用于耗材、配件和互联对象的安全认证配套器件

SO8N 4 × 5 mm

UFDFPN8
2 × 3 mm

产品状态
STSAFE-A120

特性

- 唯一 ID 码
- 身份验证目标：
  - 耗材及配件的防克隆
  - 互联对象安全连接及预附加到云（Azure、AWS 等）
  - 无线充电器 Qi 1.3 和 Qi 2.0
  - Matter 设备
  - 数字电源 OCP M-CRPS
- 与主机应用处理器配对和建立安全信道
- 可配置的安全存储
- 使用安全计数器进行使用情况监控
- 与远程主机建立安全连接，包括传输层安全（TLS 1.2 和 TLS 1.3）握手
- 签名验证服务（安全启动和固件升级）
- 基于本地主机信封的封装和解封，安全存储在主机非易失性存储器中
- 数据哈希
- 对称数据加密或解密
- 片上密钥对生成

加密和安全功能

- 高级非对称加密
  - 5 个椭圆曲线加密 (ECC) 非易失性私钥 Slot + 1 个临时 ECC 密钥 Slot
  - 支持的椭圆曲线：
    - NIST P-256 P-384, P-521
    - Brainpool P-256 P-384, P-512
    - Edwards 25519
    - Curve25519
- 支持的功能：
  - 生成数字签名并进行验证（ECDSA 和 EdDSA）
  - 建立 Diffie-Hellman 共享机密 (ECDH)
- 高级对称加密
  - 16 个支持 AES-128/256 CCM*、ECB、GCM、CMAC 和 HKDF 的对称密码 Slot
- 与主机应用处理器配对
  - AES 128 位或 256 位
- 本地封装/解封信封密钥
  - 2 个采用 AES 128 位或 AES 256 位的密钥的 Slot
- 数据哈希
  - SHA-2，包含 SHA-256、SHA-384 和 SHA-512
  - SHA-3，包含 SHA3-256、SHA3-384 和 SHA3-512

- 随机数发生器
  - 具有符合 NIST SP 800-90B 的熵源的随机数发生器
- 最新一代高度安全 MCU
  - 每块晶片上标有唯一序列号
  - 经过 CC EAL5+ AVA_VAN.5 和 ALC_DVS.2 通用标准认证
  - 主动屏蔽
  - 监控环境参数
  - 故障注入保护机制
  - 侧信道攻击保护

硬件特性

- 16 KB 可配置非易失性存储器
  - 25 °C 下数据保存时间长达 25 年
  - 25 °C 下擦除/写次数多达 500000 次
- 连续电源电压为 2.7 V 到 5.5 V
- 工作温度：-40 °C 至 +105 °C

通信协议

- I²C 总线从接口
  - 高达 400 kbps 的传输速度（快速模式）
  - 7 位寻址

封装

- 符合 ECOPACK 的 SO8N 8 引脚塑料小尺寸封装和 UFDFPN 8 引脚超薄紧密排列双扁平封装。

1 产品描述

STSAFE-A120 是一款安全芯片，可为本地或远程主机提供身份验证和安全数据管理服务，还提供哈希、加密和解密等服务。它包含一个完整的一站式解决方案，其中的安全操作系统运行于最新一代安全微控制器上。

STSAFE-A120 可以集成在耗材、配件、物联网设备、智能家居、智慧城市和工业应用以及消费电子产品中。

LICENSED DPA COUNTERMEASURES™

1.1 密钥函数概述

图 1. 远程服务器（互联设备）身份验证

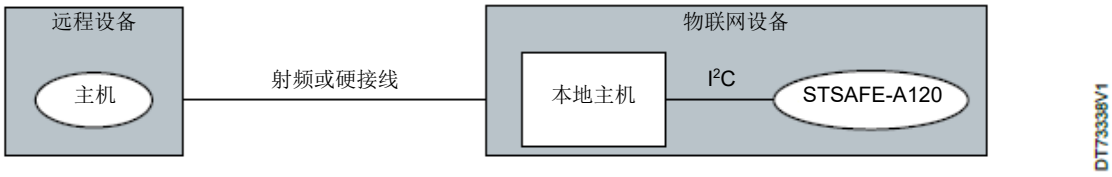
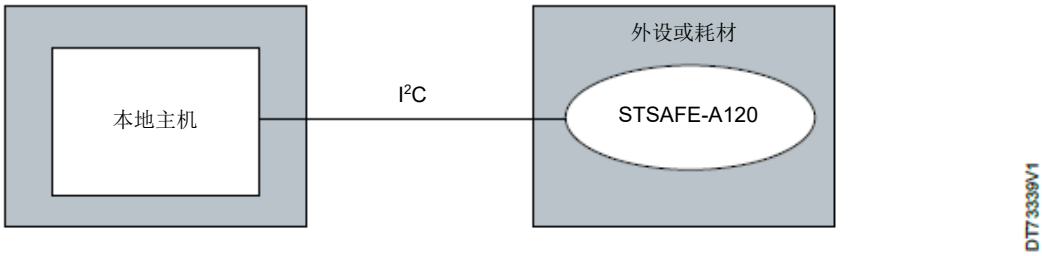


图 2. 本地主机（耗材或外设）身份验证



STSAFE-A120 可安装在以下位置：

- 对远程主机进行身份验证的设备（物联网设备），本地主机用作远程服务器的通道。
- 对本地主机进行身份验证的外设，例如游戏、移动配件或耗材。

STSAFE-A120 安全芯片支持以下功能：

- **身份验证**

  STSAFE-A120 身份验证服务可向远程或本地主机证明某个外设或物联网是合法的。因此，设备制造商可以确保只有身份可信的外设（如配件或耗材）才能与原始设备配合使用。同样，服务提供商也可以确保其服务只与适当的物联网设备一起运行。

  身份验证服务采用 ECC 加密方案，包括 NIST P-256-bit、P-384-bit、P-521-bit 曲线、brainpool P-256-bit、P-384-bit、P-512-bit 和 curve25519。它还符合 CSA Matter、WPC 和 OCP M-CRPS 等要求进行对象身份验证的各种标准。

- **安全存储**

  STSAFE-A120 配备 16 KB 非易失性存储器，分为多个区域，其读写访问权限可配置为自由访问、本地主机访问或远程主机访问。

- **安全单向计数器（外设生命周期和使用监测）**

  STSAFE-A120 提供可配置的单向计数器，可监测一次性配件或耗材。用户 NVM 中可用计数器的数量取决于 STSAFE- A120 个性化设置。

- **与主机配对并建立安全信道**

  STSAFE-A120 允许与本地主机建立基于 AES 密钥的安全信道，用于命令授权、命令数据加密、响应数据加密和响应身份验证。通常情况下，STSAFE-A120 与本地主机配对可防止在其他设备中使用 STSAFE-A120，并保护 I²C 线路不被窃听敏感信息。

- **本地主机信封的封装和解封**

  STSAFE-A120 可使用其两个本地信封密钥之一对数据进行加密或解密。通常，当本地主机需要在其非安全数据存储区内存储连接密钥和凭证等机密时，就可以使用它。

- **安全信道密钥建立 (TLS)**

  STSAFE-A120 可协助本地主机在设备和远程主机（如云服务器或网关）之间建立安全连接。它协助本地主机建立会话密钥，用于加密和解密设备与远程主机之间的数据交换。该密钥建立服务依赖于基于椭圆曲线 Diffie-Hellman（ECDH 和 ECDHE）方案的共享机密计算，在设备生成并与服务器交换 ECC NIST、brainpool 或 X25519 公钥之后执行。

- **实体身份验证**

  通过公钥 Slot，STSAFE-A120 可以验证本地或远程主机。STSAFE-A120 验证成功后，本地或远程主机就可以访问某些授权命令或内存分区。

- **签名验证**

  STSAFE-A120 可以使用本地主机提供的公钥验证椭圆曲线数字签名算法 (ECDSA) 签名。这种机制可以减轻没有加密计算能力或计算能力有限的本地主机应用处理器的负担。它通常用于验证安全启动或安全固件更新时的固件签名。

- **对称密钥**

  STSAFE-A120 最多可装载 16 个对称密钥，用于数据加密和解密。

- **数据哈希**

  STSAFE-A120 允许使用 SHA-2（SHA-256、SHA-384、SHA-512）和 SHA-3（SHA3-256、SHA3-384、SHA3-512）算法进行数据散列。

1.2 STSAFE-A120 环境

STSAFE-A120 随附的主机集成代码已通过意法半导体 (ST) STM32 通用 MCU 的测试。它还可以移植到各种通用微控制器或微处理器上。该集成代码包括一个命令封装器和最常见的通用用例的示例。

STSAFE-A120 提供预先配置的通用数据配置文件，用于评估、原型设计或生产。

意法半导体还提供并推荐安全配置服务，以便在安全的认证环境中生成密钥和存储客户叶证书。

STSAFE-A120 随附意法半导体 CA 证书，可对每个 STSAFE-A120 设备中的叶证书进行真实性验证。

2 产品用例

本节说明 STSAFE-A120 设备使用非对称加密技术的多种用途。

2.1 身份验证

该场景说明了一个命令流，其中 STSAFE-A120 安装在设备上，该设备可对远程主机（物联网设备）进行身份验证，本地主机用作远程服务器的通道。

将 STSAFE-A120 安装在对本地主机进行身份验证的外设（如游戏、移动配件或耗材）上的情况完全相同。

指令流

1. 获取主机设备中 STSAFE-A120 芯片的公钥：
   - *命令 1* 用于从 STSAFE-A120 芯片的数据分区读取 X509 公钥证书。
   - 主机设备用 CA 公钥验证 X509 公钥证书（主机负责获取该公钥的副本）。验证过程成功后，主机设备就会获得 STSAFE-A120 公钥的真实副本，并在以后用于验证签名。
2. 主机设备会生成一个质询，并将其存储起来，供以后验证签名时使用。然后，主机设备计算出该质询的哈希值，并通过 *command 2* 发送给 STSAFE-A120，以获取 STSAFE-A120 芯片用私钥计算出的签名。主机设备使用 STSAFE-A120 公钥（在本场景第一步中获得）验证签名。如果签名有效，主机就知道外设或物联网设备是真实的。

