用例中，用户可以随时随地快速访问门锁。采用始终连接策略的设备面临的最大挑战是，如何通过互联网保持点对点连接，同时保持超低功耗状态。SimpleLink Wi-Fi 甚至能够在低功耗深度睡眠 (LPDS) 周期中保持套接字状态，从而解决了这一问题。

6 关键系统要求

电子智能锁（电子锁）通常由以下关键功能块组成：

- 人机界面 (HMI)
- 无线连接
- 主机微控制器
- 电机子系统
- 传感器
- 电源管理

图 6-1 显示了支持 Wi-Fi 的电子锁系统的典型方框图。

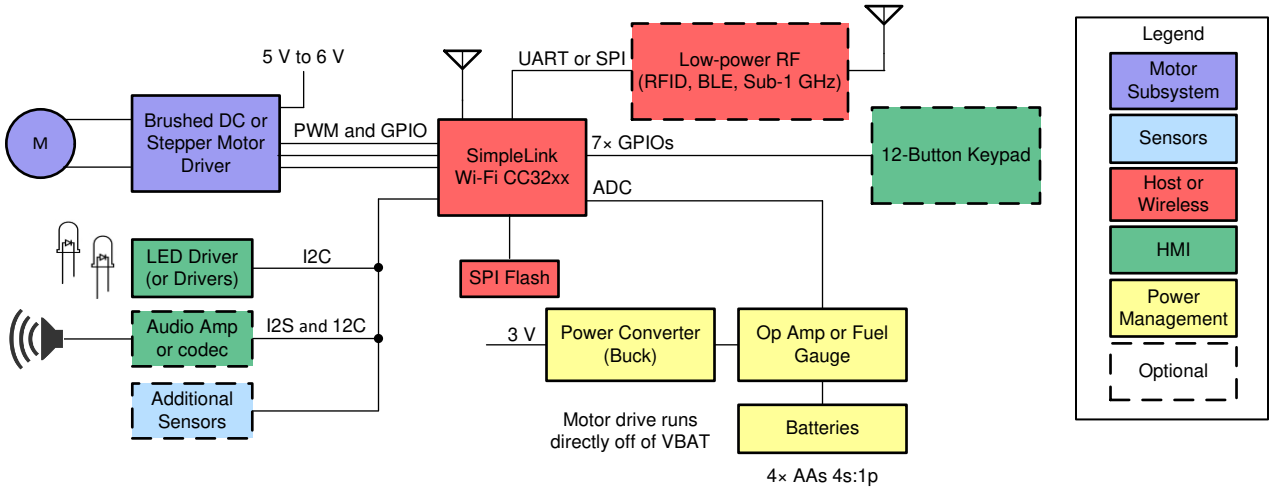

图 6-1. 支持 Wi-Fi 的电子锁系统示例方框图

HMI

HMI 为用户提供了一种与系统交互或查看电子锁响应的方法。HMI 可能包括键盘、背光、LED、扬声器，甚至麦克风。一些电子锁设计在与系统其余部分物理隔离的 PCB 上实现 HMI。采用 CapTIvate™ 触控技术的 TI MSP430™ 微控制器 (MCU) 专为电子锁提供专用的 HMI 控制器和工业电容式触控解决方案而设计。无线连接支持在远程设备（如智能手机或平板电脑）上操作键盘等部分 HMI 功能。

无线连接

无线连接[1]（如 Wi-Fi、低功耗蓝牙、Sub-1GHz 或 RFID）在锁中增加了一个额外的数据接口。此接口可用于各种用途，包括用户无线身份验证、远程控制和监控、软件更新的无线传输或与联网传感器的通信。在某些情况下，通过增加无线接口，就可以通过远程设备（如智能手机或平板电脑）操作部分 HMI 功能。

主机控制器

主机控制器负责处理来自用户和传感器的输入。它还通过驱动物理锁定机制或通过 HMI 提供反馈来生成响应。使用 CC3220 无线 MCU，可以将主机控制器和 Wi-Fi 集成到一个芯片中。

传感器

可以在电子锁中使用各种传感器，以检测锁和门的状态（例如使用加速计或惯性测量单元 (IMU) 来检测门的开关状态）或用户是否在场（例如，使用被动红外 (PIR) 传感器进行接近检测）。

电机子系统

电机子系统包括电机驱动器和用于驱动锁定机制的电机。电子锁通常使用有刷直流电机或步进电机来运行锁定机制。可以使用低压单 H 桥或双 H 桥电机驱动器（如 DRV8833、DRV8833C、DRV8837 和 DRV8837C 器件）来驱动这些类型的电机。

电源

电子锁通常由 4 芯 AA 电池供电。不同锁子系统的工作电压可能有所不同，这就要求系统中具备稳压器。设计人员必须谨慎选择合适的稳压器，因为这一选择会直接影响电池在系统中的使用寿命。

