WM_W800_ROM 功能简述

V1.0

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

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	

目录

1 引言

1.1 概述

本文档是对 W800 的 ROM 功能及使用说明进行简单描述，供开发者和设计者理解 W800 的 ROM 功能。

1.2 术语定义

术语	定义
CRC	Cyclic Redundancy Check
IMAGE	Binary File
MAC	Medium Access Control
QFLASH	Quad-SPI Flash
RAM	Read-Write Memory
ROM	Read-Only Memory
SECBOOT	Second Boot
UART	Universal asynchronous receiver-transmitter

1.3 文献索引

2 ROM 基本功能

2.1 ROM 流程图

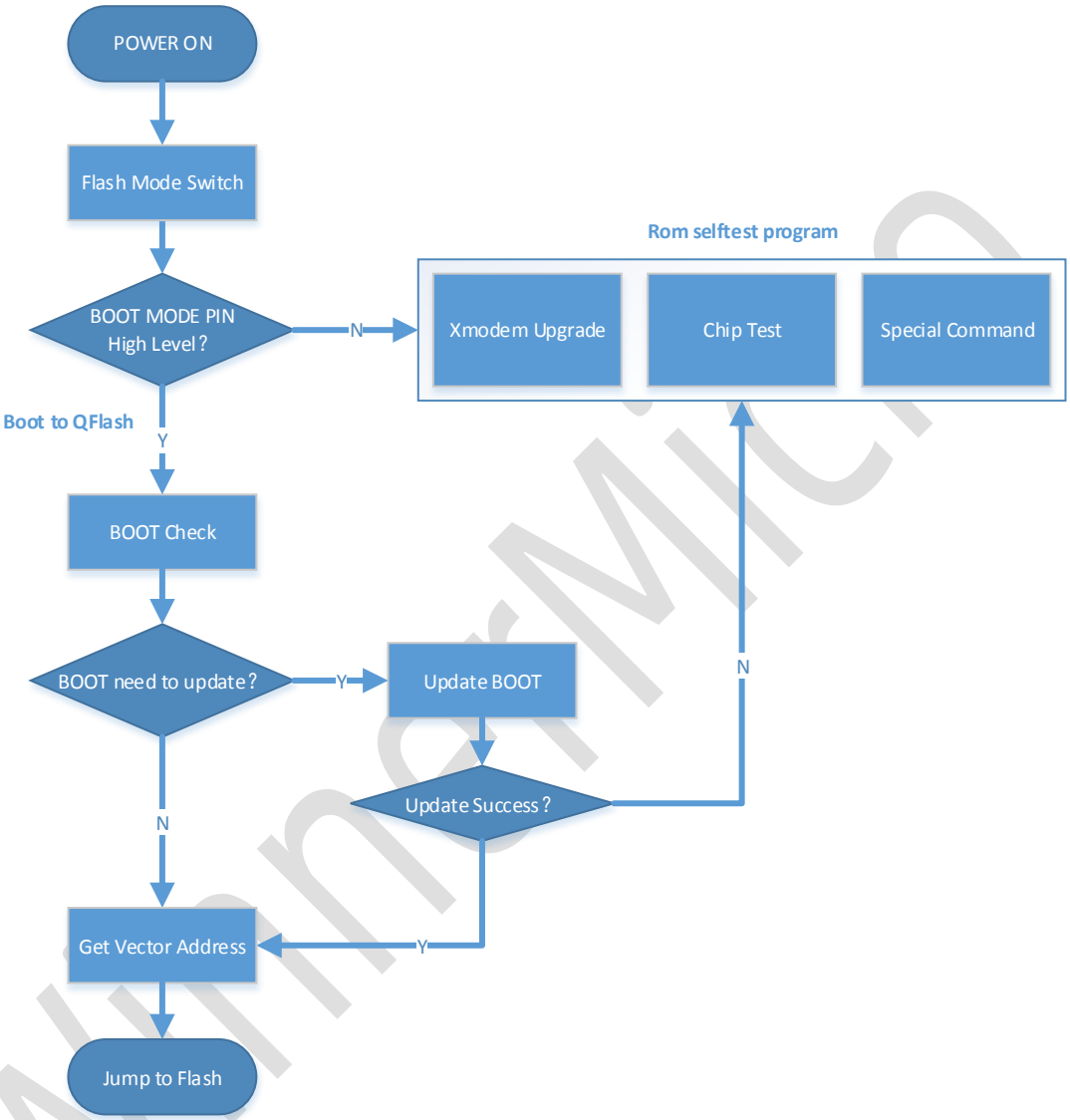

图 2-1

2.2 引导程序

2.2.1 QFLASH 自检

完成 QFLASH 工作状态检查

2.2.2 QFLASH 模式切换

ROM 启动后，QFLASH 默认是 1 线模式。要使得程序能够运行于 QFLASH，ROM 需要把 QFLASH 切换到 4 线模式。

2.2.3 IMAGE 校验