图 3. 物联网设备身份验证示例

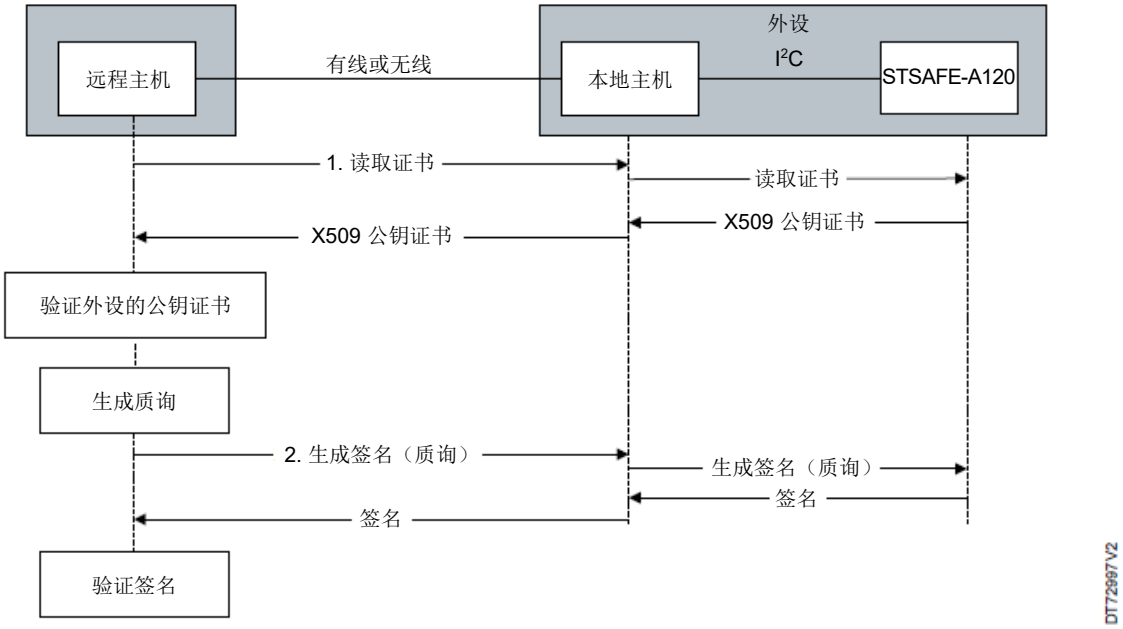
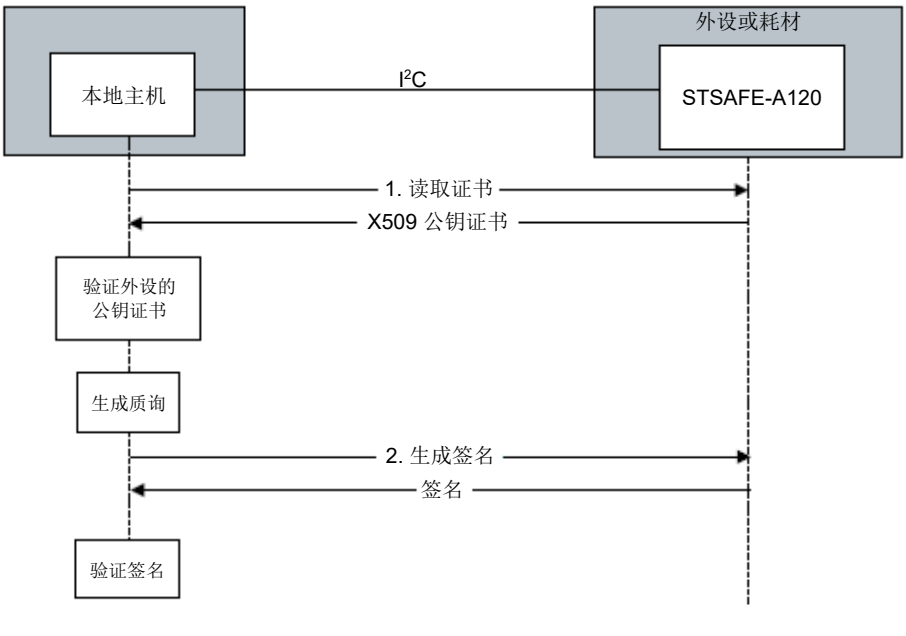


图 4. 外围设备身份验证示例



2.2 应用数据存储

STSAFE-A120 配有 16 KB 非易失性存储器，客户可对其进行配置以存储应用数据。这 16 KB 必须划分为具有适当访问权限的分区。

其中一些分区可配置为安全单向计数器（递减）分区，并提供相关数据空间。

还可为每个分区配置存储区的访问条件。访问条件可以是：

- 自由访问
- 主机安全信道访问
- 实体身份验证访问
- 主机安全信道和实体验证访问。

2.3 本地信封封装/解封

STSAFE-A120 提供数据封装服务（对数据进行加密和签名），并将其装入安全信封。该服务旨在由主机将敏感信息存储在不受保护的内存中。STSAFE-A120 可以随时拆开这个信封（解密和验证）。

图 5. 封装/解封密钥的一般原理

封装是用来保护密文或明文（如连接密钥或凭证）的机制。封装的输出是一个信封。

信封由要保护的密文或明文组成，用 AES 密钥封装算法加密。对于本地信封，该算法使用本地信封密钥。信封中还包含加密密钥或明文的 MAC，用于验证信封的真伪。

解封是用于解密信封并恢复密文或明文的机制。

可以在 WRAP LOCAL ENVELOPE 命令的命令数据中向 STSAFE-A120 发送密文或明文。在响应中，STSAFE-A120 会返回一个信封，其中包含加密密文或纯文本以及 MAC。这种信封被称为本地信封。

本地主机可以使用 UNWRAP LOCAL ENVELOPE 命令检索临时密文或明文。封装和解封过程使用本地信封密钥 Slot 中的一个密钥和 AES 密钥封装算法。

本地信封密钥 Slot

STSAFE-A120 支持两个本地信封密钥 Slot。

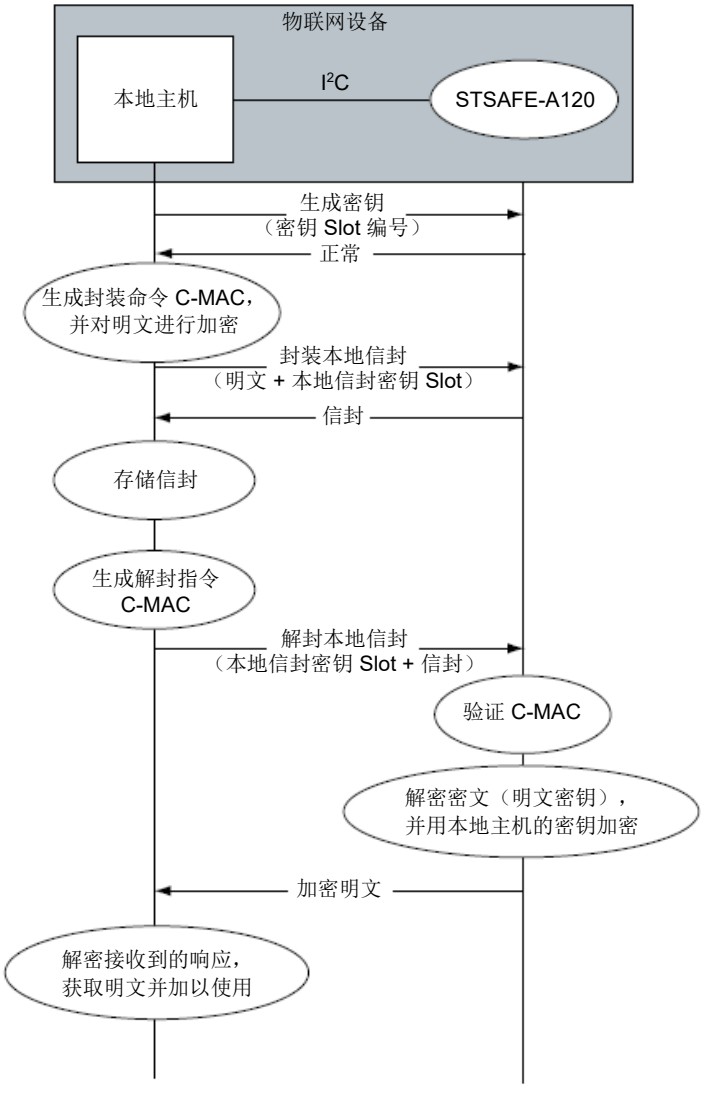
每个 Slot 可存储一个 AES-128 位或 AES-256 位密钥，用于本地信封的封装和解封。

本地信封密钥由 STSAFE-A120 通过 GENERATE KEY 命令随机生成，并且永远不会离开 STSAFE-A120。

指令流

1. 生成本地封套密钥：
   - 本地主机查询 STSAFE-A120，以便使用 GENERATE KEY 命令在两个 Slot 中的一个随机生成本地信封密钥。
2. 封装本地信封：
   - 本地主机使用 STSAFE-A120 封装本地信封命令建立本地信封。
   - 该命令需要本地主机的 C-MAC、明文数据（通常是需要用主机密钥加密的密钥）和本地信封密钥 Slot 编号（用于加密明文数据的密钥）。
   - *wrap local envelope* 命令的响应包含信封（使用 *local envelope* 密钥对明文进行加密）。
3. 接收方解封本地信封：
   - 本地主机通过 *unwrap local envelop* 命令和本地信封密钥 Slot 向 STSAFE-A120 提供本地信封。
   - 主机必须使用该命令生成本地主机的 C-MAC。
   - STSAFE-A120 在其响应中提供用本地信封密钥解密的信封密文（通常是密钥）。
   - 响应使用主机的密钥进行加密。
   - 主机使用主机的密钥对响应进行解密，并获得解密后的信封密文。

图 6. 封装/解封本地信封命令流



2.4 为安全连接 (TLS) 建立密钥

本用例展示了如何在本地主机和远程主机中生成相同的共享机密，而无需交换。其原理是在双方生成两个 ECC 临时密钥对。然后，在交换这两个密钥对的公钥后，本地主机和远程主机运行 ECDH 方案来计算共享机密。

本用例的目标是使用椭圆曲线 Diffie-Hellman (ECDH) 方案和 STSAFE-A120 中的静态密钥在本地主机和远程服务器之间共享机密。STSAFE-A120 还支持使用临时密钥的 ECDHE，此处未对其进行说明。

共享机密应进一步派生出一个或多个会话密钥，此处未对其进行说明。会话密钥可用于 TLS 等通信协议，以保证本地主机和远程服务器之间交换数据的机密性、完整性和真实性。以下是一些数据示例：

