

## BlueNRG-LP、BlueNRG-LPS（无线）固件升级

### 引言

本应用笔记介绍运行于随 BlueNRG-LP、BlueNRG-LPS 片上系统提供的 Bluetooth®低功耗（LE）栈之上的 BlueNRG-LP、BlueNRG-LPS 无线（OTA）固件升级程序。

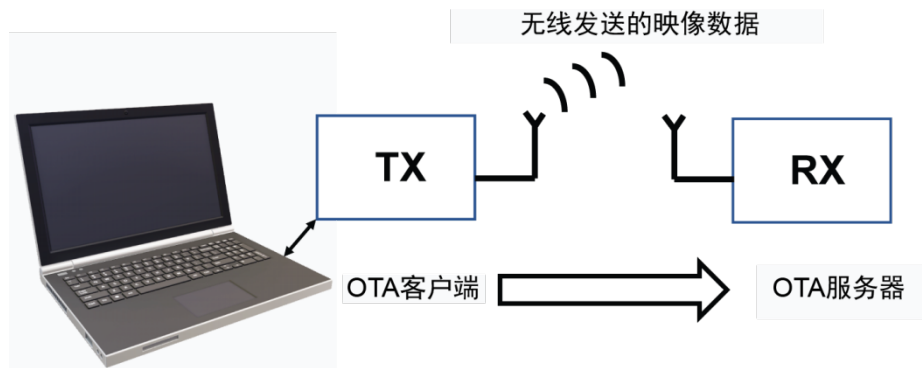
首先介绍与 OTA 固件升级过程相关的一些概念，然后帮助用户了解运行一些 OTA 固件升级会话所需的所有步骤。

**注意：** 本文内容适用于 BlueNRG-LP 和 BlueNRG-LPS 设备。BlueNRG-LP 设备和平台的任何参考也适用于 BlueNRG-LPS 设备和平台。必要时，会着重标明具体的区别。

## 1 “无线”固件升级的概念

“无线”（OTA）固件升级是一种协议，允许低功耗蓝牙从设备无线接收来自低功耗蓝牙主设备的固件映像，并将其写入 Flash 存储器。就低功耗蓝牙技术而言，OTA 固件升级框架定义了一种提供其自己的特性，并能与蓝牙 LE 栈上运行的任何给定应用使用的其他服务共存的服务。蓝牙 LE 主设备是由通过 USB 连接到 PC 的 BlueNRG-LP、BlueNRG-LPS 开发套件平台构成的组合系统。BlueNRG-LP、BlueNRG-LPS 平台由 BlueNRG GUI 驱动。鉴于这种选择，可以使用 PC 上的大量资源，尤其是用于生成固件映像的编译器，以及为了进行固件升级而在无线部署映像前存储映像所需的存储器空间。

图 1. OTA 客户端将映像数据发送到 OTA 服务器



## 2 OTA 固件升级服务描述

OTA 固件升级服务通过 BlueNRG-LP、BlueNRG-LPS DK 软件包中提供的文件 OTA\_btl.ch (Middlewares\ST\BLE\_Application\OTA folder) 实现。

下面是关于 OTA 固件升级服务及其相关特性的简述：

- Btl OTA 服务 (OTA\_SRVC\_UUID)：固件升级服务
  - aci\_gatt\_srv\_add\_service ((ble\_gatt\_srv\_def\_t\*)&ota\_service)；
- Btl 映像的特性 (IMAGE\_CHR\_UUID)：包含一些与空闲内存范围相关的信息，这是包含 OTA 固件升级服务的当前应用建议的范围
- Btl 新映像的特性 (NEW\_IMAGE\_CHR\_UUID)：包含 OTA 固件传输期间主设备想要无线发送的映像的基址和大小以及要求从设备发送确认的通知范围
- Btl 新映像内容的特性 (IMAGE\_CONTENT\_CHR\_UUID)：它包含主设备发送（通过特性写入指令）的 16 字节固件映像数据块，以及一些控制信息，例如块序号（2 字节）和用于完整性检查的校验和（1 字节）
- Btl 预期映像序号特性 (IMAGE\_SEQ\_NUM\_CHR\_UUID)：从设备通过该特性通知主设备其预期的下一个数据块或错误条件

**注意：** 在文件 OTA\_btl.c 中定义了 OTA 固件升级相关私有服务和特性的 128 位 UUID。

### 2.1 OTA 固件升级事务

本节将介绍 OTA 固件升级步骤：

1. 在安装了运行 OTA 固件升级服务的主设备和从设备后，需执行搜索程序以便连接两个设备。通过收听无线传输范围内的设备的广播进行搜索（主动扫描），并选择扫描响应中包含 OTA FW 升级服务 UUID（128 位）的设备。
2. 此外，将从广播消息中读取所选设备的名称，主设备将使用该名称强化从设备识别程序。
3. 连接后，主设备将发送“ACI\_GATT\_CLT\_DISC\_CHAR\_BY\_UUID”指令，以便读取所有 OTA 固件升级特性句柄。
4. 主设备通过“ACI\_GATT\_CLT\_READ”指令读取 Btl 映像特性，以获悉目标从设备 Flash 存储器上的空闲空间。
5. 根据上一步中获得的信息，主设备将选择合适的映像进行无线发送。候选映像（位于主设备上某位置的 \*.bin 文件）必须处于目标的空闲 Flash 存储范围内。
6. 完成选择后，主设备发送“ACI\_GATT\_CLT\_WRITE”指令，以将映像基址、大小和通知范围写入 Btl 新映像特性，并通过“ACI\_GATT\_CLT\_READ”读回以进行确认。
7. 主设备写入 Btl 预期映像序号特性描述符，以启用映像块序号和错误的从设备通知。在接收到该指令后，从设备将发回通知。

