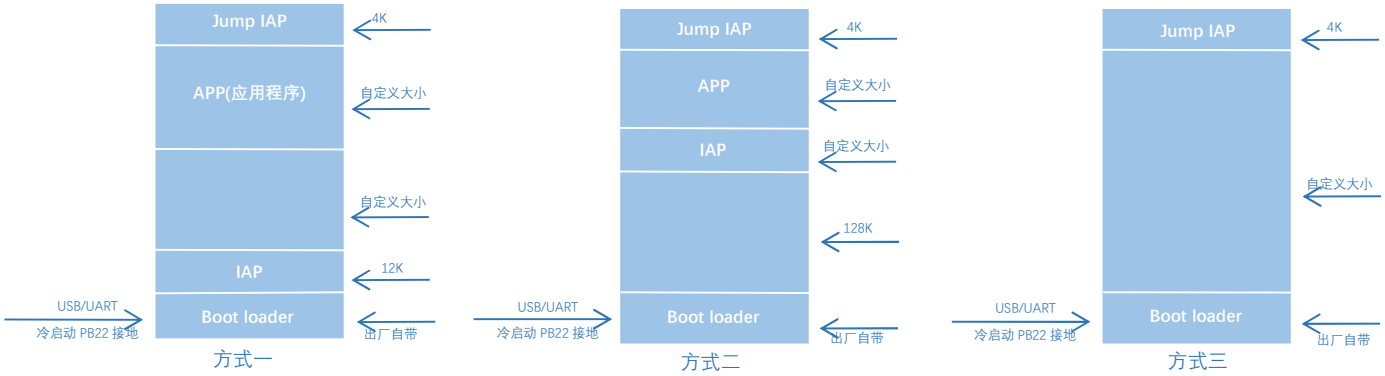
WCH 蓝牙空中升级（BLE OTA）

v1.2

1. 概述

DFU（Device Firmware Update）设备固件升级，OTA（Over The Air）是实现 DFU 的一种方式，OTA 的全称应该是 OTA DFU，即通过空中无线方式实现设备固件升级。OTA 也可以称为 FOTA，即 Firmware OTA。WCH BLE 系列芯片除了可以通过无线方式（OTA）**-方式一/二 DFU** 进行升级，也可以通过有线方式**-方式三 DFU** 进行升级，比如通过内置 BOOT（UART/USB）来升级设备固件。

不管采用 OTA 方式还是有线通信方式，DFU 包括后台式（background）和非后台式两种模式。**后台式 DFU-类似方式一 DFU**，又称静默式 DFU（Silent DFU），即新固件下载属于应用程序功能的一部分，在新固件下载过程中，应用可以正常使用，下载完成后，系统完成执行新固件的操作，至此整个升级过程结束（比如 EVT/BLE/BackupUpgrade_XXX 例子）。**非后台式 DFU-方式二 DFU**，在升级的时候整个升级过程中 APP 正常功能都无法使用。系统需要先从应用模式跳入到 BootLoader/IAP 模式，由 BootLoader/IAP 进行新固件下载工作，直接覆盖老固件，至升级结束（比如 EVT\EXAM\BLE\OnlyUpdateApp_XXX 例子）。



2. WCH BLE SDK DFU 工作原理

2.1 方式一 DFU 说明（无线升级）

备份升级方式，适用于 flash 资源充裕的应用，优点是 APP+LIB 都可以升级，缺点是 flash 需要对半分使用。

方式一上电优先运行 IAP 程序，之后跳转 APP 执行用户程序。APP 文件为独立完整的功能文件，运行时可以通过无线方式接收完整的 OTA 备份升级文件，然后软复位进入 IAP 程序，IAP 会将备份区的 OTA 升级文件拷贝到 APP 应用程序区，最后跳转回升级后的 APP 应用程序运行新的固件。升级固件带 LIB 编译（LIB 约 90K）。

```
/* 整个用户code区分成四块，4K，216K，216K，12K，后三块下面分别叫做imageA（APP），imageB（OTA）和imageIAP */
```