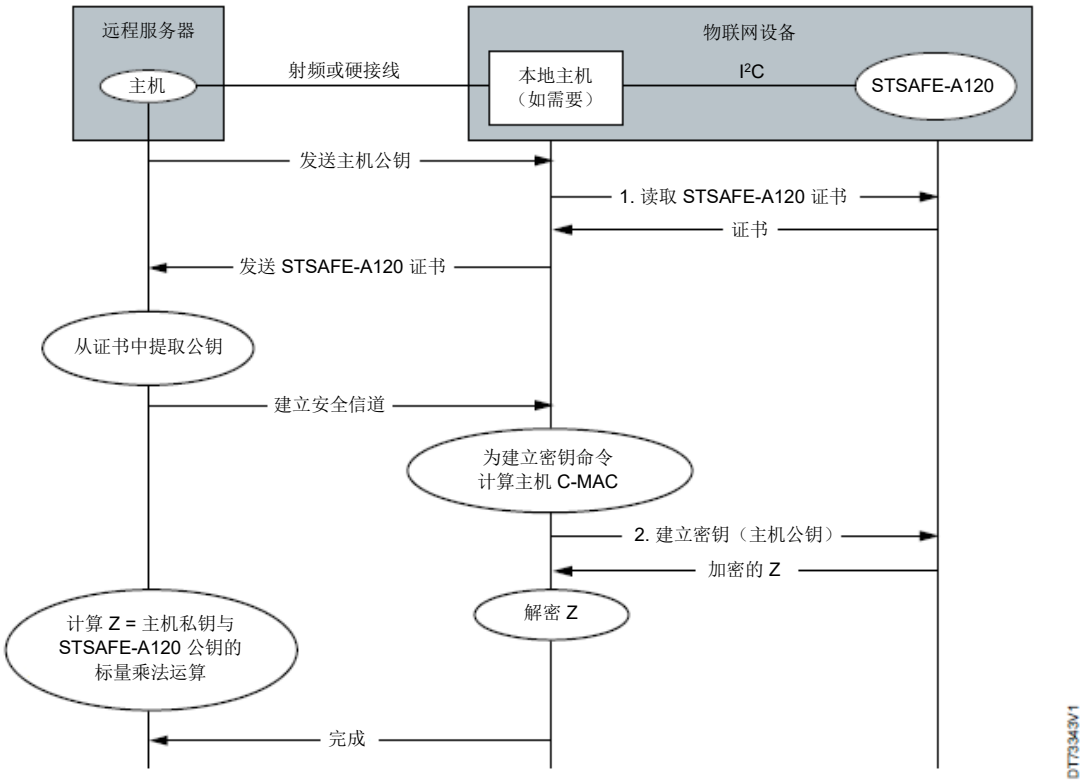
- 从本地主机到远程服务器：智能电表的耗电量、火灾传感器的警报或健康传感器的血压数据。
- 从远程服务器到本地主机：启动电动汽车电池充电，启动空调或热水器等家用电器，或向物联网设备推送固件升级。

根据个性化配置文件的不同，*建立密钥*命令需要进行 MAC 加密，其回答也需要加密，以避免窃听共享机密。该场景假定本地主机已按第 3 节：与本地主机配对所述设置了主机 C-MAC 和密钥。还假定本地主机知道主机 C-MAC 序列计数器；如果不知道，可向 STSAFE-A120 发送*查询*命令。

指令流

1. 远程主机服务器向本地主机发送证书。本地主机提取公钥，并可选择验证证书的有效性。本地主机在响应中发送 STSAFE-A120 证书。
2. 远程服务器使用 CA 公钥验证 STSAFE-A120 X.509 公钥证书（主机负责获取该公钥）。验证成功后，远程服务器就拥有了 STSAFE-A120 公钥的真实副本。
3. 然后，远程服务器将主机私钥与 STSAFE-A120 公钥进行标量相乘，计算出共享机密 (Z)。
4. 远程服务器请求本地主机建立安全连接。
5. 本地主机为*建立密钥*命令计算主机的 C-MAC。
6. 本地主机向 STSAFE-A120 发送一条*建立密钥*命令，提供远程主机的公钥和先前计算出的主机 C-MAC 附加密钥。STSAFE-A120 执行与远程主机服务器相同的操作，将其私钥与远程服务器的公钥进行标量乘法运算，计算出共享机密 (Z)。然后，它会使用主机的密钥对响应进行加密。
7. 本地主机读取 STSAFE-A120 应答，并用本地存储的主机密钥解密共享机密 (Z)。
8. 远程主机服务器和本地主机有一个共享机密 Z。

图 7. 密钥建立命令流



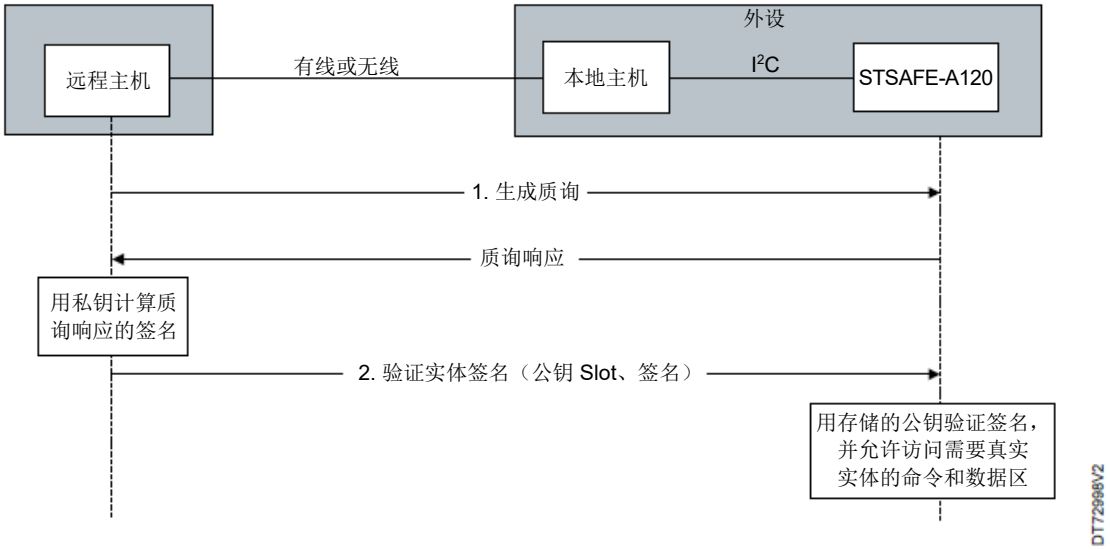
2.5 实体身份验证

STSAFE-A120 设备可通过使用私钥验证由片外实体生成的数字签名来验证该实体。这是在 STSAFE-A120 之前生成的质询响应上完成的。

实体通过身份验证后，STSAFE-A120 将允许实体访问特定命令和数据分区，这些命令和数据分区需要真实的实体状态。

该功能要求 STSAFE-A120 包含一个真实的公钥副本，该副本与片外实体签名生成过程中使用的私钥相对应。

图 8. 实体身份验证示例



2.6 公钥签名验证

STSAFE-A120 为不支持 ECC 的主机设备提供签名验证服务。这些服务可用于使物联网设备验证远程服务器的真实性，或者在安全启动时或进行固件更新时验证本地主机固件的真实性。

*验证签名*命令使用 ECDSA 或 EdDSA，其曲线定义如下：

- 与 ECDSA、EdDSA 和 ECDH 一起使用的曲线：
  - NIST P-256 P-384, P-521
  - Brainpool P-256 P-384, P-521
  - Edwards 25519
  - Curve25519

EdDSA 的签名验证是按照 RFC8032 的定义实现的。主机必须在命令数据中说明是必须使用纯 Ed25519 变体进行验证，在这种情况下，主机必须在命令数据中提供报文，还是使用预先散列的 Ed25519 变体，在这种情况下，主机必须自行计算报文的哈希值，并在命令数据中提供哈希值。

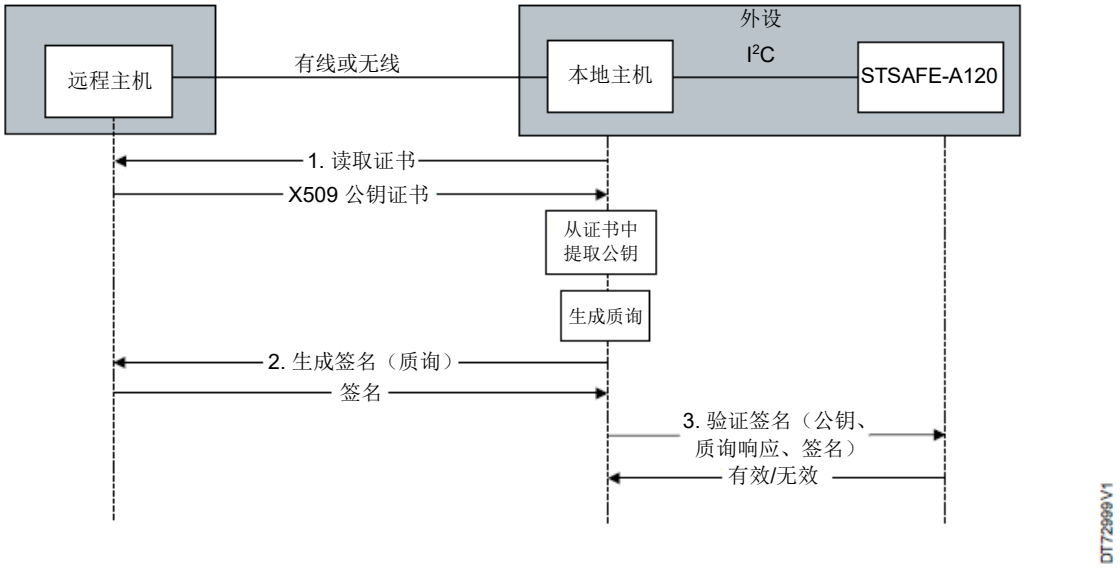
主机必须始终在命令数据中提供公钥和哈希值，除非是纯 Ed25519 签名验证，在这种情况下必须在命令数据中提供报文本身（而不是哈希值）。

*验证签名*命令的一个用例如下图所示：本地主机使用 STSAFE-A120 验证远程主机。

指令流

1. 本地主机要求远程主机提供公钥证书，远程主机做出回应。
2. 本地主机提取公钥，生成质询（随机数），并要求远程主机签署该挑战。远程主机在回应中加入签名。
3. STSAFE-A120 使用提取的公钥验证挑战的签名，并回复“有效”或“无效”。