- 映像传输开始。主设备将通过一系列“ACI\_GATT\_CLT\_WRITE\_WITHOUT\_RESP”指令以 16 字节数据块发送映像（每个 16 字节数据块一个）。目标从设备每次收到新的 WRITE 指令时，将新数据块写入 Btl 新映像内容特性。每个 (N\*16) 字节数据块附带 2 字节序号和 1 字节校验和字段，用于在目标位置检查顺序和消息完整性。每次 (N\*16) 字节数据块占满从设备的内部缓冲区时，数据块被下载到 Flash 存储器。一旦从设备完成 16 字节数据块内部缓冲区的管理，它将向主设备发送通知消息，其中包含下一个预期数据块的数据块号。它可能通过最新数据块通知 Flash 写入错误和 Flash 验证错误，假如问题出在目标设备 Flash 上，此时自举会话应停止。

$N = (OTA\_ATT\_MTU\_SIZE - 3 - 4) / 16$ ，启用 OTA 固件升级过程的数据长度扩展。

对于具有数据长度扩展功能（最大 PDU 长度= 251 字节）且 ATT\_MTU 大小增加 (> 23 字节) 的蓝牙 LE 栈 v3.0 或更高版本，将量身定制 N 值，以便在最大允许 OTA 客户端 ATT\_MTU 大小 (OTA\_ATT\_MTU\_SIZE) 范围内获得尽可能合适的 OTA 数据包大小。这样可以增加链路层的每个蓝牙 LE OTA 数据包传输的数据量，加快 OTA 固件升级程序的执行速度。

蓝牙 LE 栈 LE APIs HCI\_LE\_SET\_DATA\_LENGTH()和 ACI\_ATT\_CLT\_EXCHANGE\_MTU() API 用于设置 OTA 客户端发射器和 OTA 服务器接收器侧的数据长度扩展功能，并遵循支持的最大 ATT\_MTU 长度。

ACI\_GATT\_CLT\_WRITE\_WITHOUT\_RESP 指令使用的 OTA 固件包结构如下：

图 2. OTA\_packet\_structure



其中：

- 使用校验和字节进行包完整性检查
  - 映像数据字节包含要传输的输入文件 (N \* 16) 字节
  - 需要确认字节表示 OTA 固件传输期间 OTA 客户端预期从设备会发送通知（1：预期会发送通知；0：预期不会发送通知）
  - 序号字节用于表示 OTA 固件传输期间使用的预期映像序号值
- 如果成功下载到目标设备 Flash 上的字节数与最初提供的映像大小信息相符，OTA 固件升级程序将在每个应用中断向量表的保留条目中写入特定的应用有效性标签，以便 OTA 复位管理器能够正确识别新的有效应用的地址。
  - 中断向量表中保存的应用有效性标签允许以避免跳转至无效应用的方式来处理 OTA 固件升级会话失败（所有权总是转移至最后一个有效应用）。

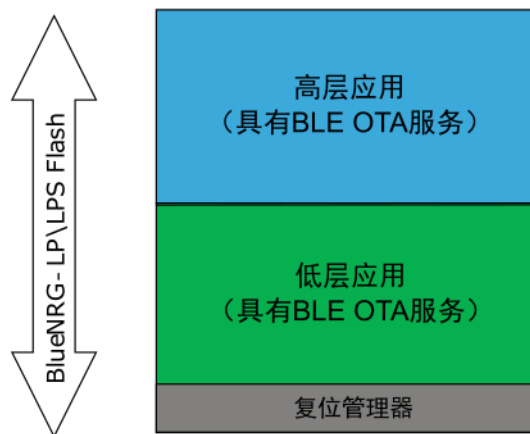
## 2.2 蓝牙 LE OTA 服务固件升级架构

蓝牙 LE OTA 服务固件升级架构包括以下组成部分：

- 复位管理器
  - 应在复位后启动，并向最近更新并有效的蓝牙 LE 应用转移控制。

- 具有蓝牙 LE OTA 服务的应用（低层应用）
  - 它定义了 OTA 服务，以便为自身提供 OTA 固件升级功能。
  - 运行时，它允许无线接收新的应用映像数据包并将其保存在特定 Flash 扇区（高层应用存储区）。
  - 如果 OTA 固件升级过程成功完成，将执行软件复位，以便通过复位管理器将所有权交给新的有效高层应用。
- 具有蓝牙 LE OTA 服务的应用（高层应用）
  - 它也定义了 OTA 服务，以便为自身提供 OTA 固件升级功能。
  - 运行时，它允许无线接收新的应用映像数据包并将其保存在特定 Flash 扇区（低层应用存储区）。
  - 如果 OTA 固件升级过程成功完成，将执行软件复位，以便通过复位管理器将所有权交给新的有效低层应用。

图 3. 蓝牙 LE OTA 服务固件升级架构

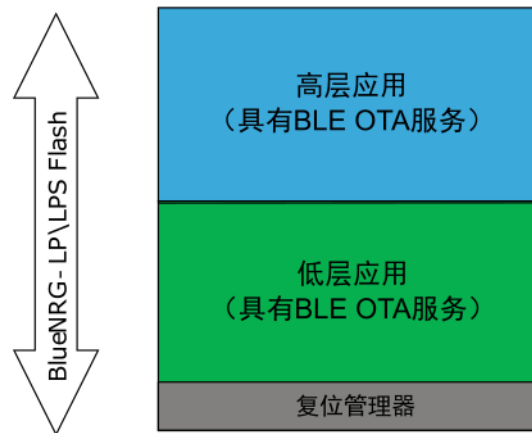


### 2.2.1 复位管理器

BlueNRG-LP、BlueNRG-LPS 的 Flash 基址从 0x10040000 开始，意味着在设备复位时，微控制器将开始执行该范围内的应用映像。当 OTA 固件升级程序从大于 Flash 基址的基址开始写入新映像时，需要一种可以在每次设备复位时向新应用跳转的方法。为此，首先需要为包含 OTA 固件升级服务的每个设备加载 OTA 复位管理器（从 Flash 地址开始）。在设备复位时，复位管理器将负责跳转至 OTA 固件升级程序成功加载的最后一个有效映像的位置，如保存在每个应用中中断向量表的保留条目中的应用有效性标签组合所示，有效性标签于 OTA 固件升级会话成功后设置（参考文件 OTA\_ResetManager.c 中的 OTA\_Check\_Application\_Tags\_Value() 函数）。下图所示为具有板载 OTA 固件升级服务的 BlueNRG-LP、BlueNRG-LPS 器件的典型 Flash 存储器布局。在最初设置设备时，必须将 OTA 复位管理器本身上传到地址 0x10040000，然后将低层应用上传到地址 0x10040800（复位管理器上端）。