SimpleLink CC3220 无线 MCU 器件集成了多个支持电子锁设计的外设，包括 12 位模数转换器 (ADC)、具有 16 位脉宽调制 (PWM) 模式的通用计时器和多个串行接口标准。可利用通用异步接收/发送 (UART) 或串行外设接口总线 (SPI) 外设与协处理器或收发器进行通信，以支持在电子锁中应用更多射频技术（例如低功耗蓝牙、RFID 或 Sub-1GHz）。可以使用内部集成电路 (I2C) 外设与数字传感器进行通信，并在设计中配置所有音频编解码器或音频放大器。可以使用多通道音频串行端口 (McASP) 向音频编解码器或音频放大器传输数字音频，该端口支持 IC 间音频 (I2S) 位流格式。

可以使用 SimpleLink CC3120 网络处理器来代替 CC3220 器件，在已包含现有 MCU 解决方案的系统中增加 Wi-Fi 连接功能。主机 MCU 可以通过 UART 或 SPI 与 CC3120 器件进行通信。

[1] 设计人员必须确保在系统中使用多个射频收发器时，能够满足共存要求。

6.1 低功耗 Wi-Fi 电子锁

一个完整电子锁通常使用四节碱性 AA 电池（采用 4 芯串联、1 芯并联配置，即 4 串 1 并）供电。电子锁设计面临的一个最主要的挑战是如何降低电机子系统的功耗。如 *智能锁参考设计* [1] 中所述，优化电子锁的电源设计有助于降低电机子系统的功耗，并将电池寿命延长至数年。

目前，与数据流应用相比，Wi-Fi 电子锁需要发送和接收的数据量相对较少。仅会短时激活无线电以进行数据传输，因此 Wi-Fi 接口的有功功耗对于功耗的影响通常不及 Wi-Fi 器件处于睡眠模式下的功耗。SimpleLink Wi-Fi 在睡眠模式下实现的低功耗等级以及旨在通过网络学习算法最大限度地缩短激活周期的优化方案共同作用，满足了电子锁的电池寿命需求。

6.1.1 电流消耗和电池寿命

使用 *智能锁参考设计* [1] 中介绍的测量方式，我们可以估算使用 SimpleLink Wi-Fi 设计的电子锁在间歇性连接和始终连接用例中的电池寿命。实际的 Wi-Fi 电子锁设计可以在这些用例间动态切换，以实现功耗和性能的必要平衡。因此，这些估算可以作为基于 SimpleLink Wi-Fi 的电子锁的电池寿命估算范围。

6.1.1.1 间歇性连接

如节 5 中所述，可以将支持 Wi-Fi 的电子锁设计为：仅在需要与远程服务器进行数据发送或接收时打开 Wi-Fi 接口。可以按照唤醒计划或通过传感器触发器打开 Wi-Fi 接口。在这种情况下，系统将间歇性地连接到本地网络和云端。假设在间歇性连接用例中，当系统未连接到网络时，仍然处于休眠模式。在休眠模式下，不会保留应用处理器和网络子系统内存。在发送数据之前，每个唤醒周期都需要执行以下步骤：

1. 初始化系统（加载应用并唤醒网络处理器）。
2. 重新连接到本地网络。
3. 建立安全套接字会话。
4. 发送和接收数据。
5. 返回休眠模式。

在此用例中，可以根据每次门上锁或开锁时，触发器唤醒器件在 Wi-Fi 发送数据场景下的测量结果来估算 SimpleLink Wi-Fi 的功耗。

在估算时，我们假设每天平均发生 24 次上锁和开锁事件，如 *智能锁参考设计* [1] 所述。我们还假设，应用程序缓存了远程服务器的 IP 地址，因此每次当器件唤醒并重新连接到网络时，无需使用 DNS 查找。

图 6-2 显示了当使用 TLS 1.2 和 TLS_RSA_WITH_AES_256_CBC_SHA 密码套件连接到本地服务器时，采用 CC3220S 器件执行第 1 步到第 5 步的完整过程所需的平均功耗和总时间。图 6-2 显示在 0.510 秒时间内，消耗的平均电流约为 46.3mA。

