

SDK OTA 设计文档

版本	修改内容	日期
1.0	新建	2025/1/15

总体流程

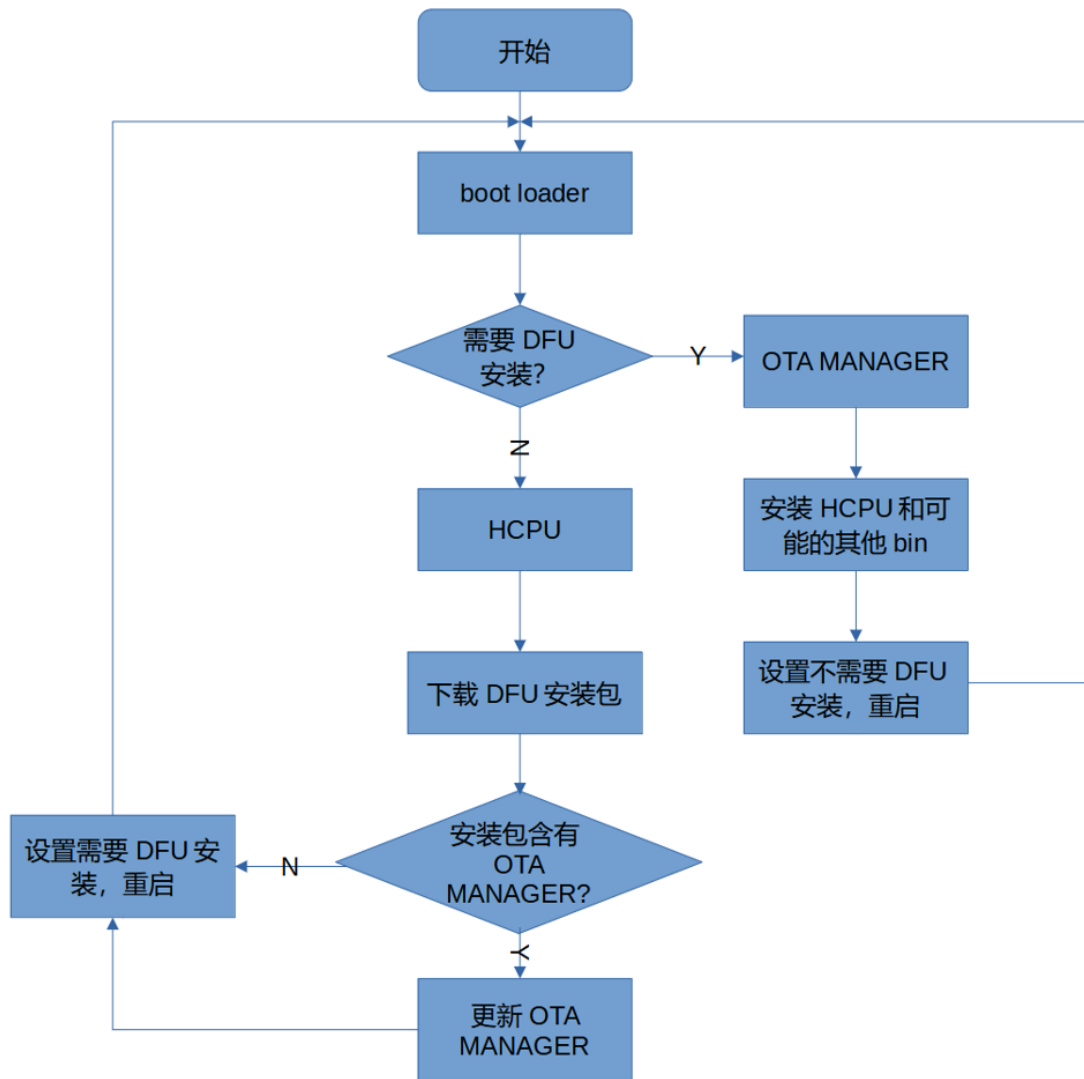
FTAB	BOOT LOADER	HCPU	OTA MANAGER	DFU DOWNLOAD BUFFER	DFU NV	BLE NV	EXTRA BIN 1	EXTRA BIN 2
------	----------------	------	----------------	------------------------	-----------	-----------	----------------	----------------

Flash 排布大致如上图

正常运行开机时，boot loader 运行后，跳转到 HCPU，执行当前用户代码。

升级步骤如下：

1. 当需要升级时，在 HCPU 下载 DFU 安装包到 dfu download buffer 区间。
2. 下载完成后，如果安装包中包含 ota manager，则先更新 ota manager。
3. 更新 ota manager 完成后或者不含 ota manager 时，板子会重启。
4. 重启后会运行 ota manager，然后把 DFU 安装包中的内容，安装到对应 bin 的区域。
5. 安装完成后再次重启，重启后运行 HCPU，升级完成。



安装包结构

OFFLINE V1

早期组合安装包，用于微克-咕咚

Offset	Length	Content
0	4	Magic(0x46, 0x43, 0x 45, 0x53)
4	1	Image count, 包含 ctrl packet
5	4	Id+image length 域的长度
9	1	第一个 Image 的 id 吗, (第一个 image 是 ctrl packet)
10	4	第一个 Image 的长度, 即 ctrl packet 的长度
14	1	第二个 image 的 id
15	4	第二个 image 的长度, (压缩后)

		...
		Ctrl packet
		Image1
		...