比如 EVT\EXAM\BLE\BackupUpgrade_OTA 的升级例程。

```
void ReadImageFlag( void )
```

读取 dataflash OTA_DATAFLASH_ADD 位置的值，更新当前的 flag 标志为 APP。

主要看\EXAM\BLE\BackupUpgrade_OTA\APP\Peripheral.c 下 OTA 升级用到的几个升级函数，其他应答返回都有函数说明不做过多解释。

```
void Rec_OTA_IAP_DataDeal(void)
```

完成对接收的 OTA 包进行处理，包含编程、擦除、校验、结束指令，命令定义在 EXAM\BLE\BackupUpgrade_OTA\APP\include\OTA.h 中。

在 `void Peripheral_Init( )` 函数中 304 行注册 Peripheral_OTA_IAPProfileCBs 里包含 OTA_IAPWriteData()函数，此函数会调用 Rec_OTA_IAP_DataDeal()；

```
static bStatus_t OTAProfile_WriteAttrCB( uint16 connHandle, gattAttribute_t *pAttr,
                                         uint8 *pValue, uint16 len, uint16 offset,uint8 method  )
```

在这个函数中接收数据

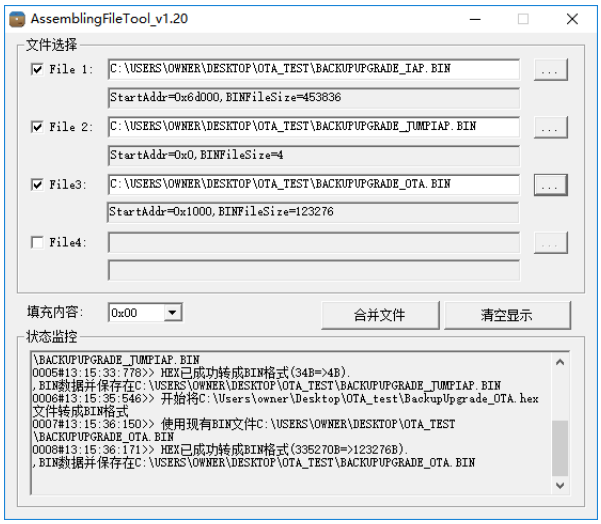
```
306   if(OTAProfileWriteLen && OTAProfile_AppCBs && OTAProfile_AppCBs->pfnOTAProfileWrite)
307   {
308     OTAProfile_AppCBs->pfnOTAProfileWrite(OTAPROFILE_CHAR,OTAProfileWriteBuf,OTAProfileWriteLen);
309     OTAProfileWriteLen = 0;
310   }
```

在这个地方调用 Rec_OTA_IAP_DataDeal()函数处理，至升级完成。

升级用的APP软件,目前提供了安卓版本的,需要把编译产生的hex文件放到Image_A文件夹下,触发OTA后,Image_A文件按钮亮，可以点击开始升级。

2.1.1 方式一 DFU 固件烧录说明

方式一 DFU 包含 3 个文件 JumpIAP + APP + IAP（APP 是用户功能代码，也是实现产品功能和升级功能的主体，对应 BackupUpgrade_OTA 产生的 hex 文件；IAP 是编程升级 APP 的代码，对应 BackupUpgrade_IAP 产生的 hex 文件；JumpIAP 为跳转 IAP 代码，对应 BackupUpgrade_JumpIAP 产生的 hex 文件）。



选择对应的文件，点击合并，产生一个 BIN 文件，然后使用 ISP 工具下载即可。

2.2 方式二 DFU 说明（无线升级）

升级方式二采用 APP+IAP+LIB 的方式，适用于 flash 资源比较紧凑的应用，优点是节省 flash，缺点是 LIB 固定的，无法升级，如果遇到 LIB 需要升级的情况，只能通过方式三进行全升级。

方式二上电优先运行 IAP 程序，之后由 IAP 跳转 APP 执行用户程序。升级时由 APP 触发升级跳转到 IAP 程序，IAP 通过无线方式接收升级固件并写入 APP 用户代码区，升级完成后跳转 APP 执行新的用户程序。

```
20 /* 整个用户code区分成四块，依次为4K，44K，16K，128K 后三块分别叫做imageA（APP），imageB（IAP），LIB */
```