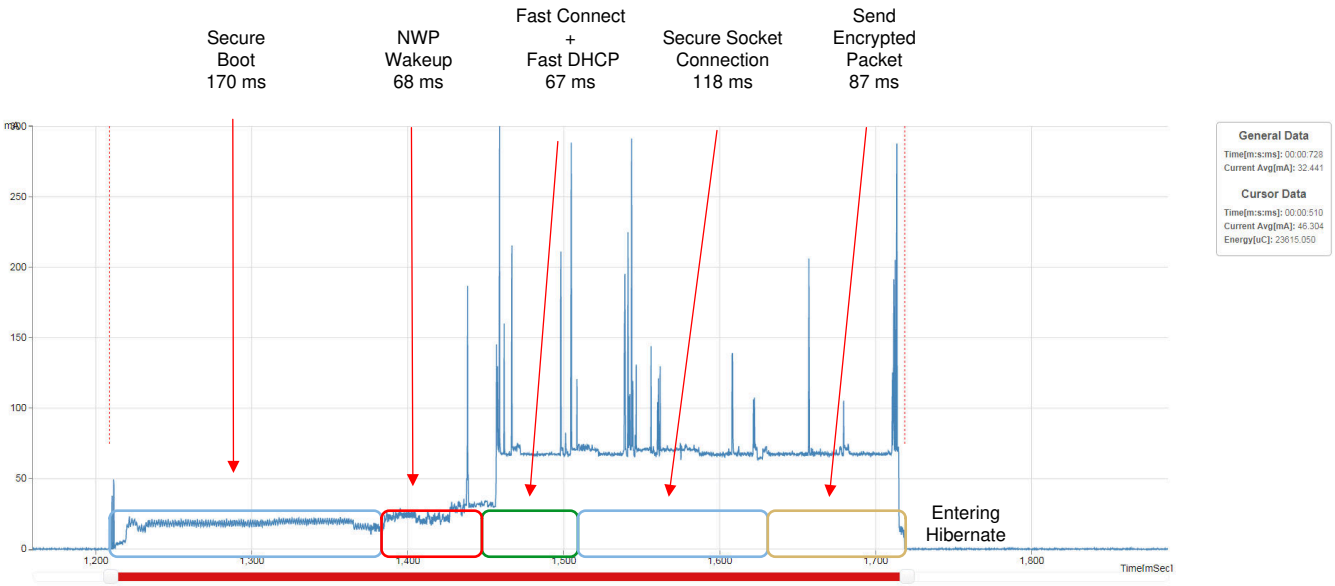

图 6-2. CC3220S 从休眠到 TLS 连接至本地服务器期间的功耗

因此可通过方程式 1 来计算 Wi-Fi 子系统的平均功耗。

$$P_{total} = \left(V_{on} \times D_{on} \times I_{on} + V_{off} \times D_{off} \times I_{off}\right)$$

$$P_{total} = 3\,V \times \left(\frac{24 \times 0.510\,s}{86400\,s} \times 46.3\,mA + \frac{86400\,s - (24 \times 0.510\,s)}{86400\,s} \times 0.0045\,mA\right)$$

$$P_{total} = 3\,V \times \left(0.00014 \times 46.3\,mA + 0.9998 \times 0.0045\,mA\right)$$

$$P_{total} = 0.0329\ mW\ (\approx 33\,\mu W) \quad (1)$$

将由方程式 1 得出的平均功耗与根据 *智能锁参考设计* [1] 计算出的总系统功耗相加，我们可以得出整个低功耗蓝牙和 Wi-Fi 锁系统的总体平均功耗为 0.523mW。根据 4 芯 AA 电池的理论总能量容量，我们可通过方程式 2 计算得出电子锁的电池寿命估值。

$$\text{Battery Life}_{yrs} = \frac{\text{Energy Capacity of Batteries}\,(mWh)}{\text{Average System Power}\,(mW)} \times \frac{1\ \text{day}}{24\ \text{hrs}} \times \frac{1\ \text{year}}{365\ \text{days}}$$

$$\text{Battery Life}_{yrs} = \frac{18000\ mWh}{0.523\ mW} \times \frac{1\ \text{day}}{24\ \text{hrs}} \times \frac{1\ \text{year}}{365\ \text{days}}$$

$$\text{Battery Life}_{yrs} \approx 3.9\ \text{years}\,(3\ \text{years, 11 months}) \quad (2)$$

图 6-3 显示了通过 *www.google.com* 连接服务器时，使用 CC3220S 器件执行第 1 步到第 5 步的完整过程所需的平均功耗和总时间。

NOTE

测量结果说明，与 Google™ 服务器建立安全连接所需的时间约为 1 秒，这是因为选择了椭圆曲线密码。椭圆曲线迪菲-赫尔曼密钥交换 (ECDHE) 和椭圆曲线数字签名算法 (ECDSA) 未通过硬件加密引擎加速。