OFFLINE V2

SDK 的组合安装包，用于 SDK 工程 DFU

Offset	Length	Content
0	4	Magic(0x46, 0x43, 0x 45, 0x53)
4	1	安装包的协议版本
5	1	安装 flag, 0xFF, 见 Boot loader 跳转逻辑
6	2	Image count, 不含 ctrl packet
8	4	所有 image 内容一起 (image1+image2+...), 做 CRC32MPEG2 的结果
12	1	第一个 image 的 id
13	1	第一个 image 的 flag
14	4	第一个 image 的长度
18	1	第二个 image 的 id
19	1	第二个 image 的 flag
20	4	第二个 image 的长度
		...
		Image1
		Image2
		...

安装包制作

```
run imgtool_new.py gen_dfu --img_para hcpu 16 0 ota 16 6 --key=s01 --sigkey=sig --
dfu_id=1 --hw_ver=51 --sdk_ver=7001 --fw_ver=1001001 --com_type=0 --offline_img=2
```

如上，是使用压缩的方式，制作 hcpu 和 ota manager。

第一个是 bin 的名字，第二个是 image flag，第三个是 image id

如果不用压缩的方式，image flag 填 0

目前按照 flash id 和 ptab.json 中 image 地址对应的方式，来确定 bin 的安装地址。例如 flash id 0 是 hcpu，hcpu 则对应 HCPU_FLASH_CODE_START_ADDR 的地址，flash id 6 是 ota manager，对应 DFU_FLASH_CODE_START_ADDR 的地址。

如果需要升级其他的 bin，则要在 dfu_flash.c 中，添加或者修改新的 image id 和地址对应逻辑

辑，然后更新 ota manager。

TODO：直接指定下载地址进行升级。

TODO：加密 bin

Boot loader 跳转

Offline v2 中，在 boot loader 中，默认是通过 RTC 寄存器决定运行 ota manager 还是 hcpu。如果发生安装中断电重启，RTC 寄存器都会被清除，需要借助安装 FLAG 来保证运行到 ota manager。