图 9. 公钥签名验证命令流



2.7 使用对称密钥表中的密钥进行对称签名、验证、加密和解密

STSAFE-A120 提供 16 个 Slot，用于存储 AES 密钥（AES-A128 或 AES-256）。这 16 个 Slot 被称为对称密钥表。每个密钥都可以独立配置，以支持以下操作模式之一：

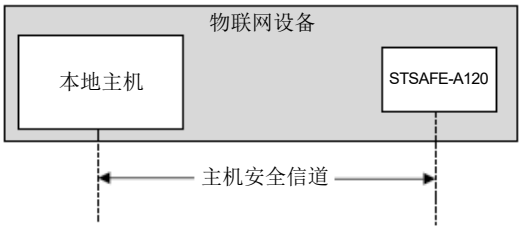
- 加密和解密
  - CCM*/CTR 模式下的 AES
  - CBC 模式下的 AES
  - ECB 模式下的 AES
  - GCM/GMAC 模式下的 AES
- 密钥派生功能 (KDF)
  - 基于 SHA2 或 SHA3 哈希函数使用 HMAC 派生的 HKDF 密钥
- MAC 计算：
  - AES 与 CMAC 结合使用
  - 基于 SHA2 或 SHA3 哈希函数的 HMAC 计算

必须使用 WRITE_SYMMETRIC_KEY 或 CONFIRM_SYMMETRIC_KEYS 命令写入密钥的操作模式。一个密钥一次只能支持一种操作模式。

3 与本地主机配对

为了保护和验证 STSAFE-A120 与本地主机之间的数据交换，使用对称加密技术建立了一个安全信道协议，即主机安全信道。

图 10. 主机安全信道



主机安全信道协议构成配对。它基于一套四个机制，使用两个对称密钥，即所谓的主机密钥。主机 MAC 密钥用于计算和验证命令 (C-MAC) 和相应响应 (R-MAC) 的消息验证码 (MAC)。主机加密密钥用于加密命令和解密各自的响应，以避免窃听。

主机 MAC 密钥和主机密钥必须在主机和 STSAFE-A120 之间共享。

STSAFE-A120 支持 AES-128 或 AES-256 密钥，主机密钥存储使用增量式 32 位 C-MAC 序列计数器（V2 Slot 类型）。

C-MAC 序列计数器决定了主机密钥的使用限制。

C-MAC 操作次数限制为 2^{32}- 1 次。之后，需要 C-MAC 的命令将失效。该计数器没有复位机制。

当 STSAFE-A120 收到无效的主机 C-MAC 时，它会递增一个称为主机 C- MAC 批准计数器的批准计数器。当计数器达到 50 时，STSAFE-A120 将拒绝使用主机 MAC 密钥。因此，需要主机 C-MAC 的命令会被拒绝。当 STSAFE-A120 收到有效的主机 C-MAC 时，在主机 MAC 密钥被阻止之前，它会将主机 C-MAC 批准计数器重置为 0。

主机密钥可以通过以下两种方式之一配置：

- 明文：主机在命令中以明文形式发送密钥
- 封装：密钥在发送时会封装一个工作 KEK（key 加密密钥），这是一个一次性使用的密钥，由 ECDHE 过程建立的易失性基础 KEK 派生。

配置明文主机密钥的命令流

本用例假设 Slot 为空。

1. 本地主机要求 STSAFE-A120 生成 128 位随机密钥，作为主机 C-MAC 密钥使用。
2. 本地主机要求 STSAFE-A120 生成 128 位随机密钥作为主机密钥。
3. 本地主机为“主机密钥 Slot”属性发送 PUT ATTRIBUTE 命令，同时发送两个生成的密钥（形成 256 位有效负载）。
4. STSAFE-A120 将密钥存储到各自的 Slot 中，并返回成功响应。
5. 本地主机将主机 C-MAC 和密钥存储在安全区域。

图 11. 提供明文主机密钥的主机安全信道设置案例

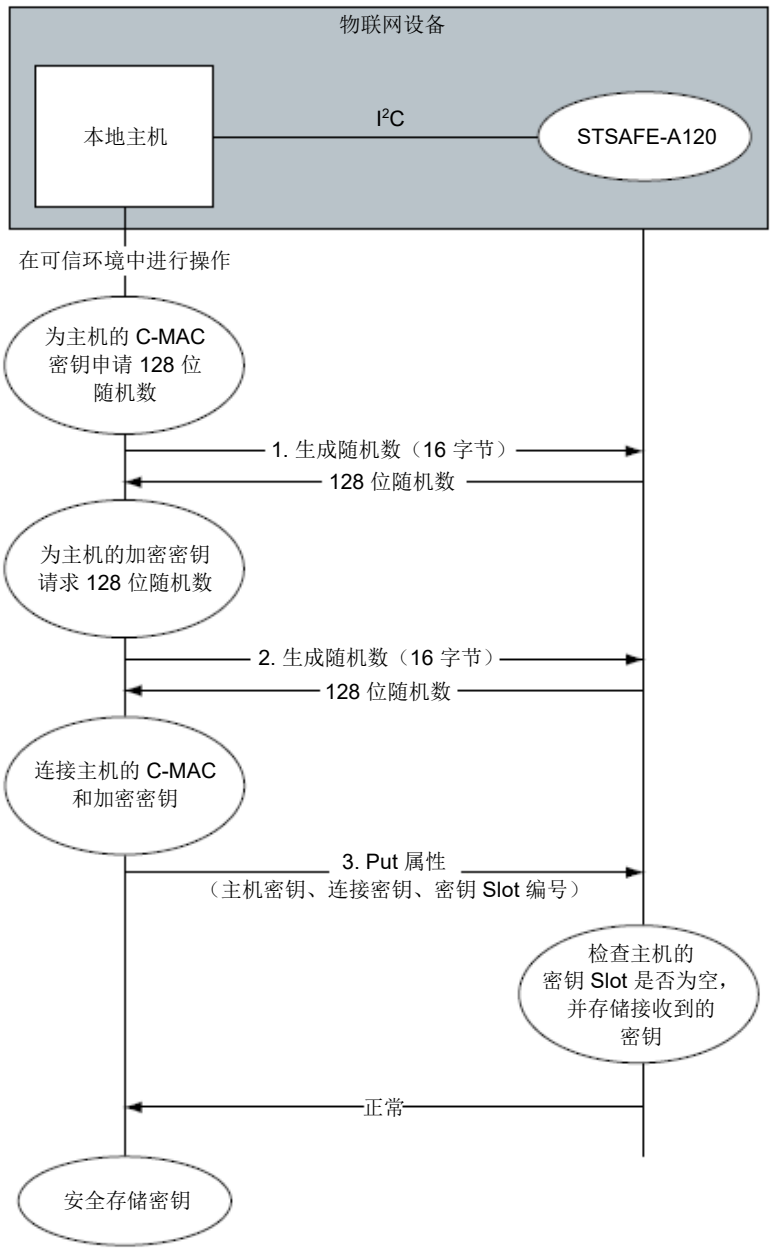
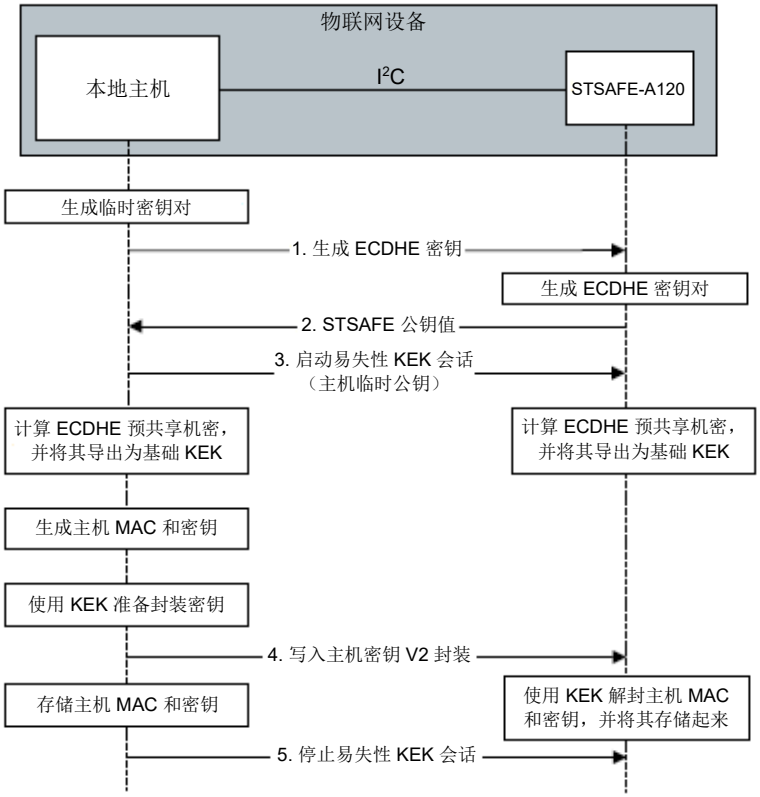