BlueNRG-LP、BlueNRG-LPS DK 软件包提供了 OTA 复位管理器应用项目 + 头文件和源文件（BLE\_OTA\_ResetManager 项目）。

图 4. 具有 OTA 服务的低层和高层应用



### 2.2.2 具有蓝牙 LE OTA 服务的应用

为了添加文件 OTA\_btl.c 中提供的蓝牙 LE OTA 服务，必须执行以下步骤（取 IAR EWARM 为参考示例）：

1. 在 EWARM 工作区，添加 CONFIG\_OTA\_LOWER 或 CONFIG\_OTA\_HIGHER 作为预处理器和链接器选项，分别用于构建具有 OTA 服务的蓝牙 LE 低层或高层应用。为了启用数据长度扩展，以支持 OTA 固件升级过程，必须添加 CONFIG\_SW\_OTA\_DATA\_LENGTH\_EXT，作为预处理器选项。此外，用户应用必须构建包含数据长度扩展功能的模块化配置选项（BLE\_STACK\_SLAVE\_DLE\_CONF 作为最低配置）。
2. 在 EWARM 工作区，使用默认的链接器文件，以与上图所示的 Flash 布局保持一致（在 BlueNRG-LP、BlueNRG-LPS DK 软件包的 OTA 演示应用文件夹中提供）。
3. 在 EWARM 工作区，添加项目文件 OTA\_btl.c，并添加 OTA\_btl.h 文件所在目录的参考路径。
4. 在用户应用中，包含头文件 OTA\_btl.h。
5. 在用户应用中，调用 OTA\_Add\_Btl\_Service() API，以便添加 OTA 蓝牙 LE 服务和相关特性。
6. 在用户应用中，为扫描响应添加如下 OTA 服务 UUID：  
hci\_le\_set\_scan\_resp\_data(18,BTLServiceUUID4Scan)。
7. 在用户应用的 aci\_gatt\_attribute\_modified\_event() 和 aci\_gatt\_srv\_write\_event() 回调中，添加对 OTA\_Write\_Request\_CB() API 的调用。
8. 在用户应用的 aci\_gatt\_srv\_read\_event() 事件回调中，添加对 OTA\_Read\_Char() API 的调用（以使蓝牙 LE 栈能够发送响应）。
9. 在用户应用中，添加 if (OTA\_Tick() == 1) 检查，以便检查何时跳转至新的已升级应用（通过调用函数 OTA\_Jump\_To\_New\_Application()）。
10. 在用户应用的 aci\_hal\_end\_of\_radio\_activity\_event() 回调中，添加对 OTA\_Radio\_Activity() API 的调用（以使 FLASH 写操作与无线活动同步）。

**注意：** 为了明确识别所需的软件组件以支持 OTA 固件升级过程，应对上面列出的第 5、6、7、8 和 9 点使用 `#if ST_OTA_FIRMWARE_UPGRADE_SUPPORT` 预处理器选项。  
即：

```
#if ST_OTA_FIRMWARE_UPGRADE_SUPPORT
```

```
    OTA_Add_Btl_Service();
```

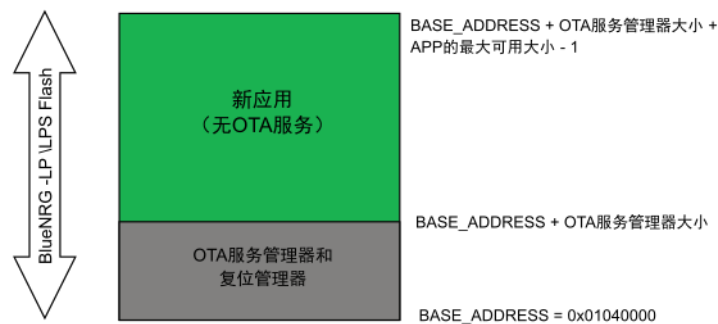
```
#endif
```

在 OTA 升级会话期间，特定的 LED 将点亮（即 BlueNRG-LP、BlueNRG-LPS 平台上的 LED DL3）。

## 2.3 OTA 服务管理器框架

图 1. OTA 客户端将映像数据发送到 OTA 服务器中所述的蓝牙 LE OTA 服务架构提供了一种更简单的方法，即使用基本 OTA 服务管理器应用，其包含蓝牙 LE OTA 服务及其特性和 OTA 复位管理器功能。

图 5. OTA 服务管理器 Flash 存储器布局



蓝牙 LE OTA 服务管理器架构包括以下组成部分：

- OTA 服务管理器
  - 它仅包含蓝牙 LE OTA 服务和特性，向任何应用提供 OTA 固件升级功能。它还包含 OTA 复位管理器功能，可向最近更新并有效的应用转移控制。
- 新应用
  - 这是通过 OTA 服务管理器下载的应用映像。
  - 无需包含 OTA 固件升级服务。
  - 为了使用此功能，应用只需激活 OTA 服务管理器（OTA\_bt1.c 文件中提供了特定的 `OTA_Switch_To_OTA_Service_Manager_Application()` API）。
  - 它位于固定的 Flash 地址。

### 2.3.1 OTA 服务管理器应用

OTA 服务管理器相当于独立的 OTA 固件升级应用，为不包括任何 OTA 服务但需要使用 OTA 固件升级功能的任何应用提供此功能。它还包含 OTA 复位管理器功能，可向最近更新并有效的蓝牙 LE 应用转移控制。