安装 FLAG 生成后是 0xFF，当在 ota manager 中开始安装其他 bin 之后，将安装 flag 写为 0x7F (0111 1111)。

后续启动中，如果 boot loader 读到 MAGIC 符合预期，且安装 flag 是 0x7F，boot loader 也会执行 ota manager。

安装结束后，将 flag 写为 0x3F (0011 1111)。

注：如果重复安装已经安装过的升级包，该保护将失效，因为 0x3F 不能直接写成 0x7F，nor flash 只能把 1 写成 0。

TODO: 可以考虑修改为，在 HCPU 中开始安装时，安装 flag 不为 0xFF 的安装包，拒绝安装。

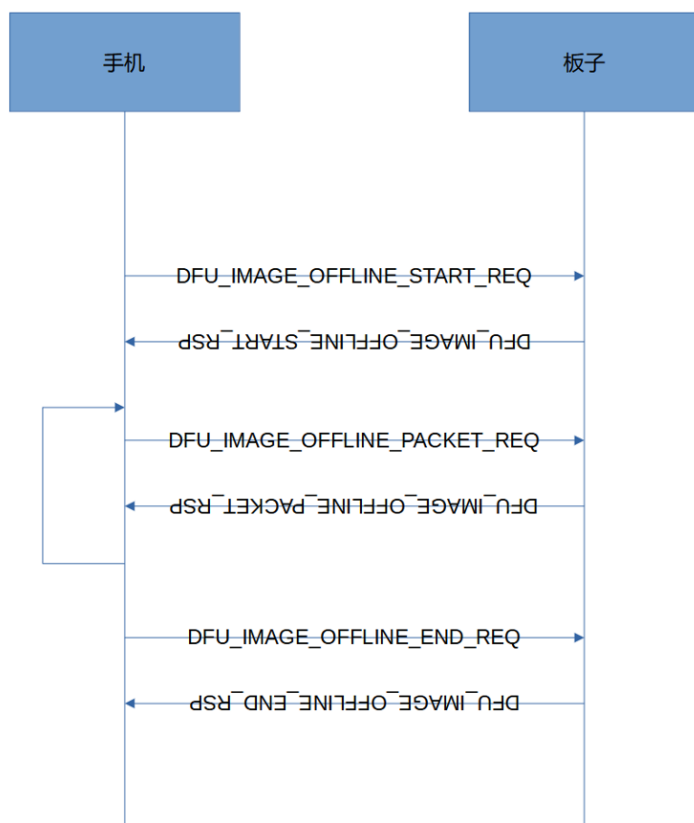
下载协议

下载和安装进行了分离，用户可以自行进行下载，也可以使用 SDK 支持的方式进行下载。

BLE

总体流程如下：

1. 手机先发送 DFU_IMAGE_OFFLINE_START_REQ 开始，携带安装包的相关信息。
2. 板子回复 DFU_IMAGE_OFFLINE_START_RSP，告知续传信息。
3. 手机将 DFU 安装包拆分成若干个小包，每一包都构建一个 DFU_IMAGE_OFFLINE_PACKET_REQ 命令，发送给板子。
4. 板子收到每一个 DFU_IMAGE_OFFLINE_PACKET_REQ 之后，都会回复 DFU_IMAGE_OFFLINE_PACKET_RSP，手机收到 RSP 之后，再发下一个 DFU_IMAGE_OFFLINE_PACKET_REQ，循环直到 DFU 安装包发送完毕。
5. 手机发送 DFU_IMAGE_OFFLINE_END_REQ，板子收到后，进行校验，结束后发送 DFU_IMAGE_OFFLINE_END_RSP。
6. 开始安装流程。



命令详细内容：

DFU_IMAGE_OFFLINE_START_REQ

域	Message id	Length	File length	Packet count	CRC value
值	38	12			
长度	2	2	4	4	4

File len：文件总长

Packet count：文件按照 2048 长度拆分，共有多少包

CRC value：从文件中读取的 CRC 值，文件格式见安装包结构-OFFLINE_V2，需要从文件中解析

DFU_IMAGE_OFFLINE_START_RSP

域	Message id	Length	Result	Reserved	Completed count
值	39	6			
长度	2	2	2	2	4

Result：为 0 则开始后续传输，其他值为失败

Completed count：已完成包数，用于续传。代表手表已收到的包，手机需要从收到的 count+1 开始传输。如果 completed count 等于 packet count，则手机跳过发包，接下来只需要发送 DFU_IMAGE_OFFLINE_END_REQ

DFU_IMAGE_OFFLINE_PACKET_REQ

域	Message id	Length	Packet index	Data length	crc	data
---	------------	--------	--------------	-------------	-----	------

值	40	12 + x		x		
长度	2	2	4	4	4	x

Packet index：手机把整个文件按照 2048 的长度进行拆分，发送时添加 index，index 从 1 开始

Data length：data 段的长度，除了最后一包的长度可能短一些，其他应该都是 2048

Crc：data 段的数据做 CRC32-MPEG2 之后的结果，每一包都需要手机计算添加。

Data：本段 data。

每一包 packet req 发送后，都要等到 packet rsp 之后，再发送下一个 packet req

DFU_IMAGE_OFFLINE_PACKET_RSP

域	Message id	Length	Result	Retransmission	Reserved	Completed count
值	41		0			
长度	2	2	2	1	1	4

Result：0 代表成功，其他代表异常

Retransmission：当 result 不为 0 时，检查该位，如果为 1，则手机需要从指定包重传。

如果 result 不为 0，retransmission 为 0，则失败退出。

Completed count：当 retransmission 为 1 时，为手表已完成的包数，需要从 count+1 进行续传

DFU_IMAGE_OFFLINE_END_REQ

域	Message id	Length	Reserved
值	42		
长度	2	2	2

手机发送完所有数据包，收到最后一个 packet rsp 之后，或者在不需要发包的情况下收到 start rsp 之后，再发送该命令，代表发送结束。

DFU_IMAGE_OFFLINE_END_RSP

域	Message id	Length	Result
值	43		
长度	2	2	2

手表回复结束，result 为 0 为成功，其他失败

PAN

TODO:

SPP

TODO:

UART

TODO:

安装

HCPU 中的安装流程

1. 检查 MAGIC，计算 CRC（规则见安装包结构），检验安装包的合法性和完整性。
2. 如果有安装包中有 ota manager，则安装 ota manager。
 - 1) 擦除原 ota manager
 - 2) 如果是非压缩的 bin，直接将 dfu 安装包对应 image 的内容，复制到目标区域。
 - 3) 如果是压缩的 bin，则解压然后写到对应区域。
3. 更新 DFU NV
4. 更新 RTC 寄存器，重启

OTA MANAGER 中的安装流程

1. 检查 MAGIC，计算 CRC（规则见安装包结构），检验安装包的合法性和完整性
2. 安装除了 ota manager 之外的所有 bin，安装处理同 hcpu 中的安装。
3. 更新 DFU NV
4. 更新 RTC 寄存器，重启

TODO：使用差分算法进行安装