图 12. 封装主机密钥的主机安全信道设置案例



4 命令集

4.1 通用命令

Echo

将接收到的命令数据作为响应返回。

复位

中断任何正在进行的会话。

Put 属性

用于为 STSAFE-A120 添加属性，如低功耗模式和 I²C 参数。

4.2 随机生成

生成随机数

返回请求的随机字节数。

生成质询

返回一个随机字节字符串，该字符串可由片外实体签名，以获得 STSAFE-A120 的验证（即实体验证）。

4.3 数据散列命令

开始散列

开始对报文进行哈希计算。

处理散列

继续散列计算。

完成散列

结束散列计算并返回摘要。

4.4 私钥和公钥命令

写入公钥

在通用公钥表中写入公钥。每个 Slot 只能写入一次。

生成签名

根据所选私钥 Slot 中的曲线，用 ECDSA 或 EdDSA 签名对远程主机质询或数据散列进行签名。

验证签名

用于报文验证。它用提供的公钥验证远程主机的报文签名。

生成密钥对

生成一对密钥。

建立密钥

它用于使用 ECHE 协议与特定远程主机建立共享机密（符合 TLS 1.3 标准）。

开始签名会话

启动非对称签名会话。它通知 STSAFE-A120，必须启动对命令或响应序列的签名计算。

获取签名

返回自最近一次开始签名会话以来的命令或响应序列签名。

验证实体签名

通过**生成质询**命令，验证片外实体对 STSAFE-A120 先前生成的质询响应所生成的签名。

解压缩公钥

支持解压缩以压缩形式提供的 NIST 或 brainpool 公钥及其 X 坐标。它返回公钥的 Y 坐标。

4.5 本地信封命令

生成本地信封密钥

生成本地信封密钥。

封装本地信封

该命令用于使用 AES 密钥封装算法将数据与本地密钥信封进行封装。

解封本地信封

该命令用于使用本地信封密钥解封本地信封。

4.6 数据分区命令

递减

使计数区中的单向计数器递减。当计数器为零时，命令被拒绝。

读取

从数据分区读取数据。它从分区内指定的偏移量开始读取数据，并读取所要求的长度。它会检查访问条件（例如 MAC），并只返回从指定偏移量开始直到区域边界的数据。

此命令还可用于将分区的读取访问条件改为更严格的值。

更新

更新分区中的数据。它会检查写入的数据是否会超出区域边界，如果会，则不执行操作。它还会检查访问条件是否满足（例如 MAC），如果不满足，则不执行操作。

此命令还可用于将区域的更新访问条件更改为更严格的值。

4.7 对称密钥表命令

写入对称密钥明文

支持在对称密钥表中为明文格式的密钥设置 Slot

写入封装的对称密钥

支持在对称密钥表中为封装密钥配置 Slot。

建立对称密钥

支持使用 ECDHE 协议在对称密钥表中配置新密钥。

确认对称密钥

支持在对称密钥表中与

建立对称密钥命令结合使用，以配置和确认新密钥。

派生密钥

支持从对称密钥表中的输入密钥或作为命令数据的一部分传递的输入密钥派生一个或多个输出密钥。

擦除对称密钥 Slot

删除对称密钥表中指定密钥 Slot 的内容。当使用**派生密钥**命令配置 Slot，且密钥 Slot 未锁定时，需要执行此操作。

加密

使用对称密钥表中的一个 AES 密钥加密数据。

解密

使用对称密钥表中的一个 AES 密钥解密数据。

生成 MAC

用对称密钥表中的一个 AES 密钥签署数据。

验证 MAC

用对称密钥表中的一个 AES 密钥验证数据。

开始加密

使用对称密钥表中的一个 AES 密钥对长数据报文进行分块加密。它必须与**处理加密**和**完成加密**命令结合使用。

处理加密

继续加密过程。它可以连续多次使用，用对称密钥表中的一个 AES 密钥加密多个数据块。它必须与**开始加密**和**完成加密**命令结合使用。

完成加密

使用对称密钥表中的一个 AES 密钥结束多个数据块的长报文的加密过程。它必须与**开始加密**和**处理加密**命令结合使用。

开始解密

使用对称密钥表中的一个 AES 密钥对多个数据块的长报文进行解密。它必须与**处理解密**和**完成解密**命令结合使用。

处理解密

继续解密过程。它可以连续多次使用，用对称密钥表中的一个 AES 密钥解密多个数据块。它必须与**开始解密**和**完成解密**命令结合使用。

完成解密

使用对称密钥表中的一个 AES 密钥结束多个数据块的长报文的解密过程。它必须与**开始解密**和**处理解密**命令结合使用。

5 待机模式

STSAFE-A120 支持具有专用属性的待机模式。可以使用 PUT_ATTRIBUTE[LOW POWER MODE] 命令将该属性设置为无或待机。

当 STSAFE-A120 处于待机模式时 ($I_{CC-STDBY}$)，它对传入的 I²C 启动条件不做应答，直到 $t_{WAKE-STDBY}$。

图 13. STSAFE-A120 从待机状态唤醒

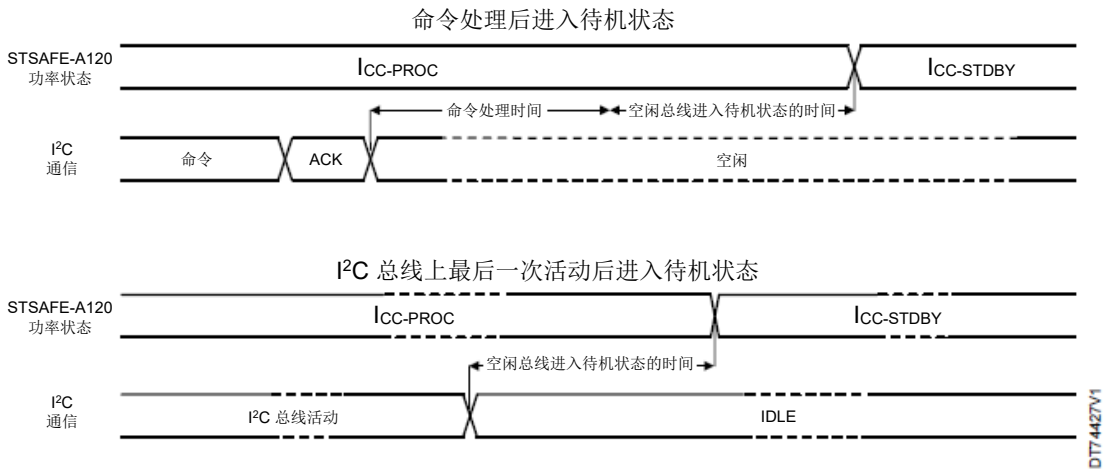
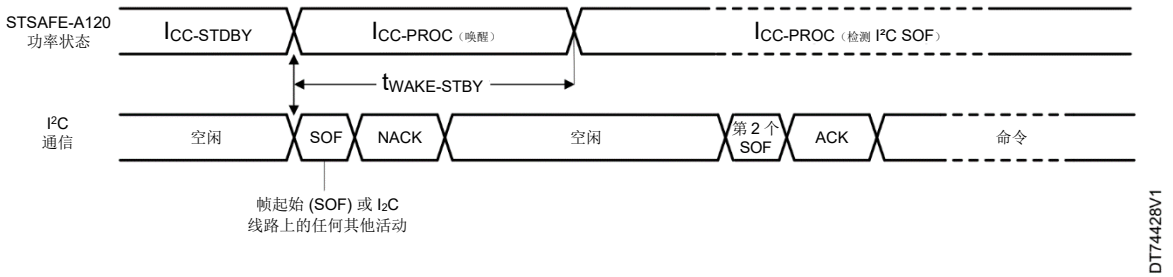


表 1. STSAFE-A120 待机唤醒时间

名称	说明	最小值	典型值	最大值	单位
$t_{WAKE-STDBY}$	待机唤醒时间	-	60	-	µs

如果启用低功耗模式，STSAFE-A120 会在 IDLE BUS TIME TO STANDBY 毫秒后自动进入待机模式，具体方案如图 14 所示。

图 14. STSAFE-A120 进入待机模式



来自主机的查询时间应大于 $t_{WAKE-STDBY}$ 并小于 IDLE BUS TIME TO STANDBY，以避免死循环。

IDLE BUS TIME TO STANDBY 可以调整，从 50 ms 开始，以 50 ms 为步长，最高可达 1600 ms。

为了优化功耗，当与其他 I²C 设备共享总线时，不建议禁用待机模式。

6 电气集成

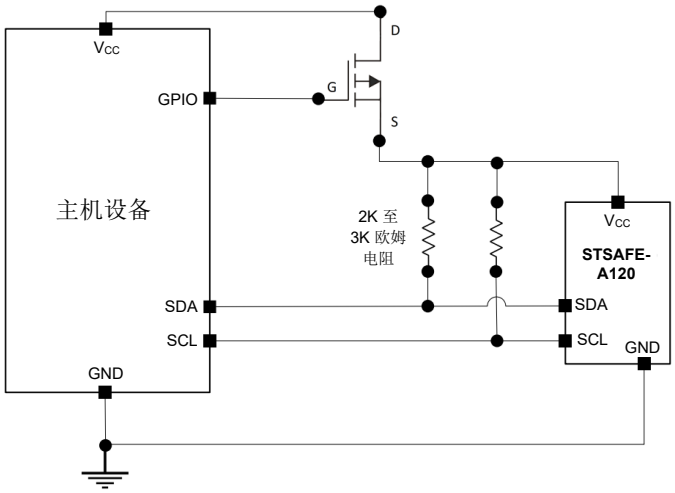
不使用 STSAFE-A120 时，可以通过控制 V_{CC} 引脚来关闭设备电源。控制 STSAFE-A120 V_{CC} 引脚或为其供电的方法有两种：通过晶体管或 GPIO。后文说明了这两种方法。

6.1 通过晶体管进行 V_{CC} 控制

通过 GPIO 控制的晶体管可用于控制 STSAFE-A120 电源。通过这种方法，STSAFE-A120 可直接从系统 V_{CC} 域供电。

I^2C 上拉电阻必须与 STSAFE-A120 V_{CC} 引脚连接在同一电源域上。

图 15. 用晶体管控制 STSAFE-A120 V_{CC} 引脚



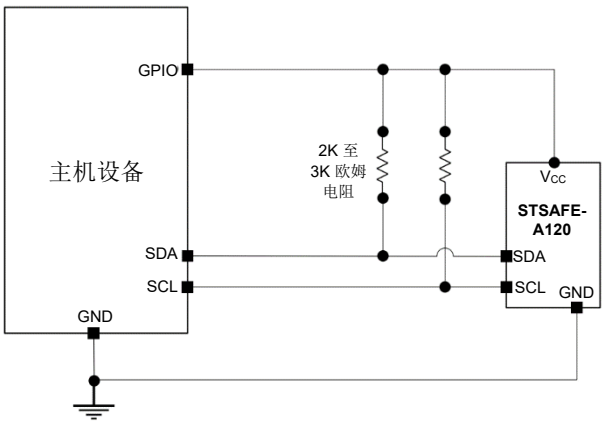
DT74401V1

6.2 通过 GPIO 向 V_{CC} 供电

如果 STSAFE-A120 位于专用总线上，则可通过主机 GPIO 供电。必须遵守以下说明：

- 不要超过 GPIO 的最大源电流
- 不要超过主机设备允许的总电流。请参考主机设备的电气特性。

图 16. 通过 GPIO 进行 STSAFE-A120 V_{CC} 引脚供电



DT74402V1

7 电气特性

本节概括了工作和测量条件及设备的直流和交流特性。后续直流和交流特性表中的参数来自各测量条件下的测试，这些测量条件在相关的表中有概括。当用户引用直流和交流特性表中的参数时，应检查其所设计电路的测量条件是否与表中描述的工作条件匹配。