图 6-3 显示了在 1.353 秒时间内，消耗的平均电流约为 38.1mA。

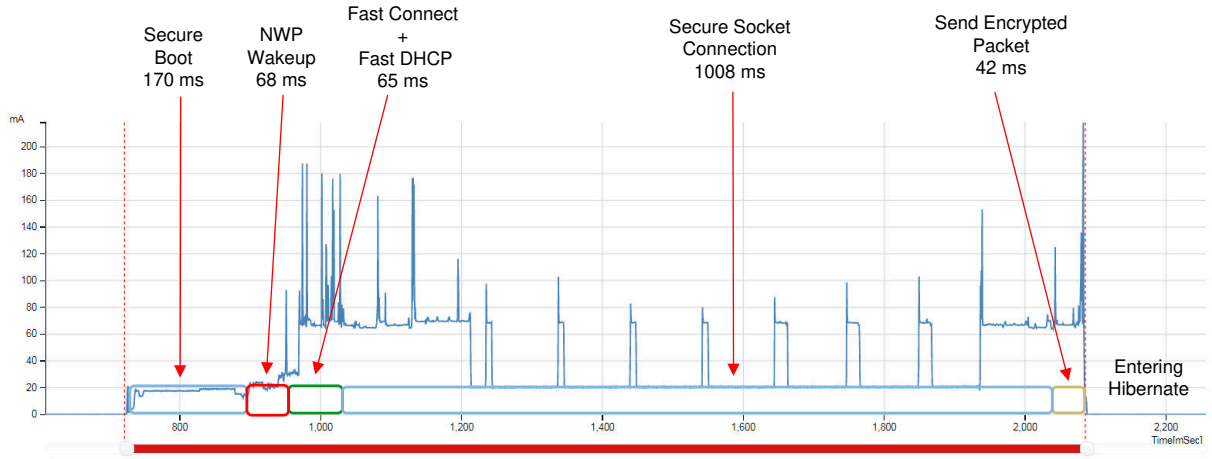

图 6-3. CC3220S 从休眠到 TLS 连接至 www.google.com 期间的功耗

因此，根据方程式 1 可计算出，连接到 www.google.com 时 Wi-Fi 子系统的平均功耗为 0.0569mW（约 57μW）。

将由方程式 1 得出的平均功耗与根据 *智能锁参考设计* [1] 计算出的平均系统功耗相加，我们可以得出整个低功耗蓝牙和 Wi-Fi 锁系统的总体平均功耗为 0.547mW。根据 4 芯 AA 电池的理论总能量容量，我们得出电子锁的电池寿命估值约为 3.8 年（3 年 9 个月）。

6.1.1.2 始终连接

除了节 6.1.1.1 中讨论的间歇性连接用例，还可以将电子锁设计为始终连接到 AP，从而为用户提供按需访问。在本例中，系统进入 LPDS 模式，并始终保持与远程服务器的安全套接字连接。系统仍然可以由传感器触发器唤醒以发送数据，还可以定期唤醒以接收来自 AP 的信标。通过接收信标，系统可以保持与 AP 的连接，并检索 AP 为系统缓存的所有数据。

在 802.11 省电模式的 SimpleLink Wi-Fi 实现和扩展中，可以跳过特定数量的信标，从而延长器件的睡眠时间，降低其在空闲状态下的总功耗。当 SimpleLink 器件处于睡眠模式时，AP 将缓存要发送给器件的数据，以防止数据丢失。跳过的信标数量由配置器件处于 LPDS 状态的持续时间决定，该时间被称为长睡眠间隔 (LSI)。网络学习算法可优化器件处于唤醒状态以接收每个信标的时间，将 LSI 与网络学习算法搭配使用时，SimpleLink Wi-Fi 可进一步降低功耗。对于本分析，我们假定 LSI 为 500 毫秒。

NOTE

AP 不会无限期缓存已连接站点的数据；因此，选择的 LSI 时间如果过长则会影响系统与 AP 的兼容性。开发人员负责为自己的产品选择合适的 LSI。

因为电子锁在每个锁定周期或解锁周期传输的数据量相对较少（估计小于 1000 字节），Wi-Fi 无线电每天只在一段很短的时间内处于激活状态。因此，可按照器件不发送数据时的功耗来估算始终连接模式下 Wi-Fi 子系统的平均功耗。图 6-4 显示了 SimpleLink Wi-Fi CC3220S 器件处于空闲状态（不发送数据）且 LSI 为 500 毫秒时的平均功耗。