BlueNRG-LP、BlueNRG-LPS DK 软件包提供了 OTA 服务管理器应用项目 + 头文件和源文件（BLE\_OTA\_ServiceManager 工作区）。

为了启用数据长度扩展，以支持 BlueNRG-LP、BlueNRG-LPS 器件、蓝牙 LE 栈 v3.x 的 OTA 固件升级过程，必须在 OTA 服务管理器应用上添加 CONFIG\_SW\_OTA\_DATA\_LENGTH\_EXT 作为预处理器选项。

此外，OTA 服务管理器应用采用模块化方式构建，OTA 基本配置包括数据长度扩展功能（BLE\_STACK\_SLAVE\_DLE\_CONF）：

- 无控制器私有
- 无 LE 安全连接
- 无主/中央设备
- 数据长度扩展

### 2.3.2 新蓝牙 LE 应用

对于需要使用 OTA 服务管理器功能的应用，需执行以下基本步骤：

1. 在 EWARM 工作区，添加 CONFIG\_OTA\_USE\_SERVICE\_MANAGER 作为预处理器和链接器选项。
2. 在 EWARM 工作区，使用默认的链接器文件，以与 Flash 布局保持一致（在 BlueNRG-LP、BlueNRG-LPS DK SW 软件包的演示应用文件夹中提供）。
3. 在 EWARM 工作区，添加项目文件 OTA\_btl.c，并添加 OTA\_btl.h 文件所在目录的参考路径。
4. 在新的用户应用源文件中，包含头文件 OTA\_btl.h。
5. 在新的用户应用源文件中，添加一些代码，以允许应用启动 OTA 服务管理器应用。可以使用简单的按钮控制对 OTA\_Jump\_To\_Service\_Manager\_Application()（文件 OTA\_btl.c 中提供了该 API）进行调用。
6. 在用户应用的 aci\_hal\_end\_of\_radio\_activity\_event()回调中，添加对 OTA\_Radio\_Activity() API 的调用（以使 FLASH 写操作与无线活动同步）。

**注意：** 在使用 OTA 服务管理器时，新应用无需包含任何 OTA 固件升级服务。此外，应用必须始终位于固定的基址。



### 3 硬件和软件资源

介绍如何设置蓝牙 LE OTA 固件升级演示应用前，请参考所需的硬件和软件资源列表。参考示例中使用了 BlueNRG-LP 和相关开发套件。类似的概念也适用于 BlueNRG-LPS 和相关开发套件。

表 1. OTA 固件升级的硬件和软件资源

资源
2 个 BlueNRG-LP 平台和相关 USB 线（即 STEVAL-IDB011Vx, x = 1,2）
BlueNRG-LP、BlueNRG-LPS DK x.x.x 资源： <ul style="list-style-type: none"> <li>• OTA 复位管理器和服务管理器</li> <li>• 蓝牙 LE 传感器演示和蓝牙 LE SerialPort 应用，构建用于支持 OTA 固件升级服务或 OTA 服务管理器方法</li> <li>• BlueNRG navigator PC 应用</li> <li>• BlueNRG-X flasher PC 应用</li> </ul>
STSW-BNRGUI 软件包提供了 BlueNRG 图形用户界面（GUI）。 还可以使用实现 OTA 固件升级客户端侧的 OTA_Central_3_x.py 脚本（STSW-BNRGUI 软件包中也有提供）。
具有以下资源的 PC： <ul style="list-style-type: none"> <li>Windows®10</li> <li>至少 128 MB RAM</li> <li>2 个 USB 端口</li> <li>有 40 Mb 硬盘空间可用</li> <li>IAR embedded workbench 8.40.1 或更高版本（取 IAR EWARM 为参考工具链）</li> </ul>

## 4 运行 BlueNRG-LP、BlueNRG-LPS DK 软件包 OTA 演示应用

演示应用项目 “sensor demo” 和 “SerialPort” 具有特定的工作区，可用来练习以下两种方法：

1. 构建蓝牙 LE 应用以包含 OTA 固件升级服务并使用 OTA 复位管理器
2. 构建使用 OTA 服务管理器的蓝牙 LE 应用

下面是对具有 OTA 固件升级功能的 Sensor Demo 应用可用项目工作区的简单描述：

**表 2. 具有 OTA 固件升级功能的 Sensor Demo IAR 工作区**

Sensor Demo 应用项目工作区	说明
LowerApp_OTA	包含采用“低层应用”内存布局的 OTA 固件升级服务的应用配置（参考图 4. 具有 OTA 服务的低层和高层应用以及第 2.2 节“蓝牙 LE OTA 服务固件升级架构”）
HigherApp_OTA	包含采用“高层应用”内存布局的 OTA 固件升级服务的应用配置（参考图 4. 具有 OTA 服务的低层和高层应用以及第 2.2 节“蓝牙 LE OTA 服务固件升级架构”）
Use_OTA_ServiceManager	使用“OTA 服务管理器”内存布局的应用配置（参考图 6.OTA 过程：OTA 自举程序窗口和第 2.3 节“OTA 服务管理器框架”）

下面是对具有 OTA 固件升级功能的蓝牙 LE SerialPort 聊天应用可用项目工作区的简单描述：

**表 3. 具有 OTA 固件升级功能的 BLE\_SerialPort 演示 IAR 工作区**

BLE_SerialPort 应用项目工作区	说明
Server_LowerApp_OTA	服务器应用配置包含采用“低层应用”内存布局的 OTA 固件升级服务的服务器应用配置（参考图 4. 具有 OTA 服务的低层和高层应用以及第 2.2 节“蓝牙 LE OTA 服务固件升级架构”）
Server_HigherApp_OTA	服务器应用配置包含采用“高层应用”内存布局的 OTA 固件升级服务的服务器应用配置（参考图 4. 具有 OTA 服务的低层和高层应用以及第 2.2 节“蓝牙 LE OTA 服务固件升级架构”）
Server_Use_OTA_ServiceManager	使用“OTA 服务管理器”内存布局的服务器应用配置（参考图 6.OTA 过程：OTA 自举程序窗口和第 2.3 节“OTA 服务管理器框架”）。