7.1 绝对最大额定值

在超过绝对最大规格的范围内操作 STSAFE-A120，可能会对设备造成永久性损坏。器件长时间处在绝对最大额定条件下可能影响器件的可靠性。

表 2. 绝对最大额定值

名称	说明	条件	最小值	典型值	最大值	单位
$V_{CC\ ABS}$	绝对最大供电功率	引脚：VCC	-0.3	-	6.5	V
V_{IO}	相对地面的输入或输出电压	-	-0.3	-	VCC +0.3	V
V_{ESD}	静电放电电压符合 ANSI/ESDA/ JEDEC JS-001 标准	人体模型	-	6000	-	V
T_A	环境工作温度	-	-25	-	85	°C
T_{STG}	存储温度	-	-40	-	125	°C
T_{LEAD}	焊接期间铅的温度(1)	-	-	-	260	°C

1. *焊接期间 SO8N 和 UFDFPN8 封装温度应该与 JEDEC Std J-STD-020D（对应于小尺寸、Sn-Pb 或 Pb 装配）、意法半导体 ECOPACK® 7191395 规范、以及欧洲危险物质限制指令（ROHS 指令 2011/65/EU，2011 年 7 月）兼容。*

7.2 电源

7.2.1 电源规格

下表详细说明了 STSAFE-A120 的电源要求。

表 3. 电源规格

名称	说明	条件	最小值	典型值	最大值	单位
V_{POR}	上电复位电压	-	-	-	2.05	V
V_{CC}	电源电压	考虑到 V_{CC} 线路上 +/- 10% 的纹波(1)	2.7	-	5.5	V
$V_{CC-HIPS}$	大功率电源检测	-	5.7	6	-	V
$I_{CC-PROC}$	处理命令时的供电电流	-	-	10	11.5	mA
$I_{CC-STDBY}$	待机电流	IO 上拉至 VCC， TA = 25 °C，3 V	-	270	500	µA
		IO 上拉至 VCC， TA = 25 °C，5 V	-	350		
$I_{CC-RESET}$	复位时的电源电流	RESET = 0 复位引脚保持低电平。 使能硬件复位。 TA = 105 °C，3.3 V	-	0.8	1.5	mA

1. *最小电源电压值 (2.7 V) 考虑了 V_{CC} 线路上 +/- 10% 的纹波。*

   如果 V_{CC} 线路上没有纹波，则电源电压最低为 2.43 V，最高受 $V_{cc-HIPS}$ 限制，为 5.7 V。

7.2.2 上电和断电序列以及电源毛刺容差

STSAFE-A120 产品的上电序列必须遵循以下要求：

- $\overline{\text{RESET}}$ 引脚不得在 V_{CC} 电源引脚之前连接*高电平*。
- $\overline{\text{RESET}}$ 引脚必须在 V_{CC} 电源引脚之前或一起连接低电平。
- V_{CC} 引脚上的电压必须小于或等于 0.3 V，才能启动新的上电序列。

更多信息，请参见图 17. 上电和复位序列。

出于安全考虑，STSAFE-A120 安装了检测器。当这些触发器被触发时，STSAFE-A120 器件会进入*复位*状态，直到电源周期或复位事件发生。

建议使用能够通过主机 GPIO 管理 $\overline{\text{RESET}}$ 引脚的应用程序，以便在检测到警报时强制复位。

7.2.3 复位引脚（外部复位）

当 $\overline{\text{RESET}}$ 引脚上的复位信号为逻辑电平“0”时，电路处于复位状态。如果该信号为低电平的时间小于 t_{WL}，则不予考虑。

当 $\overline{\text{RESET}}$ 引脚处于浮动状态时，外部复位不可用，器件保持在复位状态，因为该引脚连接到内部弱下拉电阻。

当引脚 V_{CC} 连至高电平时，如果 $\overline{\text{RESET}}$ 引脚从高电平切换到低电平，然后再切换到高电平，就会发生热复位。更多信息，请参见图 18. 热复位序列。

7.2.4 上电和复位序列

图 17. 上电和复位序列

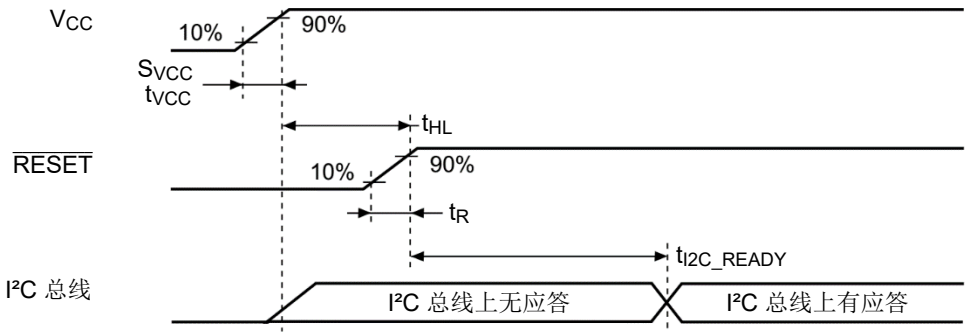


图 18. 热复位序列

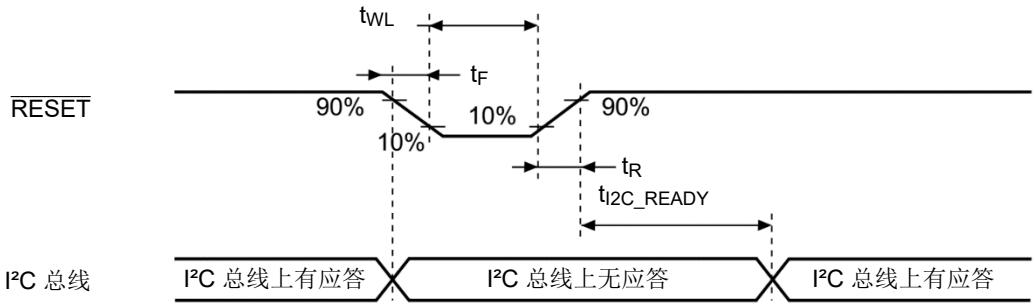


表 4. 上电和复位序列时序

名称	说明	条件	最小值	典型值	最大值	单位
t_{HL}	上电后复位激活的最短时间	-	0	-	-	µs
S_{VCC}	V_{CC} 上升斜率（从标称值的 10% 到 90%）	-	-	-	5	V/µs
t_{WL} 复位	复位脉冲宽度(1)	-	5	-	-	µs
$t_{R/tF}$ 复位	复位上升和下降时间	$V_{CC} > V_{POR}$	-	-	1	µs
t_{I2C_READY}	复位序列后，STSAFE-A120 接受 I²C 命令的延迟时间。	-	-	4.5	20	ms

1. *任何短于 5 µs 的低脉冲（从 1 到 0，再从 0 到 1）都将被忽略。*

7.2.5 功耗优化

在不使用 STSAFE-A120 时，可以通过适当移除电源来降低功耗。

这可以通过使用一个晶体管来引导 STSAFE-A120 电源，或使用一个 GPIO 来提供 $I_{CC-PROC}$ 电流来实现，该电流应符合 STSAFE-A120 的供电条件，如第 6 节所示：电气集成。

注： *$\overline{RESET}$ 信号在断电后必须保持低电平。*

7.3 DC 特性

下表详细描述了 STSAFE-A120 在 2.7 V 至 5.5 V 电压范围内的直流工作条件。

表 5. 直流操作规格和输入参数

名称	说明	条件	最小值	典型值	最大值	单位
V_{IH}	输入高电压（CLK、RESET、I/O）	-	0.7 x V_{cc}	-	V_{cc}	V
V_{IL}	输入低电压（CLK、RESET、I/O）	-	0	-	0.2 x V_{cc}	V
I_{IH}	输入高电流、高阻态 (SDA)	$0.7xV_{CC} < V_{IH} < V_{CC}$	-1	-	1	µA
	输入高电流、高阻态 (CLK)	$0.7xV_{CC} < V_{IH} < V_{CC}$	-100	-	200	nA
	输入高电流，下拉 (RST)	$0.7xV_{CC} < V_{IH} < V_{CC}$	3	7	15	µA
I_{IL}	输入低电流、高阻态 (SDA)	$0V < V_{IL} < 0.2xV_{CC}$	-1	-	1	µA
	输入低电流、高阻态 (CLK)	$0V < V_{IL} < 0.2xV_{CC}$	-100	-	100	nA
	输入低电流，下拉 (RST)	$0V < V_{IL} < 0.2xV_{CC}$	-1	1.5	10	µA
V_{OL}	输出低电压 (I/O)	IOL = 6 mA	-	-	460	mV
C_{IN1}	SCL 输入电容	V_{IN}= 0 至 $V_{CC\ Max}$	-	-	30	pF
C_{IN2}	SDA 输入电容	V_{IN}= 0 至 $V_{CC\ Max}$	-	-	30	pF

注： *$V_{CC\ MAX}$ 是表 3 中定义的最大 V_{CC}。电源规格。*

7.4 交流特性

表 6. I²C 工作条件

名称	说明	标准模式		快速模式		单位
		最小值	最大值	最小值	最大值	
f_{SCL}	子设备的 SCL 频率：处理器	-	100	-	400	kHz
$t_{HD;STA}$	输入低电平至时钟低电平（启动条件保持时间）	4.0	-	0.6	-	µs
t_{LOW}	SCL 时钟的低电平周期	4.7	-	1.3	-	µs
t_{HIGH}	SCL 时钟的高电平周期	4.0	-	0.6	-	µs
$t_{SU;STA}$	时钟高电平到输入转换/（重复）启动条件的设置时间	4.7(1)	-	1.3(1)	-	µs
$t_{HD;DAT}$	时钟低电平到输入转换	0(2)	-(3)	0(2)	(3)	µs
$t_{VD;DAT}$	数据有效时间(4)	-	-	-	0.93(5)	µs
$t_{SU;DAT}$	输入转换到时钟转换数据设置时间	250	-	100	-	ns
$t_{SU;STO}$	时钟高电平至输入高电平（停止）	4.0	-	0.6	-	µs
t_R	负载电容为 30 pF 时的时钟和数据上升时间	-	1000	20	300	ns
t_F	负载电容为 30 pF 时的时钟和数据下降时间	-	300	20 x (VDD/ 5.5 V)	300	ns

1. *不支持重复启动。*
2. *器件内部必须为 SDA 信号提供至少 300 ns 的保持时间，才能桥接 SCL 下降沿的未定义区域。*
3. *标准模式和快速模式下的 $t_{HD;DAT}$ 最大值分别可达 3.45 µs 和 0.9 µs，但必须小于 $t_{VD;DAT}$ 或 $t_{VD;ACK}$ 最大值（差值为跳变时间）。只有器件未延长 SCL 信号的低电平周期 (t_{LOW}) 时，才必须满足该最大值条件。如果时钟延长 SCL 信号，数据必须在建立时间内保持有效，之后才能释放时钟。*
4. *$t_{VD;DAT}$ = 数据信号从 SCL 低电平到 SDA 输出（高电平或低电平，取决于哪个更差）的时间。*
5. *I²C 规格值为 0.9 µs。*