完成 IMAGE 头校验和 IMAGE 内容校验

2.2.4 向量表重定向

W800 的程序最终是要运行在 QFLASH 里（代码的运行基址：0x8000000），因此需要对向量表进行重定向。

重定向地址规则：（异常向量+中断）总共是 64 个 word，根据 VBR 寄存器的要求，向量表地址必须是 0x400 的整数倍。

2.3 升级程序

利用 Xmodem 协议实现把 IMAGE 升级到 QFLASH 或内存区域，升级到内存区域的 Image 在升级完成后即跳转到内存执行，升级的 FLASH 的需要重启后跳转执行。

升级 IMAGE 格式：

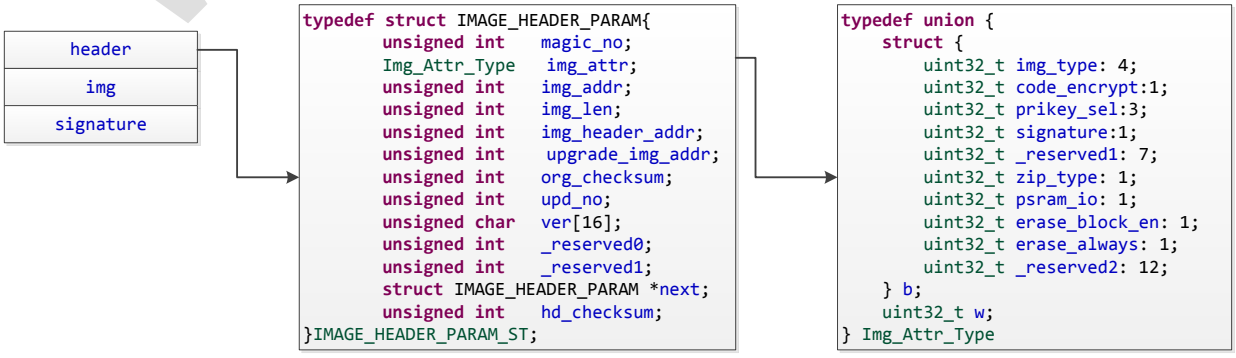

图 2-2

W800 的 IMAGE 包括 header、image area 和 signature 三部分。Header 包含 magic_no、img_attr 等内容，其中 img_attr 是一个 Uint32 类型，包含 img_type、code_encrypt 等字段。

W800 的 IMAGE header 字段描述：

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秘钥，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	当前未使用
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：始终先擦后写