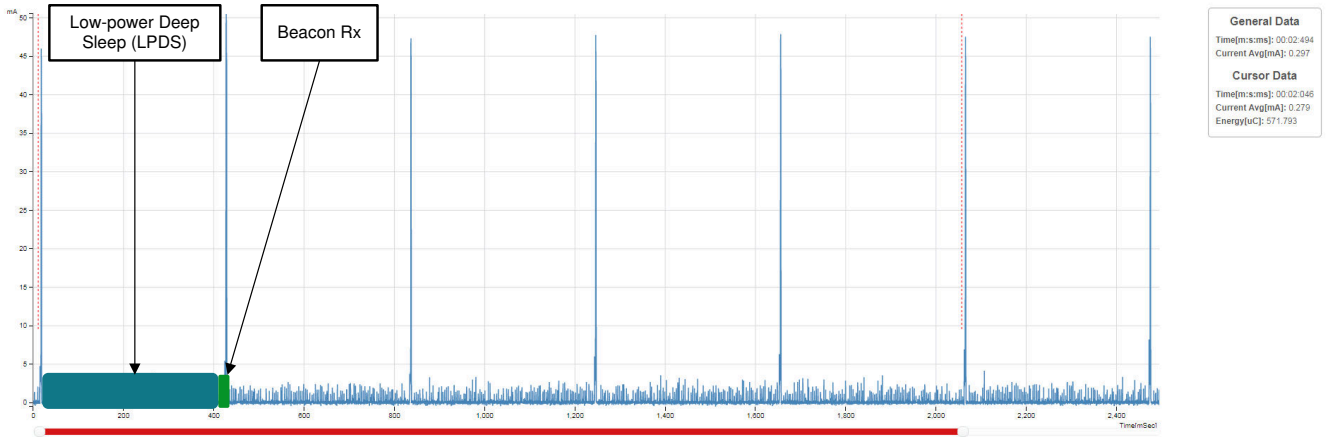

图 6-4. LSI = 500 毫秒时始终连接模式下的空闲电流

图 6-4 显示当器件处于空闲状态时，平均电流约为 279µA。按照此测量结果，我们可以通过方程式 3 来估算始终连接模式下 Wi-Fi 的平均功耗。

$$P_{always\_connected} \cong V_{idle} \times I_{idle} = 3\ V \times 279\ \mu A = 0.837\ mW\ (837\ \mu W) \quad (3)$$

将由方程式 3 得出的平均功耗与根据*智能锁参考设计* [1] 计算出的平均系统功耗相加，我们可以得出整个低功耗蓝牙和 Wi-Fi 锁系统的总体平均功耗约为 1.33mW。按照节 6.1.1.1 中的相同计算方式，我们得出本例中系统的估算电池寿命为 1.54 年（大约 1 年 6 个月）。

6.2 Wi-Fi 电子锁的安全性

由于电子锁是安全系统中的关键组件，其设计过程必须将安全性考虑在内。电子锁通过锁定未经授权的用户，同时确保可供所有授权用户使用，对资产设置访问权限。例如，电子锁可对住宅、办公楼或酒店客房等设置访问权限。

概括来讲，通过使用访问凭证和白名单来设置访问权限。如果使用机械锁，访问凭证是实体钥匙，白名单则是持有实体钥匙的一组用户。

与保护实体钥匙类似，电子锁系统必须保护 PIN 码、数字 ID、数字钥匙（访问凭证）和授权用户（白名单）的所有数据库。除了这些资产，Wi-Fi 电子锁还必须应对其他安全挑战，例如：

- 保护最终用户私有数据
- 防止恶意或无效 OTA 更新
- 保护知识产权 (IP)
- 确保仅授权器件能连接云服务

保护最终用户私有数据 - 使 Wi-Fi 电子锁由特定授权用户控制的任何数据必须保持私密状态。在通过 Wi-Fi 接口、互联网传输最终用户数据以及将数据存储在门锁上的非易失性存储器时，必须对数据进行保护。最终用户私有数据可包括进入密钥、白名单或通过特定用户帐户与门锁关联的任何其他数据。

防止恶意或无效 OTA 更新 - 这对于确保 Wi-Fi 电子锁正常工作非常重要，以便在授权用户访问时能够正常工作。如果由于攻击者更改了软件，或者由于更新至包含错误的新版本而造成电子锁被锁定，那么这个电子锁就无法使用。通过防护功能保护系统完整性，防止恶意或无效更新，从而确保电子锁在需要时正常工作。

保护 IP - 这对于保护系统知识产权 (IP) 的机密性至关重要，例如电子锁软件。保护 IP 有助于确保攻击者无法复制门锁设计，也无法以利用潜在漏洞为目的而了解系统的工作原理。

确保仅授权器件才能连接云服务 - 构建安全的系统需要的不仅仅是实行安全功能来保护电子锁。开发人员还必须增加一种机制来验证每个连接到应用服务器的电子锁的标识，从而采取措施保护其他资产，如应用服务器和云服务。

SimpleLink Wi-Fi 的设计中内置了一系列安全功能，以帮助电子锁开发人员应对这些安全挑战。图 6-5 显示了 SimpleLink Wi-Fi 中的几种信息安全机制以及它们如何应对安全挑战。节 6.2.1 至 节 6.2.7 介绍了图 6-5 中以红色文本显示的机制以及它们如何简化电子锁的设计。