图 19. AC 时钟和数据定时

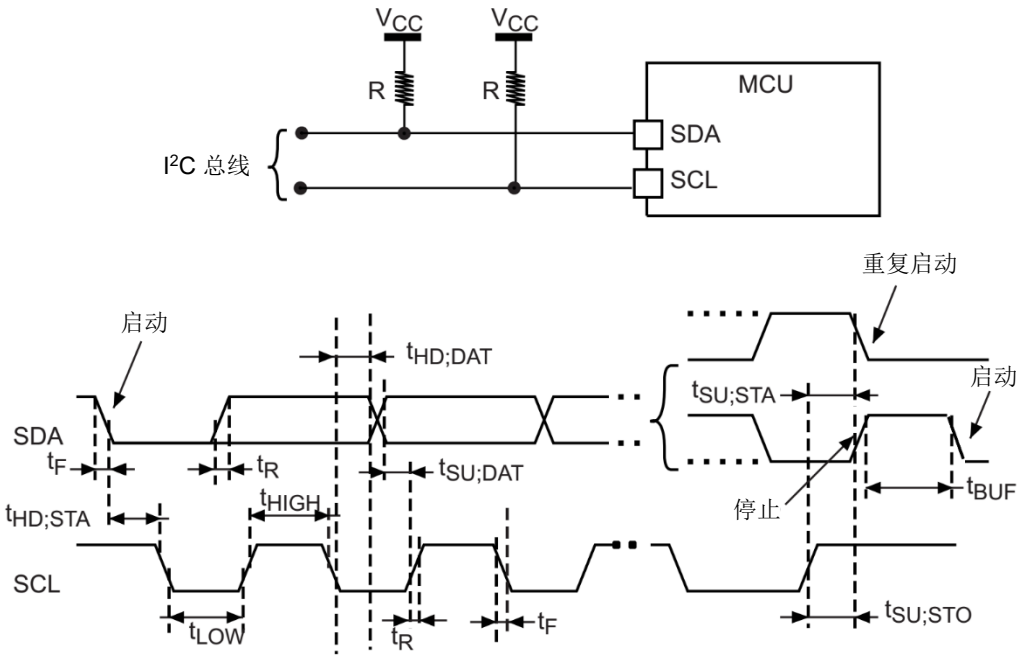


表 7. **AC 测量条件**

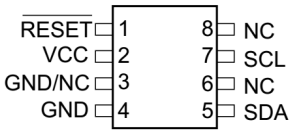
说明	范围	单位
输入上升和下降时间	最大 10 ns	ns
输入脉冲电压	V_{IL} 至 V_{IH}	V
输入时序参考电压	0.5 × V_{CC}	V
输出时序参考电压	V_{OL} 至 V_{OH}	V

8 封装信息

为满足环境要求，意法半导体为这些器件提供了不同等级的 ECOPACK 封装，具体取决于它们的环保合规等级。ECOPACK 规范，级别定义和产品状态请查阅网页：www.st.com。ECOPACK 是意法半导体的商标。

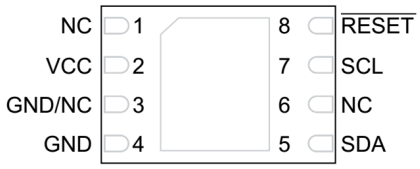
8.1 引脚说明

图 20. **SO8N 引脚排列 - 俯视图**



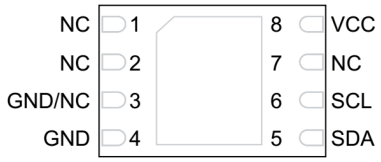
DT72963V2

图 21. **UFDFPN8 引脚排列 1- 俯视图**



DT72964V2

图 22. **UFDFPN8 引脚排列 2- 俯视图**



DT74422V1

注： UPDFN8 引脚排列 2 没有复位引脚。本文档中提及的所有复位引脚均不适用于此引脚排列。

下表列出了 STSAFE-A120 设备上四个触点的名称和说明。有关每个触点的详细情况将在本文后文提供。

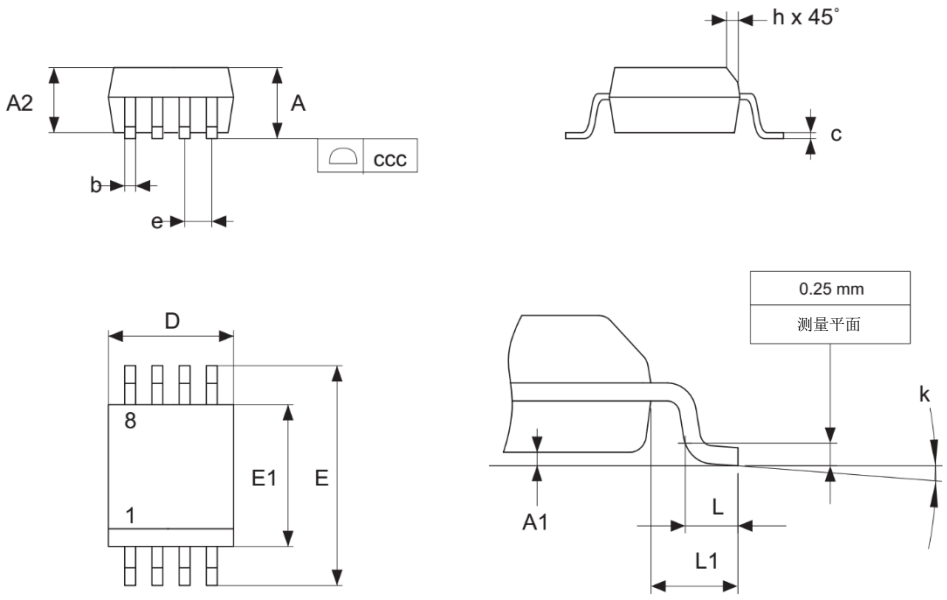
表 8. **信号描述**

信号	名称	说明
V_{CC}	电源电压	该电源电压可为 STSAFE-A120 的所有内部功能供电。
GND	电源和信号接地	电源和所有 I/O 信号的接地参考引脚。
$\overline{\text{RESET}}$	复位	该输入信号用于复位 STSAFE-A120。$\overline{\text{RESET}}$ 引脚默认为下拉引脚，这意味着如果该引脚接地或浮空，设备将复位。如果 $\overline{\text{RESET}}$ 引脚连接高电平，则设备处于激活状态。
SCL	串行时钟	此输入信号用于选通进出 STSAFE-A120 的所有数据。 I²C 主设备驱动时钟信号。
SDA	串行数据	该 I/O 信号用于将数据传入或传出 STSAFE-A120。 该信号采用漏极开路输出配置。需要一个外部上拉电阻来“上拉”输出。
NC	-	内部未连接。
GND/NC	-	要么接地，要么根本不接。

8.2 SO8N 封装信息

SO8N 是一种 8 引脚，4.9 × 6 mm 塑料小尺寸，150 mils 体宽，封装。

图 23. SO8N - 封装图



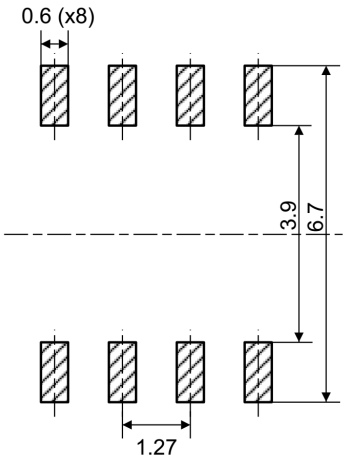
1. *图纸未按比例绘制。*

表 9. **SO8N - 机械数据**

符号	毫米			英寸(1)		
	最小值	典型值	最大值	最小值	典型值	最大值
A	-	-	1.750	-	-	0.0689
A1	0.100	-	0.250	0.0039	-	0.0098
A2	1.250	-	-	0.0492	-	-
b	0.280	-	0.480	0.0110	-	0.0189
c	0.170	-	0.230	0.0067	-	0.0091
D	4.800	4.900	5.000	0.1890	0.1929	0.1969
E	5.800	6.000	6.200	0.2283	0.2362	0.2441
E1	3.800	3.900	4.000	0.1496	0.1535	0.1575
e	-	1.270	-	-	0.0500	-
h	0.250	-	0.500	0.0098	-	0.0197
k	0°	-	8°	0°	-	8°
L	0.400	-	1.270	0.0157	-	0.0500
L1	-	1.040	-	-	0.0409	-
ccc	-	-	0.100	-	-	0.0039