W800 的 Flash 区域划分：

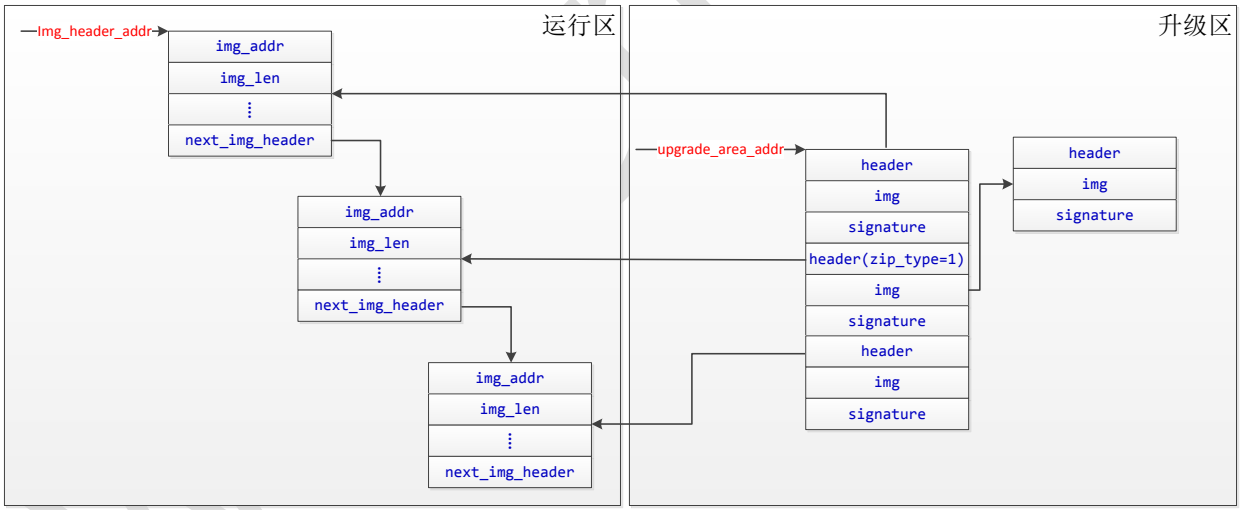

图 2-3

ROM 程序根据 upgrade_area_addr 参数，判断第一个 header 的 img_type 是否为 sec boot，如果是，在校验 header 和 img 的 crc 和签名，比较版本号，如果校验通过并且版本更新，则将 header 搬到 img_header_addr 的地址，将 img 和 signature 搬到 img_addr 的地址。

ROM 程序根据 img_header_addr 参数，找到 SECBOOT 程序的 img header，校验

img header 和 img 的 crc 和签名成功后，跳转 img_addr 执行 SECBOOT。

SECBOOT 程序根据 upgrade_area_addr 参数，依次遍历 header，直至 img_type 是 img 的 header，然后类似 ROM 程序，搬运 header 到 next_img_addr 的地址，搬运 img 和 signature 到 img_addr 的地址。

升级区可以支持包含 SECBOOT 在内的多个 img 升级,仅需要将待升级程序首尾相接放在 upgrade_area_addr 的地址即可。

对于 header 中 zip_type=1 的 img，img 部分是将原始 img 的 header+img+signature 三部分压缩后的结果，搬运前先解压。SECBOOT 不支持压缩。

2.4 OTP 参数区

W800 的 OTP 参数区存放一些有关固件升级和签名验证相关的参数。

2.5 测试程序

W800 针对芯片测试阶段的测试程序，没有放在 ROM 中，需要测试前先通过 uart xmodem 的方式升级到内存或 Flash 中运行。

2.6 操作指令

W800 的 ROM 程序支持模块生产阶段的部分操作：波特率切换，QFLASH ID 和容量获取，获取 ROM 版本，系统重启等。

指令发送方式：十六进制

2.6.1 命令列表

功能	子命令（SubCmd）	数据内容（Data Segment）	说明
波特率切换	0x31	≤2000000	波特率最大支持到 2M 设置大于 2M，报 S（命令参数错）

QFlash 擦除	0x32	4bytes	struct{
			uint16_t index;
			uint16_t count;
			};
			index:起始位置（index 最高 bit 为 1 表示 Block 擦除，为 0 表示 Sector 擦除）
			count:擦除块数

设置 BT MAC 地址	0x33	6bytes~8bytes	
获取 BT MAC 地址	0x34	无	
设置 GAIN 参数	0x35	84bytes	Wi-Fi 发射时使用的增益参数(**谨慎使用**)
获取 GAIN 参数	0x36	无	读取设置长度的 Gain 值。
设置 MAC 地址	0x37	6bytes~8bytes	
获取 MAC 地址	0x38	无	
获取上一个错误	0x3B	无	获取上一个错误信息，直到下一个操作清除。
获取 QFLASH ID 和容	0x3C	无	例如 GD 32MB 返回：FID:C8,19