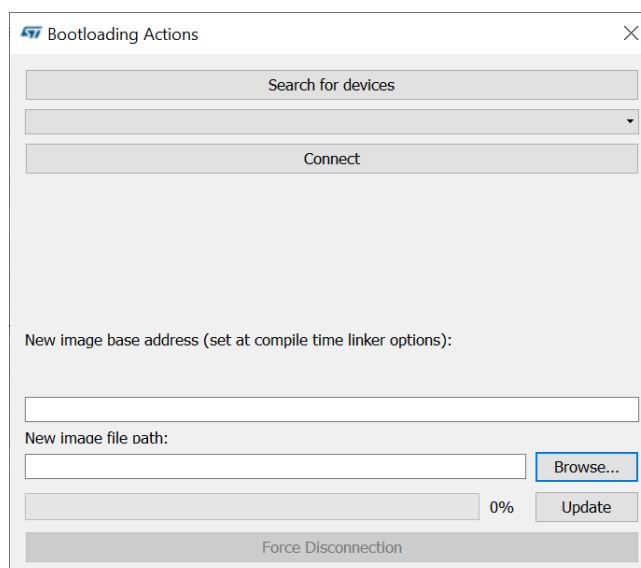
注意：

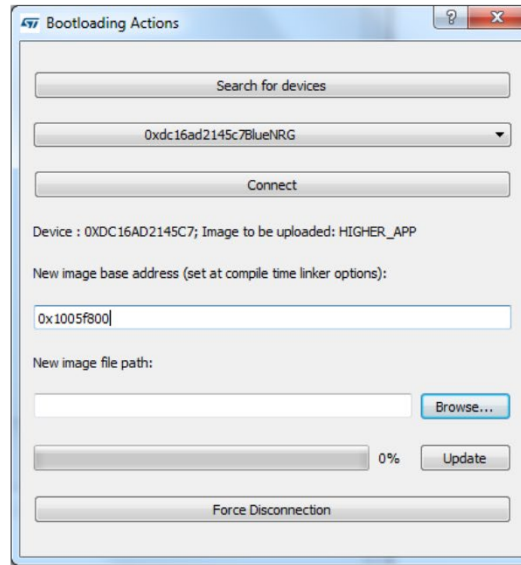
- `OTA_Central_3_x.py` 是一个 python 脚本，根据第 2.2 节“蓝牙 LE OTA 服务固件升级架构”中所述的 OTA 固件升级架构实现了 OTA 固件升级客户端。
- 蓝牙 LE Beacon 应用还提供了集成 OTA 服务管理器的 Beacon 应用的工作区示例 (`Use_with_OTA_ServiceManager`)。

### 4.1 构建应用以包含 OTA 固件升级服务

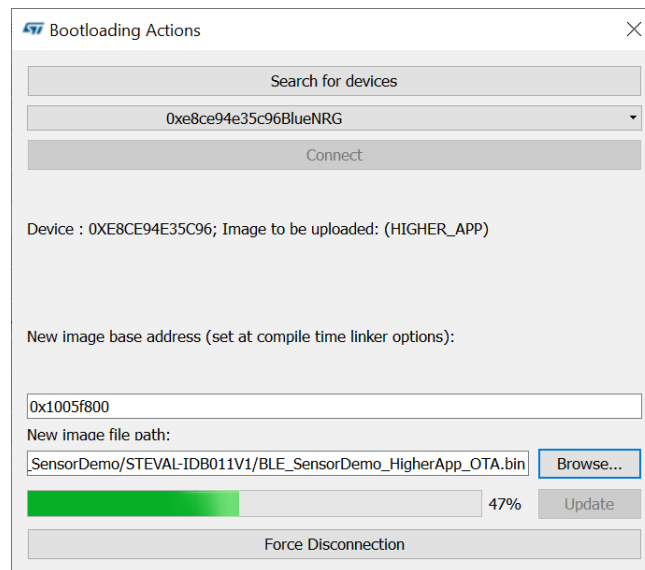
下面是对使用 BlueNRG-LP 传感器演示应用（具有 OTA 服务支持）运行 BlueNRG GUI OTA 自举程序工具的分步描述（使用 STEVAL-IDB011V1 作为参考平台，并使用 IAR EWARM 作为参考工具链）：