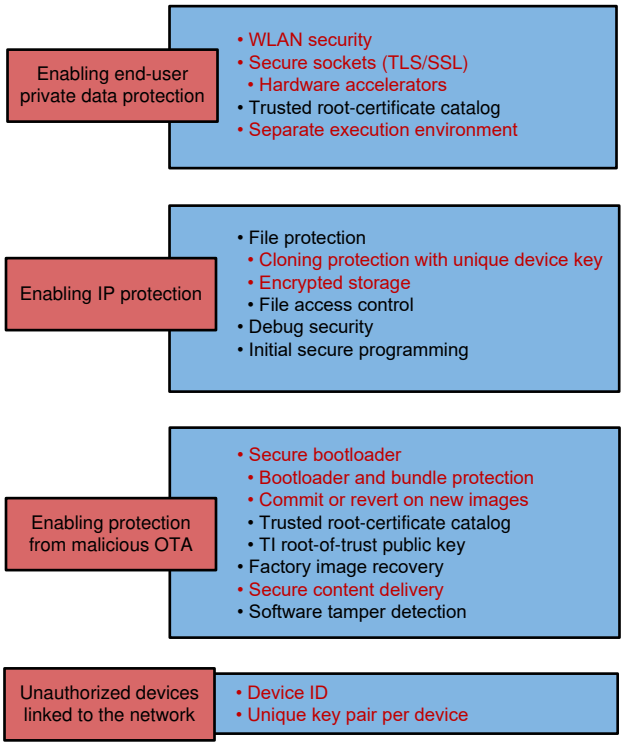

图 6-5. 电子锁安全挑战和 SimpleLink™ Wi-Fi 的信息安全机制

如需了解 SimpleLink Wi-Fi 器件系列中提供的完整安全功能集，请参阅 *SimpleLink™ CC3120、CC3220 Wi-Fi® Internet-on-a chip™ 解决方案内置安全功能应用报告*。

6.2.1 无线 LAN 和互联网安全

在电子锁的日常使用中，可以在电子锁和 AP 之间传输进入密钥、用户个人资料信息和软件等数据，然后将数据发送至远程应用服务器。为了保护局域网，系统必须使用与 AP 的安全 Wi-Fi 连接。SimpleLink Wi-Fi 支持适用于

个人和企业网络的所有常见 Wi-Fi 安全模式，包括 WEP、WPA/WPA2 PSK、WPA2 企业版 (802.1x)、WPA2 + PMF 和 WPA3。Wi-Fi 安全提供了一种机制，本地网络可以借助它对门锁进行身份验证，并对通过本地链路传输的数据进行加密。

数据是通过互联网传输的，因此必须采取措施保护器件和应用服务器之间的通信链路。保护通过互联网传输的数据的一个关键步骤是使用安全套接字 (TLS/SSL)。通过使用安全套接字，服务器和客户端都能验证标识并协商要使用的加密协议，以保护传输的数据。

NOTE

由于在传输前对数据应用了其他标头和密码，安全套接字实现的吞吐量低于 TCP 套接字的最大吞吐量。

CC3120 和 CC3220 器件支持最多六个同步安全套接字，可用的套接字共 16 个。为了提供出色保护，电子锁必须以应用服务器支持的最高安全等级传输被识别的资产。有关受支持的密码套件的完整列表，请参阅 *CC3120、CC3220 SimpleLink™ Wi-Fi® 和物联网处理器编程指南*。

6.2.2 安全存储

安全地存储节 6 中所列的所有关键资产对电子锁而言至关重要，因为这可以阻止恶意用户访问资产。安全存储有助于防范直接和间接读取非易失性内存的意图。虽然直接 (或物理) 攻击可能不易扩展，但是防止攻击者克隆电子锁系统，或防止小偷窃取失窃电子锁非易失性内存中的个人信息仍然非常重要。

SimpleLink CC3120 和 CC3220 器件使用串行闪存形式的外部非易失性内存。由网络处理器将串行闪存中存储的内容整理到文件系统中。文件系统中内置了许多功能，可用于在存储过程中保护资产，具体包括以下功能：

- 加密数据 - 使用 AES-128 保证数据的机密性。
- 检查数据完整性 - 更改文件时应用签名，打开文件进行读取时验证内容。
- 控制数据访问权限 - 使用文件令牌设置访问权限。
- 向系统发送篡改警报 - 检测无效和可能恶意的文件访问尝试。

根据应用要求，专为电子锁应用定制的文件可使用文件创建标志和文件令牌来创建，并具有不同的保护等级。但是，必须安全存储的特定系统文件必须强制创建标志。表 6-1 列出了这些文件和相关的创建标志。

表 6-1. 安全的系统文件

文件名	CC3120、CC3220S、CC3220SF	CC3220R	注释
/sys/servicepack.ucf /sys/certstore.lst	TI 安全签名 + 公共写入 + 失效防护	TI 安全签名	• 这些文件由 TI 提供。 • 服务包包含器件代码修复；受信任根证书目录包含 TI 支持的根 CA 和撤销证书列表。 • TI 可根据需要提供这些文件的新版本。 • TI 强烈建议设计主机程序，用于支持文件的后续更新。
/sys/mcuimg.bin //CC3220R/ CC3220S /sys/mcuflashimg.bin // CC3220SF	安全签名	不安全	文件包含主机程序。
/sys/cert/private.key /sys/cert/client.der /sys/cert/ca.der	安全	安全，仅供读取	文件包含 SSL 连接的密钥和证书。