量			PUYA 8MB 返回：FID:85,17
获取 ROM 版本	0x3E	无	
系统重启	0x3F	无	

2.6.2 常用指令集合

波特率变更：

2M 设置指令： 21 0a 00 ef 2a 31 00 00 00 80 84 1e 00

1M 设置指令： 21 0a 00 5e 3d 31 00 00 00 40 42 0f 00

921600 设置指令： 21 0a 00 5d 50 31 00 00 00 00 10 0e 00

460800 设置指令： 21 0a 00 07 00 31 00 00 00 00 08 07 00

115200 设置指令： 21 0a 00 97 4b 31 00 00 00 00 c2 01 00

BT MAC 地址获取： 21 06 00 D8 62 34 00 00 00

WiFi MAC 地址获取： 21 06 00 ea 2d 38 00 00 00

获取上一个错误： 21 06 00 36 B6 3B 00 00 00

QFLASH ID 和容量获取：21 06 00 1b e7 3c 00 00 00

获取 ROM 版本： 21 06 00 73 0a 3e 00 00 00

系统重启： 21 06 00 c7 7c 3f 00 00 00

QFlash 擦除(1M)： 21 0a 00 e2 25 32 00 00 00 02 00 fe 00

QFlash 擦除(2M)： 21 0a 00 c3 35 32 00 00 00 02 00 fe 01

2.7 ROM 的错误码

ROM 启动过程中，如果遇到异常，则会进入 ROM 右侧死循环程序，然后打印一个错误码，指示当前遇到的错误信息，供使用者分析遇到的问题。

错误码定义如下:

错误码	说明
C	正常
升级过程（XMODEM 协议）	
D	主机取消
F	超时没有收到数据
G	包序号错
I	IMAGE 过大
J	IMAGE 烧录地址不合法
K	IMAGE 烧录地址页不对齐
L	IMAGE 头校验错误
M	IMAGE 内容校验错
P	IMAGE 内容不完整或者签名缺失
启动过程	
N	FLASH ID 自检失败
Q	固件类型错误
L	SECBOOT 头校验错
M	SECBOOT 校验错
Y	解密读 SECBOOT 失败

Z	签名验证失败
功能模块	
R	命令校验错
S	命令参数错
T	获取 FT 参数失败（Mac 和 Gain 等）
U	设置增益失败
V	设置 MAC 失败

3 QFLASH 和 RAM 使用情况

3.1 QFLASH 布局

W800 支持四地址模式，最大支持 128MB Flash，但是，ROM 程序仅支持三地址模式，最大支持 16MB 地址访问。

ROM 视角的 QFLASH 布局：

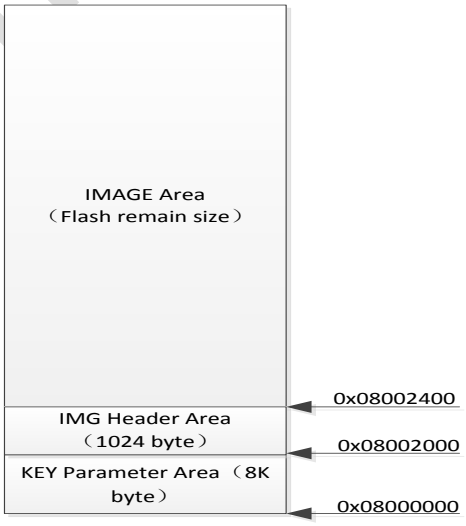

图 3-1

3.2 RAM 的使用

W800 的内存分成两块：160Kbyte 和 128Kbyte，ROM 里的分布如下：

内存块	功能	起始地址	终止地址	大小	说明
160Kbyte	Stack&Heap	0x20000000	0x20003FFF	16Kbyte	ROM 使用
	NC	0x20004000	0x20027FFF	144Kbyte	NC
128Kbyte	NC	0x20028000	0x20047FFF	128Kbyte	NC