1. *英寸值由毫米值换算而来，四舍五入至四位小数。*

图 24. **SO8N - 封装尺寸示例**

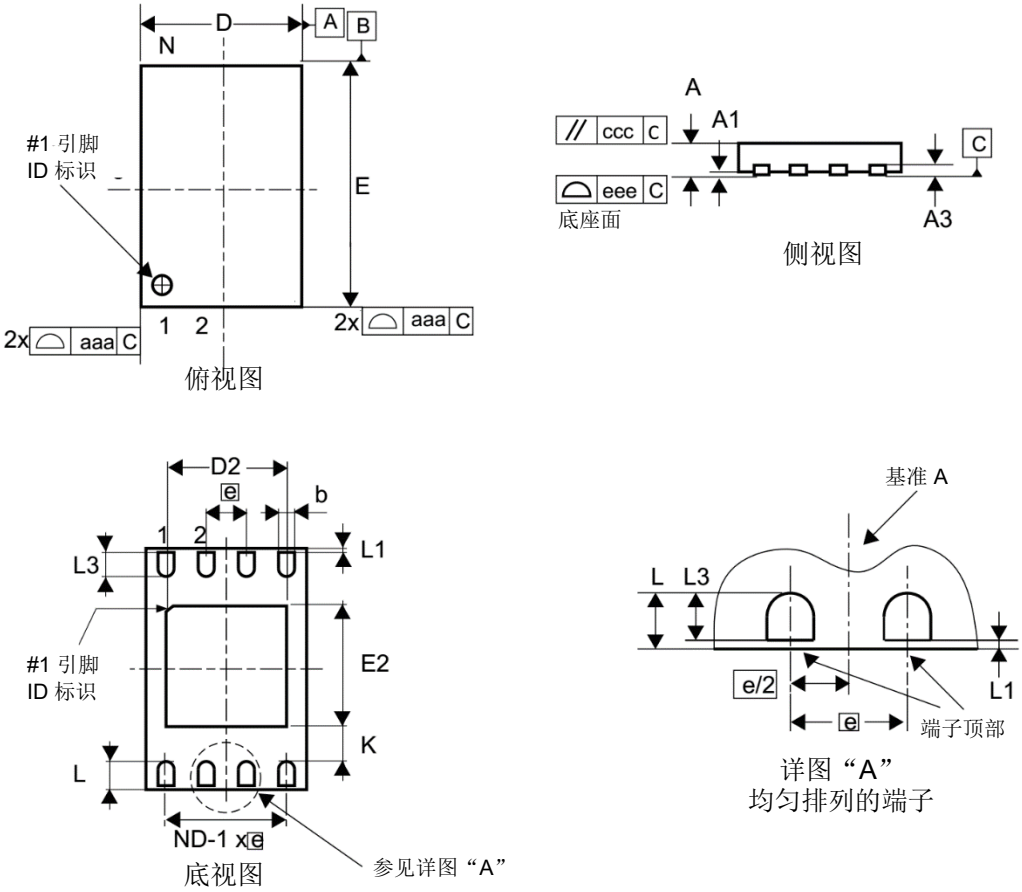


1. *尺寸单位为毫米。*

8.3 UFDFPN8 (DFN8) 封装信息

UFDFPN8 是一种 8 引脚，2 × 3 mm，0.55 mm 厚的超薄紧密排列双扁平封装。

图 25. **UFDFPN8 - 封装图**



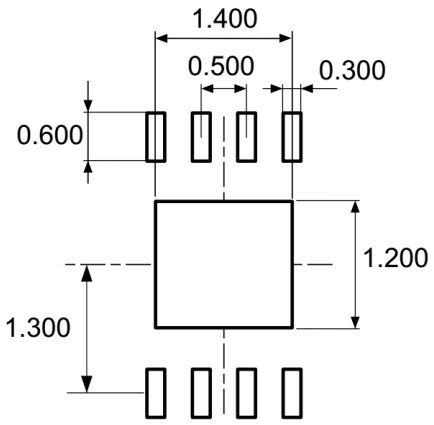
1. *最大封装翘曲为 0.05 mm。*
2. *露铜并非系统性，根据横截面可能部分或全部出现。*
3. *图纸未按比例绘制。*
4. *在最终应用中，中央焊盘（上图中 E2 乘 D2 的区域）必须连接到 V_{SS} 或保持浮动（未连接）。*

表 10. UFDFPN8 - 8引脚，2 × 3 mm，0.5 mm 间距，超薄紧密排列双扁平机械数据

符号	毫米			英寸(1)		
	最小值	典型值	最大值	最小值	典型值	最大值
A	0.450	0.550	0.600	0.0177	0.0217	0.0236
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
b(2)	0.200	0.250	0.300	0.0079	0.0098	0.0118
D	1.900	2.000	2.100	0.0748	0.0787	0.0827
D2	1.200	-	1.600	0.0472	-	0.0630
E	2.900	3.000	3.100	0.1142	0.1181	0.1220
E2	1.200	-	1.600	0.0472	-	0.0630
e	-	0.500	-	-	0.0197	-
K	0.300	-	-	0.0118	-	-
L	0.300	-	0.500	0.0118	-	0.0197
L1	-	-	0.150	-	-	0.0059
L3	0.300	-	-	0.0118	-	-
aaa	-	-	0.150	-	-	0.0059
bbb	-	-	0.100	-	-	0.0039
ccc	-	-	0.100	-	-	0.0039
ddd	-	-	0.050	-	-	0.0020
eee(3)	-	-	0.080	-	-	0.0031

1. *英寸值由毫米值换算而来，四舍五入至 4 位小数。*
2. *尺寸 b 用于镀层端子，测得其距端子顶部的距离在 0.15 mm 和 0.30 mm 之间。*
3. *适用于裸露的片板及端子。测量不包含裸片板的内嵌部分。*

图 26. UFDFPN8 - 8引脚，2 × 3 mm，0.5 mm 间距，超薄紧密排列双扁平封装尺寸示例



1. *尺寸单位为毫米。*

8.4 卷带和盘装封装

本节提供 SO8N 和 DFN8 封装的卷带信息。

图 27. **S08N 卷带式包装**

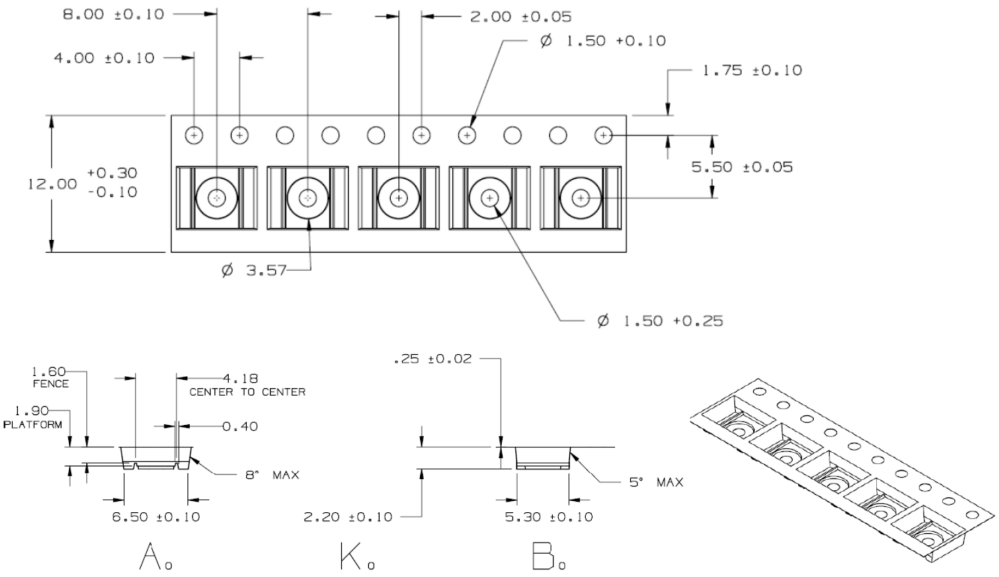
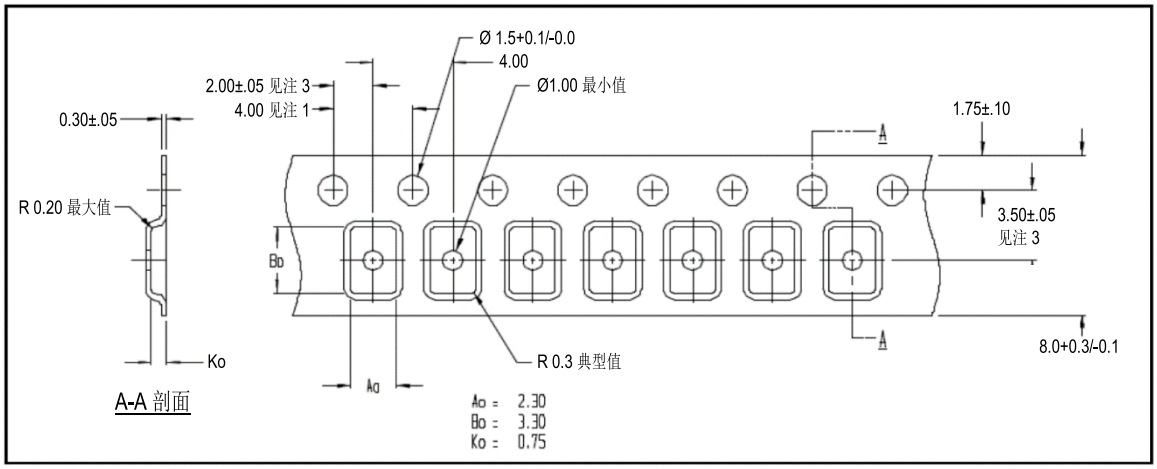


图 28. **DFN8 卷带式包装**



9 订购信息

例如：STSAFA120 S8 xxx yy

产品名称

STSAFA120 = STSAFE-A120

封装编码

S8 = SO8N

DF = UFDFPN8 引脚排列 1

D2 = UFDFPN8 引脚排列 2

客户个性化标识

xxx = 个性化设置

个性化修订

yy = 个性化修订

注：有关可用选件（速度、封装等）列表或本器件任何方面的更多信息，请联系最近的意法半导体销售办事处。

附录 A 术语表

表 11. 术语列表

术语	说明
AES	高级加密标准
CA	认证机构
CC	通用标准
CCM	密码块链接-消息认证码计数器
CMAC	基于密码的 MAC
CRC	循环冗余校验
EAL	评估保证等级
ECB	电子密码本
ECC	椭圆曲线加密
ECDH	椭圆曲线 Diffie-Hellman（静态密钥）
ECDHE	椭圆曲线 Diffie-Hellman（临时密钥）
ECDSA	椭圆曲线数字签名算法
EdDSA	Edwards 曲线数字签名算法
GPIO	通用输入/输出
I²C	跨集成电路总线
IoT	物联网
KEK	Key 加密密钥
MAC	消息认证码
MCU	微控制器单元
NIST	美国国家标准技术研究院
NVM	非易失性存储器
OTA	无线
RF	射频
R-MAC	响应 MAC
SHA	安全散列算法
ST	意法半导体
TLS	传输层安全性
TRNG	真随机数发生器

修订历史

表 12. 文档修订历史

日期	版本	变更
2024 年 4 月 2 日	1	初始版本。

目录

表格索引

图片索引

重要通知——请仔细阅读

意法半导体公司及其子公司（“意法半导体”）保留随时对意法半导体产品和/或本文档进行变更、更正、增强、修改和改进的权利，恕不另行通知。买方在订货之前应获取关于意法半导体产品的最新信息。意法半导体产品的销售依照订单确认时的相关意法半导体销售条款。

买方自行负责对意法半导体产品的选择和使用，意法半导体概不承担与应用协助或买方产品设计相关的任何责任。

意法半导体不对任何知识产权进行任何明示或默示的授权或许可。

转售的意法半导体产品如有不同于此处提供的信息的规定，将导致意法半导体针对该产品授予的任何保证失效。

意法半导体和意法半导体徽标是意法半导体的商标。关于意法半导体商标的其他信息，请访问 www.st.com/trademarks。所有其他产品或服务名称是其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。