

# WM\_W800\_QFLASH 布局说明

V1.1

北京联盛德微电子有限责任公司 (winner micro)

地址：北京市海淀区阜成路 67 号银都大厦 18 层

电话：+86-10-62161900

公司网址：[www.winnermicro.com](http://www.winnermicro.com)

## 文档修改记录

版本	修订时间	修订记录	作者	审核
V0.1	2019/9/25	[C]创建文档	Cuiyc	
V0.2	2020/7/8	统一字体	Cuiyc	
V1.0	2020/8/10	升级版本号	Cuiyc	
V1.1	2021/2/23	更新用户区位置, 与 SDK 保持一致	Cuiyc	

## 目录

文档修改记录 .....	2
目录 .....	3
1 引言 .....	5
1.1 编写目的 .....	5
1.2 预期读者 .....	5
1.3 术语定义 .....	5
1.4 参考资料 .....	5
2 W800 QFLASH 的布局 .....	6
2.1 QFLASH 大于 2M 的布局 .....	6
2.1.1 物理层参数区 .....	6
2.1.2 SECBOOT 参数区 .....	7
2.1.3 SECBOOT 存放区 .....	8
2.1.4 升级 IMG 存放区 .....	8
2.1.5 运行 IMG 参数区 .....	9
2.1.6 运行 IMG 存放区 .....	10
2.1.7 用户参数区 .....	10
2.1.8 系统参数区 .....	10
2.1.9 升级 IMG 参数区 .....	11
2.2 QFLASH 小于 2M 的布局 .....	11
3 FAQ .....	14
3.1 为什么布局划分总是以 64KB 为倍数划分? .....	14

3.2 为什么总是留一部分升级区在内部 Flash 里? ..... 14

WinnerMicro

## 1 引言

### 1.1 编写目的

本文档主要用于阐述 W800 中的 QFLASH 布局，使读者了解当前 W800 的 QFLASH 的使用情况。

### 1.2 预期读者

该文档适用的读者包括研发人员、测试人员、W800 的工程使用人员等。

### 1.3 术语定义

序号	术语/缩略语	说明/定义
1	QFLASH	W800 internal Quad-SPI FLASH
2	IMG	IMAGE
3	RF	Radio Frequency
4	MAC	Media Access Control
5	SECBOOT	Second Boot
6	ROM	Read-Only Memory
7	UPD	Image Upgrade Area
8	MB	Mega Byte
9	KB	Kilo Byte

### 1.4 参考资料

无

## 2 W800 QFLASH 的布局

地址空间: 0x8000000-0x8XFFFFFF, 共(X+1)MB, X >= 1, 针对 2M 及以上的 QFLASH。

### 2.1 QFLASH 大于 2M 的布局

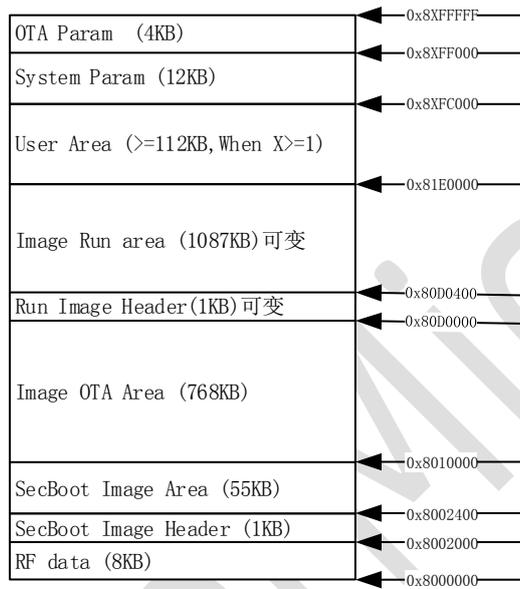


图 2-1 升级 Image 为压缩格式

#### 2.1.1 物理层参数区

地址空间: 0x8000000-0x8001FFF, 共 8KB

参数内容:

系统 RF 及 MAC 相关参数。

参数布局:

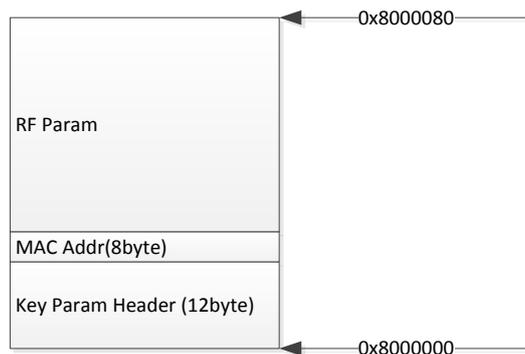


图 2-3

### 2.1.2 SECBOOT 参数区

地址空间：0x8002000-0x80023FF，共 1KB

参数内容：

SECBOOT 启动校验相关信息及启动地址

参数布局：

字段	描述
magic_no	魔术字，固定值 0xA0FFFF9F
img_attr	Img_Attr_Type, IMAGE Attribute
img_addr	Image area 在 flash 中的位置，运行位置
img_len	Image area 的字节数长度
img_header_addr	IMAGE header 在 flash 中的位置
upgrade_img_addr	升级区地址，升级 IMAGE header 在 flash 中存放位置
org_checksum	Image area 的 crc32 结果
upd_no	升级版本号，值较大的表示版本较新；当版本号为 0xFFFFFFFF 时，可升级任意版本号固件
ver	Image 版本号，字符串
next	下一个 image header 在 flash 中的位置
hd_checksum	Image header 的以上字段的 crc32 的值

W800 的 IMAGE Attribute 字段描述：

字段	Bit	描述
----	-----	----

img_type	4	0x0: SECBOOT; 0xE: ft 测试程序; 其它值: 用户自定义
code_encrypt	1	0: 固件明文存储; 1: 固件由客户加密后存储
pricey_sel	3	芯片内置 8 组 RSA 私钥用于解密固件加密的密钥, 用户可任选一组使用, 取值范围 0~7
signature	1	0: IMAGE 不包含签名部分; 1: IMAGE 包含 128Bytes 签名
zip_type	1	0: 不压缩; 1: image area 部分为压缩档
reserved	1	保留
erase_block_en	1	0: 不支持 64KB Block 擦除; 1: 支持 Block 擦除
erase_always	1	0: Sector 或 Block 擦除前检查 flash 是否全 F, 全 F 的 Sector 或 Block 不进行擦除操作; 1: 总是先擦后写

### 2.1.3 SECBOOT 存放区

地址空间: 0x8002400-0x800FFFF, 共 55KB

参数内容:

SECBOOT IMAGE 内容

参数布局:

平铺的 SECBOOT IMAGE, 可为加密文件

### 2.1.4 升级 IMG 存放区

地址空间:

0x8010000-0x80CFFFF, 共 768KB

参数内容:

OTA 升级 IMAGE 文件 (可为 secboot, User Image)

参数布局:

### 2.1.5 运行 IMG 参数区

地址空间: 0x80D0000-0x80D03FF, 共 1KB

参数内容:

运行区 IMAGE 启动校验相关信息及启动地址

参数布局:

字段	描述
magic_no	魔术字, 固定值 0xA0FFFF9F
img_attr	Img_Attr_Type, IMAGE Attribute
img_addr	Image area 在 flash 中的位置, 运行位置
img_len	Image area 的字节数长度
img_header_addr	IMAGE header 在 flash 中的位置
upgrade_img_addr	升级区地址, 升级 IMAGE header 在 flash 中存放位置
org_checksum	Image area 的 crc32 结果
upd_no	升级版本号, 值较大的表示版本较新; 当版本号为 0xFFFFFFFF 时, 可升级任意版本号固件
ver	Image 版本号, 字符串
next	下一个 image header 在 flash 中的位置

hd_checksum	Image header 的以上字段的 crc32 的值
-------------	------------------------------

### 2.1.6 运行 IMG 存放区

地址空间:

0x80D0400-0x81DFFFF, 共 1087KB

参数内容:

平铺的运行时 IMAGE

参数布局:

### 2.1.7 用户参数区

地址空间: 0x81E0000-0x8XFBFFF, 共 (X+1) MB - 1808KB, X >=1。

参数内容:

用于用户存放自定义参数时使用。

用户可用参数区大小与用户 Image 空间大小相关

参数布局:

用户自定义

### 2.1.8 系统参数区

地址空间: 0x8XFC000-0x8XFEFFF, 共 12KB

参数内容:

系统运行时所需的相关参数

参数布局:

MAGIC Number:4Byte	
PARTITION_NUM:2Byte	MODIFY_CNT:2Byte
RESERVED:4Byte	
RESERVED:2Byte	Length:2Byte(整个参数的大小, 包含 CRC 值, 由系统参数决定)
Data Content(系统参数决定)	
CRC Value:4byte (CRC 之前的内容的值)	

- 1) 系统参数 1 区 (0x8XFC000-0x8XFCFFF)
- 2) 系统参数 2 区 (0x8XFD000-0x8XFDFFF)
- 3) 系统参数 3 区 (0x8XFE000-0x8XFEFFF)

### 2.1.9 升级 IMG 参数区

地址空间: 0x8XFF000-0x8XFFFFF, 共 4KB

参数内容:

OTA 升级 IMAGE 校验信息, 用于区分是否 OTA。

SECBOOT 搬移 OTA 固件后改写。

参数布局:

### 2.2 QFLASH 小于 2M 的布局

针对上述的不同 Size, QFlash 的布局会不同, 以 1MB 举例如下。

- 1) <2MB, 不考虑 OTA 升级的场景

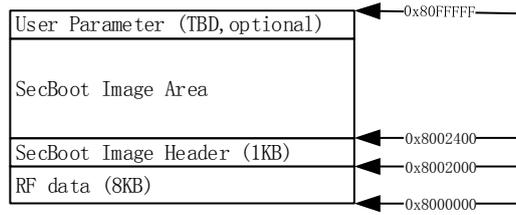


图 3-1

2) <2MB, 考虑 OTA 升级的场景

(1) QFlash 空间够, 则布局如下:

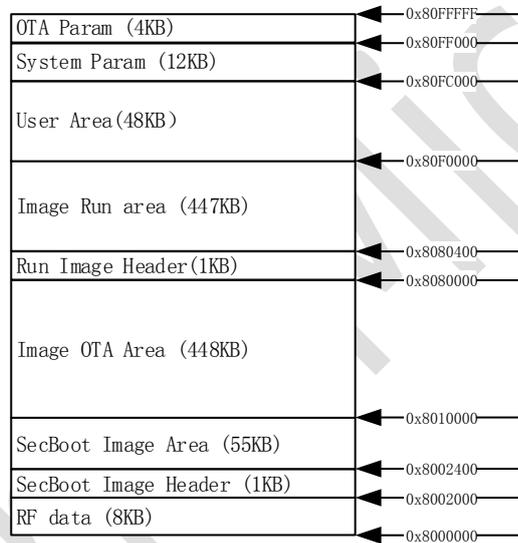


图 3-2

(2) QFlash 空间不足够, 则布局如下, 部分 OTA 区域要放置到内部 QFlash, 部分 OTA 和全部用户区都放到外部存储设备:

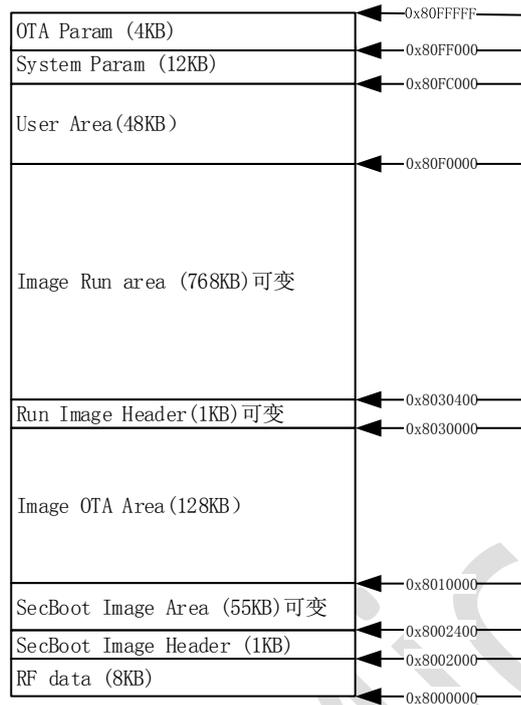


图 3-3

如下是针对不同 Flash Size 和基本功能支持情况做的划分。

SIZE	功能			应用场景
	Wi-Fi 使用	BL/BLE	OTA	
16KB	基本收发功能	基本收发功能	不支持	
32KB	基本收发功能	基本收发功能	不支持	
64KB	基本收发功能	基本收发功能	不支持	
128KB	基本收发功能	基本收发功能	不支持	
256KB	基本收发功能	基本收发功能	不支持	
512KB	Wi-Fi 所有功能	不确定	有条件支持	
1MB	Wi-Fi 所有功能	基本功能	有条件支持	
>=2MB	Wi-Fi 所有功能	基本功能	支持	

注：

有条件支持：内部 Flash 基本都划分为代码空间，要通过外挂存储设备才可实现 OTA 固件的存储。

支持： 内部存储空间已经满足运行区和 OTA 区域

不支持：内部存储空间不足以支撑 OTA 相关代码(Wi-Fi+OTA 应用，蓝牙+OTA 应用)的运行。

## 3 FAQ

### 3.1 为什么布局划分总是以 64KB 为倍数划分？

考虑到 QFlash 的实现方式不同，针对掉电过程中，如果有 QFlash 的写动作，可能会破坏整个扇区的操作。

### 3.2 为什么总是留一部分升级区在内部 Flash 里？

因为 ROM 里总是认定 SECBOOT 的升级区域在内部 QFlash 里。

为了预防 SECBOOT 升级，必须把 OTA 区域预留在内部 QFlash 里。