方式二 OTA 提供完整的演示 demo，APP - EVT\EXAM\BLE\OnlyUpdateApp_Peripheral，仿用户功能文件。

IAP - EVT\EXAM\BLE\OnlyUpdateApp_IAP 升级文件，可以用来升级 APP。

LIB 文件在 EVT\EXAM\BLE\LIB 文件夹下，CHxxxBLE_ROM 文件。

使用固定库的程序使用的 RAM 范围有所变动，只能使用后 14K。

```
6     RAM (xrw) : ORIGIN = 0x20004800, LENGTH = 14K
```

在 EVT\EXAM\BLE\OnlyUpdateApp_Peripheral 中，进入 OTA 升级模式的具体步骤如下：

0xFFE3 通道下传数据，触发 OTA 升级条件（条件可以自定义），然后软复位进入 IAP 程序执行升级流程。

```
629 static void simpleProfileChangeCB( uint8 paramID, uint8 *pValue, uint16 len )
630 {
631
632   switch( paramID )
633   {
634     case SIMPLEPROFILE_CHAR1:
635     {
636       uint8 newValue[SIMPLEPROFILE_CHAR1_LEN];
637       tmos_memcpy( newValue, pValue, len );
638       PRINT("profile ChangeCB CHAR1.. \n");
639       break;
640     }
641
642     case SIMPLEPROFILE_CHAR3:
643     {
644       uint8 newValue[SIMPLEPROFILE_CHAR3_LEN];
645       tmos_memcpy( newValue, pValue, len );
646       PRINT("profile ChangeCB CHAR3..\n");
647       PRINT("jump OTA \n");
648       mDelaymS(5);
649       Jump_OTA();
650       break;
651     }
```

EXAM\BLE\OnlyUpdateApp_IAP 例子负责接收升级包升级 APP 区域，升级完成后跳转执行 APP 代码。

```
void Peripheral_Init( )
```

在这个函数中注册回调函数

```
// Register callback with OTAGATTprofile
OTAProfile_RegisterAppCBs( &Peripheral_OTA_IAPProfileCBs );
```

```
static bStatus_t OTAProfile_WriteAttrCB( uint16 connHandle, gattAttribute_t *pAttr,
                                         uint8 *pValue, uint16 len, uint16 offset,uint8 method )
```

接收手机发下来的数据，

```
if(OTAProfileWriteLen && OTAProfile_AppCBs && OTAProfile_AppCBs->pfnOTAProfileWrite)
{
  OTAProfile_AppCBs->pfnOTAProfileWrite(OTAPROFILE_CHAR,OTAProfileWriteBuf,OTAProfileWriteLen);
  OTAProfileWriteLen = 0;
}
```

处理收到的 OTA 包，至升级完成。

升级用的 APP 软件，目前提供了安卓版本的，需要把编译产生的 hex 文件放到的 Image-A 文件夹下，触发 OTA 后，点击开始升级，至提示成功。

2.2.1 方式二 DFU 固件烧录说明

方式二 DFU 包含 4 个文件 JumpAPP + APP + IAP + LIB（APP 是用户功能代码，也是实现产品功能的主体，对应 OnlyUpdateApp_Peripheral 产生的 hex 文件;IAP 是升级 APP 的代码,对应 OnlyUpdateApp_IAP 产生的 hex 文件;JumpIAP 为跳转 IAP 代码，对应 OnlyUpdateApp_JumpIAP 产生的 hex 文件；LIB 就是提供的 LIB-ROM 文件）。

选择对应的文件，点击合并，产生一个 BIN 文件，然后使用 ISP 工具下载即可。

2.3 方式三 DFU 说明（有线升级）

冷启动 PB22 接地进入 BOOT 程序，使用 USB（PB10/PB11）和 UART（PA8PA9），然后可以通过 ISP 工具进行升级。

2.4 OTA 安卓 APP

官网下载 BLE_OTA_Android.ZIP

2.5 APP 合并工具

官网下载 WCH_AssemblingFileTool