1. 将两个 BlueNRG-LP 套件平台插入 PC 上的 USB 连接器。
2. 选择一个 BlueNRG-LP 套件平台并连接到 PC USB 端口。
3. 打开 EWARM IAR 工具。
4. 打开 BLE\_OTA\_ResetManager.eww IAR 项目，在菜单中选择“项目”->“下载”->“擦除存储器”以擦除器件 Flash。
5. 在所选平台上构建并下载相关的 OTA 复位管理器应用映像（Firmware\BLE\_Examples 文件夹中提供了预构建映像，也可通过 BlueNRG-LP navigator PC 工具或 BlueNRG-X Flasher 工具加载预构建映像）。
6. 在所选平台上打开 BLE\_SensorDemo.eww IAR 项目和 LowerApp\_OTA 工作区，构建并下载相关的应用映像（Firmware\BLE\_Examples 文件夹中提供了预构建映像，也可通过 BlueNRG-LP Navigator 或 Flasher 工具加载预构建映像）。
7. [可选] 获取“BlueNRG app for smartphones (IoS or Android)”，以发现、连接并和步骤 6 中加载到 BlueNRG-LP 平台上的 Sensor Demo 应用进行数据交互。
8. [可选] 如果执行了步骤 7 中的操作，则操作“BlueNRG app for smartphones (IoS or Android)”断开与 BlueNRG-LP 套件平台的连接。最低层 Sensor Demo 应用断开连接后，开始广告。这将使该应用成为通过 BlueNRG GUI 自举程序工具或 OTA\_Central\_3\_x.py 脚本执行蓝牙 LE OTA 固件升级程序的潜在候选应用。
9. 通过 BlueNRG GUI 工具，将 DTM 应用程序下载到第二个 BlueNRG LP 套件平台。（Firmware\BLE\_Examples 文件夹中提供了预构建 DTM 映像 DTM\_UART\_WITH\_UPDATER.hex，也可通过 BlueNRG-LP Navigator 或 Flasher 工具加载预构建映像）。
10. 在 PC 上打开 BlueNRG GUI，选择与步骤 9 中配置的 BlueNRG-LP 平台相关的 COM 端口（在下拉列表中选择“Port”并单击“Open”）。
11. 选择“Tools”->“OTA 自举程序”打开包含 OTA 固件升级操作的对话框，并单击“Search for devices”。
12. 在单击“Search for devices”后，GUI 将启动搜索过程，并返回无线传输范围内运行 OTA 固件升级服务的设备的地址和应用名称相关信息。一旦前面的过程结束，就可以通过“Search for devices”按钮下方的组合框箭头打开设备列表，此时用户可以选择要连接的设备，然后使用“Connect”按钮进行连接以便执行后续的升级过程（操作界面上会显示应用程序的地址和名称）。如果发现连接了错误的设备，用户只需单击“Force Disconnection”按钮，并在组合框内重新选择设备。在选择设备并单击“Connect”按钮进行连接后，可以读取相关空闲内存范围，它要求用户为从设备提供以符合预期范围的基址和大小编译的新映像文件。因此，用户可以打开 SensorDemo IAR 工作区 HigherApp\_OTA，并构建相关的 BLE\_SensorDemo\_HigherApp\_OTA.bin 映像（位于 BLE\_SensorDemo\EWARM\STEVAL-IDB011V1\BLE\_SensorDemo\_HigherApp\_OTA\Exe 文件夹），该映像包含使用等于最高地址的基址编译的传感器演示版本。

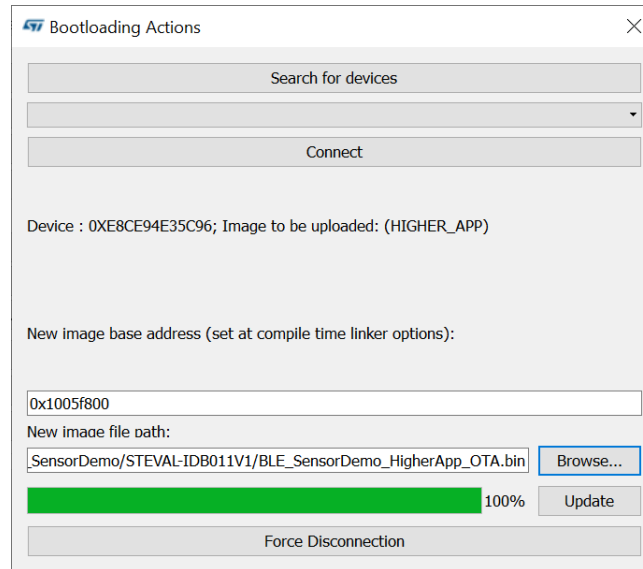
**图 6. OTA 过程：OTA 自举程序窗口**


**图 7. OTA 过程：搜索设备并连接**


- 用户通过“Browse”按钮选择使用了正确基址编译的映像文件后，可以选择“Update”按钮启动 OTA 固件升级过程：进度条将显示完成此过程需要的时间：

**图 8. OTA 过程：自举程序升级**


- 当过程结束时，启动新应用。

**图 9. OTA 过程：自举程序升级完成**

**注意：**

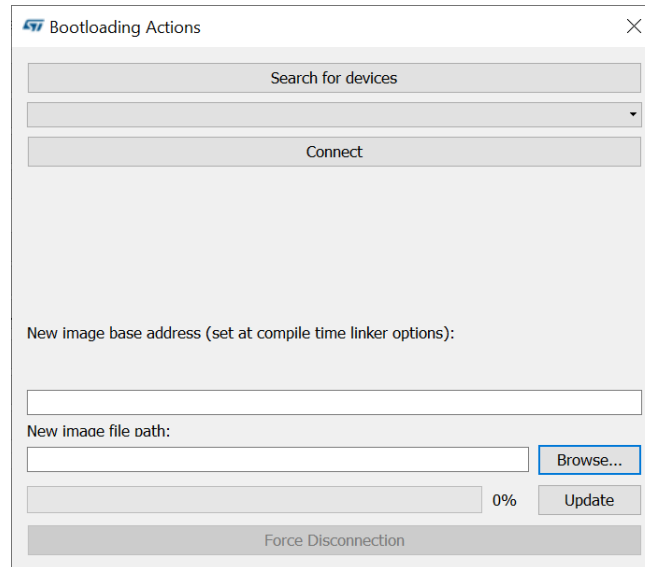
- 可以对 BlueNRG-LP 蓝牙 LE SerialPort 演示应用使用类似程序，以便验证蓝牙 LE OTA 固件升级服务功能（请参考 BLE\_SerialPort\EWARM\BLE\_SerialPort.eww、Server\_LowerApp\_OTA 和 Server\_HigherApp\_OTA 工作区）。
- OTA\_Central\_3\_x.py 脚本也提供与 BlueNRG GUI OTA 自举程序工具相同的 OTA 客户端功能。