6.2.3 独立执行环境

CC3220 器件架构针对应用 MCU 和网络处理器采用独立的执行环境。图 6-6 显示了 CC3220 器件架构的简图。

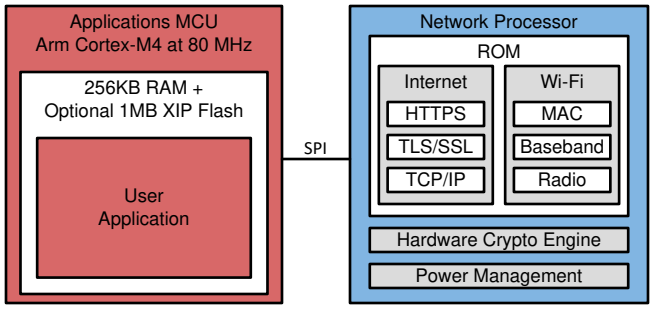

图 6-6. 独立执行环境

独立的应用和网络执行环境是有利的，因为这种隔离让网络处理器能够减轻主机 MCU 的负担。应用可以继续运行时间关键型任务，同时网络处理器可以运行网络堆栈并执行计算密集型工作，如处理加密算法。

使用独立执行环境的另一项优势是，可以降低应用暴露到通过网络接口执行的攻击中的概率。独立执行环境还有助于减少证书和私钥的暴露。只有当设置安全套接字连接时，网络处理器才需要访问证书和私钥，这意味着这些文件被存储为安全文件，仅供读取访问。主机控制器可以对文件执行写操作以更新文件，但主机控制器无法将文件读取到内存中，因为在内存中这些文件将暴露为纯文本。

6.2.4 安全内容交付

CC3120 和 CC3220 器件引入了一项被称为*安全内容交付*的功能，开发人员可利用此机制为数据传输增加额外保护，而该功能与传输层的安全性无关。安全内容交付以 SimpleLink Wi-Fi 网络处理器生成临时 ECC 密钥对的功能为基础。远程服务器可以使用器件生成的公钥来获取共享密钥，然后对内容进行加密。

因此，可以由网络处理器对内容进行解密，因为系统不会将私钥泄露给主机。当主机向安全文件执行文件写入操作时，网络处理器会执行解密。安全内容交付对于保护文件（如证书和私钥）非常有用，这些文件仅供主机进行只读访问，但随着时间的推移，可能需要通过主机写入或更新。

6.2.5 安全启动

ROM 引导加载程序内置在 SimpleLink Wi-Fi CC3220S 和 CC3220SF 器件中。ROM 引导加载程序包括验证运行时二进制（应用程序映像）的完整性和真实性的步骤。必须将映像编程为安全签名文件，因此可以提供验证步骤。

当引导加载程序运行时，它会使用开发人员提供的证书来验证开发人员应用于映像中的签名。然后，根据得到的完整信任链对证书进行验证。

NOTE

若要验证证书，必须将完整的信任链编程到外部闪存中。信任链的根 CA 必须是 SimpleLink Wi-Fi 受信任根证书目录中包含的一个根 CA。可以在 *tools/cc32xx_tools/certificate-catalog/readme.html* 内的 SDK 中找到根 CA 列表。该目录由 TI 提供，用于验证信任链是否来自已知的可信来源。

将运行时二进制作为引导加载程序的一部分进行验证，旨在为阻止执行来自未知供应商的映像提供帮助，如在出现恶意 OTA 更新时。更多有关安全启动功能的信息，请参阅 *SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ 解决方案内置安全功能*。

6.2.6 失效防护文件和捆绑包保护

若要在电子锁中使用 OTA 更新，就需要采取措施保护执行更新的系统的完整性。向系统提供不完整或无效的更新可导致系统中止工作并会无法使用。电子锁开发人员设计的系统必须能够防止更新失败，以确保锁一直正常工作。

SimpleLink Wi-Fi 在文件系统中引入了两种机制，有助于在更新过程中保护系统的完整性。这两种功能被称为*失效防护文件*和*捆绑包保护*。借助失效防护文件，开发人员能够存储更新文件的副本，并在将新副本交付到文件系统之前进行测试。所有捆绑包文件也在同一时间交付，以防止部分更新。通过将捆绑包文件置于等待交付状态，系

统可以在将新文件实际交付给文件系统使用（变为激活状态）之前，利用所有新文件重新启动应用，并运行用户定义的测试。验证 OTA 更新内容的这一额外步骤有助于确保更新完成后电子锁能够正常工作。