## 4.2 构建使用蓝牙 LE OTA 服务管理器的应用

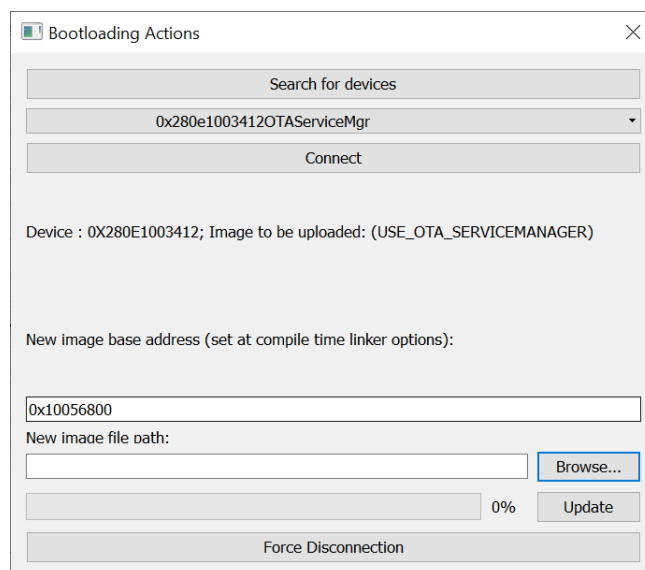
下面是对使用 BlueNRG OTA 服务管理器和 SensorDemo、SerialPort 工作区（处理 OTA 服务管理器配置）运行 BlueNRG GUI OTA 自举程序工具的分步描述（使用 STEVAL-IDB011V1 作为参考平台，并使用 IAR EWARM 作为参考工具链）：

1. 将两个 BlueNRG-LP 套件平台插入 PC 上的 USB 连接器。
2. 选择一个套件平台并连接到 PC USB 端口。
3. 打开 EWARM IAR 工具。
4. 打开 BLE\_OTA\_ServiceManager.eww IAR 项目、工作区中选择 Release，并在菜单中选择“项目”->“下载”->“擦除存储器”以擦除器件 Flash。
5. 在所选平台上构建并下载相关的应用映像（Firmware\BLE\_Examples 文件夹中提供了预构建映像，也可通过 BlueNRG-LP Navigator 或 Flasher 工具加载预构建映像）。
6. 在该平台上打开 BLE\_SensorDemo.eww IAR 项目和 Use\_OTA\_ServiceManager 工作区，构建并下载相关的应用映像（Firmware\BLE\_Examples 文件夹中提供了预构建映像，也可通过 BlueNRG-LP Navigator 或 Flasher 工具加载预构建映像）。
7. [可选]获取“BlueNRG app for smartphones (IoS or Android)”，以发现、连接并和步骤 6 中加载到 BlueNRG-LP 平台上的 Sensor Demo 应用进行数据交互。
8. [可选]如果执行了步骤 7 中的操作，则操作“BlueNRG app for smartphones (IoS or Android)”断开与 BlueNRG-LP 套件平台的连接。
9. 通过 BlueNRG GUI 工具，将 DTM 应用程序下载到第二个 BlueNRG LP 套件平台。（Firmware\BLE\_Examples 文件夹中提供了预构建 DTM 映像 DTM\_UART\_WITH\_UPDATER.hex，也可通过 BlueNRG-LP Navigator 或 Flasher 工具加载预构建映像）。
10. 在 PC 上打开 BlueNRG GUI，选择与步骤 9 中配置的 BlueNRG-LP 平台相关的 COM 端口（在下拉列表中选择“Port”并单击“Open”）。
11. 如果在运行 SensorDemo 应用的 BlueNRG-LP 平台上执行了步骤 7 和 8 中的操作，则按下按钮 PUSH1 以激活 OTA 服务管理器；此操作将控制权交给管理 OTA 固件升级过程的 OTA 服务管理器应用。

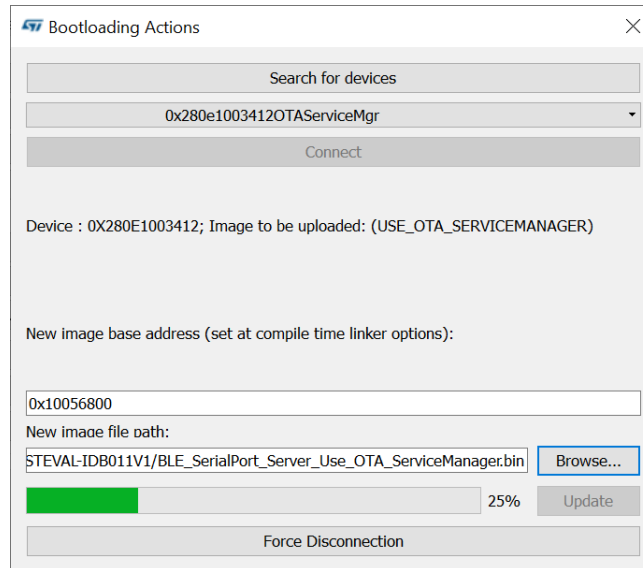
- 在 BlueNRG GUI 上，选择 “Tools” -> “OTA 自举程序” 打开包含 OTA 固件升级操作的对话框，并单击 “Search for devices”。

**图 10. OTA 服务管理器过程：OTA 自举程序窗口**


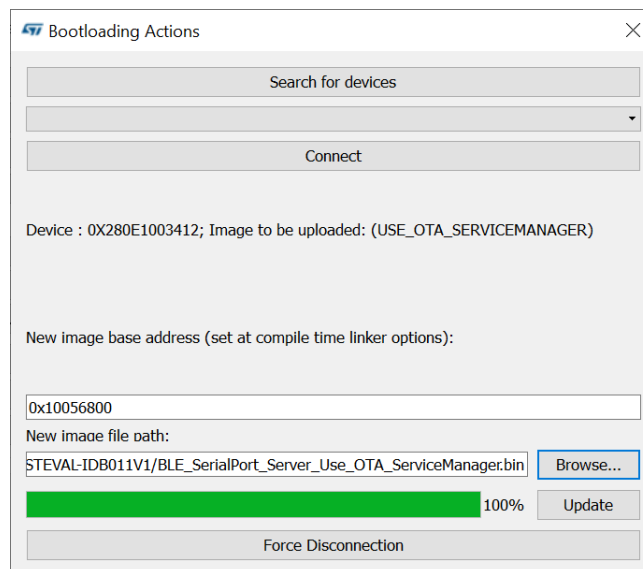
- 在单击 “Search for devices” 后，GUI 将启动搜索过程，并返回无线传输范围内运行 OTA 固件升级服务的设备的地址和应用名称相关信息。一旦前面的过程结束，则可以通过 “Search for devices” 按钮下方的组合框箭头打开设备列表，用户可以从中找到运行 OTA 服务管理器的设备，然后选择 “Connect” 按钮。如果发现连接了错误的设备，只需选择 “Force Disconnection” 按钮，并在组合框内重新选择设备。在选择设备并单击 “Connect” 按钮进行连接后，可以读取相关空闲内存范围，用户必须在蓝牙 LE 设备上提供以符合预期范围的基址和大小编译的新映像文件：
  - 因此，用户可以打开 BLE\_SerialPort IAR 工作区 Use\_OTa\_ServiceManager，并构建相关的 BLE\_SerialPort\_Server\_Use\_OTa\_ServiceManager.bin 映像（位于 BLE\_SerialPort\EWARM\STEWAL-IDB011V1\BLE\_SerialPort\_Server\_Use\_OTa\_ServiceManager\Exe 文件夹），该映像包含使用所需基址编译的 BLE SerialPort 演示版本。

**图 11. OTA 服务管理器过程：搜索设备并连接**


- 用户通过“Browse”按钮选择使用了正确基址编译的映像文件 BLE\_SerialPort\DTM\_UART\_WITH\_UPDATER.hex\BLE\_SerialPort\_Server\_Use\_OTA\_ServiceManager\Exe\BLE\_SerialPort\_Server\_Use\_OTA\_ServiceManager.bin 后，可以选择“Update”（更新）按钮启动 OTA 自举加载过程：进度条将显示完成此过程需要的时间。

**图 12. OTA 服务管理器过程：自举程序升级**


- 当过程结束时，启动新的蓝牙 LE SerialPort 应用。

**图 13. OTA 服务管理器过程：自举程序升级完成**


**注意：** OTA\_Central\_3\_x.py 脚本也提供与 BlueNRG GUI OTA 自举程序工具相同的 OTA 客户端功能。

## 5 缩略语列表

表 4. 本文缩略语列表

术语	意义
蓝牙低功耗	超低功耗蓝牙
BTL	自举程序
FW	固件
GUI	图形用户界面
OTA	无线
SW	软件
USB	通用串行总线



## 版本历史

表 5. 文档版本历史

日期	版本	变更
2020 年 7 月 24 日	1	初始版本。
2022 年 4 月 6 日	2	更新了“引言”章节、第 1 节““无线”固件升级的概念”、第 2.2 节“蓝牙 LE OTA 服务固件升级架构”和第 3 节“硬件和软件资源”。 更新了图 1. OTA 客户端将映像数据发送到 OTA 服务器、图 3. 蓝牙 LE OTA 服务固件升级架构、图 4. 具有 OTA 服务的低层和高层应用以及图 5. OTA 服务管理器 Flash 存储器布局。

## 目录

<b>1</b>	<b>“无线” 固件升级的概念</b>	<b>2</b>
<b>2</b>	<b>OTA 固件升级服务描述</b>	<b>3</b>
<b>2.1</b>	OTA 固件升级事务	3
<b>2.2</b>	蓝牙 LE OTA 服务固件升级架构	4
<b>2.2.1</b>	复位管理器	5
<b>2.2.2</b>	具有蓝牙 LE OTA 服务的应用	6
<b>2.3</b>	OTA 服务管理器框架	7
<b>2.3.1</b>	OTA 服务管理器应用	7
<b>2.3.2</b>	新蓝牙 LE 应用	8
<b>3</b>	<b>硬件和软件资源</b>	<b>9</b>
<b>4</b>	<b>运行 BlueNRG-LP、BlueNRG-LPS DK 软件包 OTA 演示应用</b>	<b>10</b>
<b>4.1</b>	构建应用以包含 OTA 固件升级服务	10
<b>4.2</b>	构建使用蓝牙 LE OTA 服务管理器的应用	13
<b>5</b>	<b>缩略语列表</b>	<b>16</b>
	<b>版本历史</b>	<b>17</b>

## 表格索引

表 1.....	OTA 固件升级的硬件和软件资源	9
表 2. ....	具有 OTA 固件升级功能的 Sensor Demo IAR 工作区.....	10
表 3. ....	具有 OTA 固件升级功能的 BLE_SerialPort 演示 IAR 工作区.....	10
表 4. ....	本文缩略语列表 .....	16
表 5. ....	文档版本历史 .....	17

## 图片目录

图 1.....	OTA 客户端将映像数据发送到 OTA 服务器	2
图 2.	OTA_packet_structure.....	4
图 3.	蓝牙 LE OTA 服务固件升级架构 .....	5
图 4.	具有 OTA 服务的低层和高层应用 .....	6
图 5.	OTA 服务管理器 Flash 存储器布局 .....	7
图 6.	OTA 过程: OTA 自举程序窗口 .....	11
图 7.	OTA 过程: 搜索设备并连接.....	12
图 8.	OTA 过程: 自举程序升级 .....	12
图 9.	OTA 过程: 自举程序升级完成.....	13
图 10.	OTA 服务管理器过程: OTA 自举程序窗口 .....	14
图 11.	OTA 服务管理器过程: 搜索设备并连接.....	14
图 12.	OTA 服务管理器过程: 自举程序升级 .....	15
图 13.	OTA 服务管理器过程: 自举程序升级完成 .....	15

#### 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 ST 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。

ST 和 ST 标志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](http://www.st.com/trademarks)。其他所有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。

© 2023 STMicroelectronics - 保留所有权利