6.2.7 唯一设备标识

当电子锁等产品连接到云服务器时，服务器应验证设备的标识，以确保设备是有效的产品，并有权访问可用服务。如果缺乏身份验证，恶意设备就可以连接到云服务，并可能增加服务器使用率和成本。这个问题的一个解决方案是为每个门锁创建唯一的设备证书和密钥，并进行编程。然而，创建、编程和管理大量设备和唯一的文件会耗费大量时间和成本。

为了简化分配唯一设备标识的过程，每个 SimpleLink CC3120 和 CC3220 器件在量产过程中都内置了一个不可修改的 128 位码和一个唯一的 ECC 密钥对。128 位码可以作为唯一设备标识符 (UDID)，唯一 ECC 密钥对可用于对数据进行签名。可将 UDID 和唯一密钥对搭配使用，以验证每个 SimpleLink Wi-Fi 器件的标识。在电子锁设计中，此机制是有利的，因为它可以节省开发人员时间，帮助开发人员确保仅已知设备才可访问相关的云服务。

6.3 互操作性

在设计支持 Wi-Fi 的电子锁时，必须选择能够与各种 AP 进行交互的 Wi-Fi 解决方案。互操作性包括建立和维持与 AP 的连接，并提供恒定的低功耗运行，而不会影响解决方案的稳健性。

SimpleLink Wi-Fi 针对 200 多个 AP 进行了测试，以确保解决方案的质量，从而支持在全球多个地区部署设计。德州仪器 (TI)™ 的 CC3120 和 CC3220 器件和模块还获得了 Wi-Fi 联盟认证。

SimpleLink Wi-Fi 解决方案提供的高水平互操作性可确保电池供电的电子锁在各种部署场景（包括各种住宅与建筑）下具有一致的性能。如需详细了解 SimpleLink CC3220 器件的 WLAN 无线电性能，请参阅 *CC3220 SimpleLink™ Wi-Fi® 无线和物联网解决方案 - 单芯片无线 MCU*。

7 总结

具有无线连接功能的电子锁简化了商业楼宇和家庭的门禁控制。与电子锁的其他射频技术相比，Wi-Fi 连接通过提供直接的门锁远程监控方法，实现了一些关键优势。Wi-Fi 还可自动提供软件更新并加快更新过程，从而改善用户体验。

借助 SimpleLink Wi-Fi CC3120 网络处理器和 CC3220 无线 MCU，能够将 Wi-Fi 连接直接集成到电子锁设计中，而不会影响电池寿命。SimpleLink Wi-Fi 还提供了稳健的电子锁设计所需的关键安全功能和高级互操作性。

8 参考资料和相关文档

TI.com 上的产品页面

[1] 使用 4 芯 AA 电池并可实现 5 年以上电池使用寿命的智能锁参考设计

[2] 适用于 MCU 应用的 CC3120 SimpleLink™ Wi-Fi® 网络处理器、物联网解决方案

[3] SimpleLink™ Wi-Fi® 和物联网单芯片无线 MCU 解决方案（CC3220R、CC3220S 和 CC3220SF）

[4] SimpleLink™ Wi-Fi® CC3220S 无线微控制器 LaunchPad™ 开发套件或 SimpleLink™ Wi-Fi® CC3220SF 无线微控制器 LaunchPad™ 开发套件

[5] SimpleLink™ Wi-Fi® CC3120 无线网络处理器 BoosterPack™ 插件模块 + SimpleLink™ MSP432P401R LaunchPad™ 开发套件

[6] SimpleLink™ Wi-Fi® CC3220 软件开发套件 (SDK)

[7] SimpleLink™ MSP432™ 软件开发套件 (SDK)

[8] DRV8833 2A 低压双路有刷直流或单路双极步进电机驱动器（PWM 控制器）

[9] DRV8833C 1A 低压步进电机或单路/双路有刷直流电机驱动器（PWM 控制器）

[10] DRV8837 1.8A 低压有刷直流电机驱动器（PWM 控制器）

[11] DRV8837C 1A 低压 H 桥驱动器

博客

[12] 德州仪器 (TI)，*智能 Wi-Fi® 锁很快将走进千家万户*

用户指南

[13] 德州仪器 (TI)，*IP 智能门锁：降低功耗并为 SimpleLink™ Wi-Fi® 云连接增加安全功能*

[14] 德州仪器 (TI)，*CC3120、CC3220 SimpleLink™ Wi-Fi® 和物联网处理器编程指南*

应用报告

[15] 德州仪器 (TI)，*SimpleLink™ CC3120、CC3220 Wi-Fi® Internet-on-a chip™ 解决方案内置安全功能*

[16] 德州仪器 (TI)，*SimpleLink™ CC3120、CC3220 Wi-Fi® Internet-on-a chip™ 网络子系统电源管理*

9 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision * (December 2017) to Revision A (September 2020)	Page
• 更新了整个文档中的表格、图和交叉参考的编号格式	2
• 在 节 6.2.1 *无线 LAN 和互联网安全* 中增加了 WPA2 + PMF 和 WPA3	10

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265