Machine Translated by Google

Brief description of WM_W800_ROM function

V1.0

WinnerMicro

Beijing Lianshengde Microelectronics Co., Ltd. (winner micro)

Address: Floor 18, Yindu Building, No. 67, Fucheng Road, Haidian District, Beijing

Tel: +86-10-62161900

Company website: www.winnermicro.com

Machine Translated by Google

Document modification record

Version revision time	revision history	author review	
V0.1	2019/9/25 [C] Create document	Cuiyc	
V0.2	2020/7/8 unified font	Cuiyc	
V1.0	2020/8/10 Upgrade version number	Cuiyc	

WinnerMicro

Machine Translated by Google

Table of contents

Documentation Modification History 2

Table of contents..... 3

1 **Introduction** 5

1.1 Overview..... 5

1.2 Definition of Terms..... 5

1.3 Literature Index..... 5

2 ROM basic functions..... 6

2.1 ROM flow diagram..... 6

2.2 bootloader..... 6

2.2.1 QFLASH self-test..... 6

2.2.2 QFLASH mode switch..... 7

2.2.3 IMAGE verification.....7

2.2.4 Vector Table Redirection..... 7

2.3 Upgrade procedure..... 7

2.4 OTP parameter area..... 10

2.5 test program..... 10

2.6 Operating Instructions..... 10

2.6.1 command list 11

2.6.2 Commonly used instruction set..... 12

2.7 ROM error codes..... 13

3 QFLASH and RAM usage..... 14

WinnerMicro

Machine Translated by Google

3.1 QFLASH layout..... 14

3.2 RAM usage..... 15

WinnerMicro

Machine Translated by Google

1 **Introduction**

1.1 Overview

This document is a brief description of W800 ROM functions and instructions for developers and designers to understand ROM function of W800.

1.2 Definition of terms

the term	definition
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 Literature Index

WinnerMicro

Machine Translated by Google

2 ROM basic functions

2.1 ROM flow chart

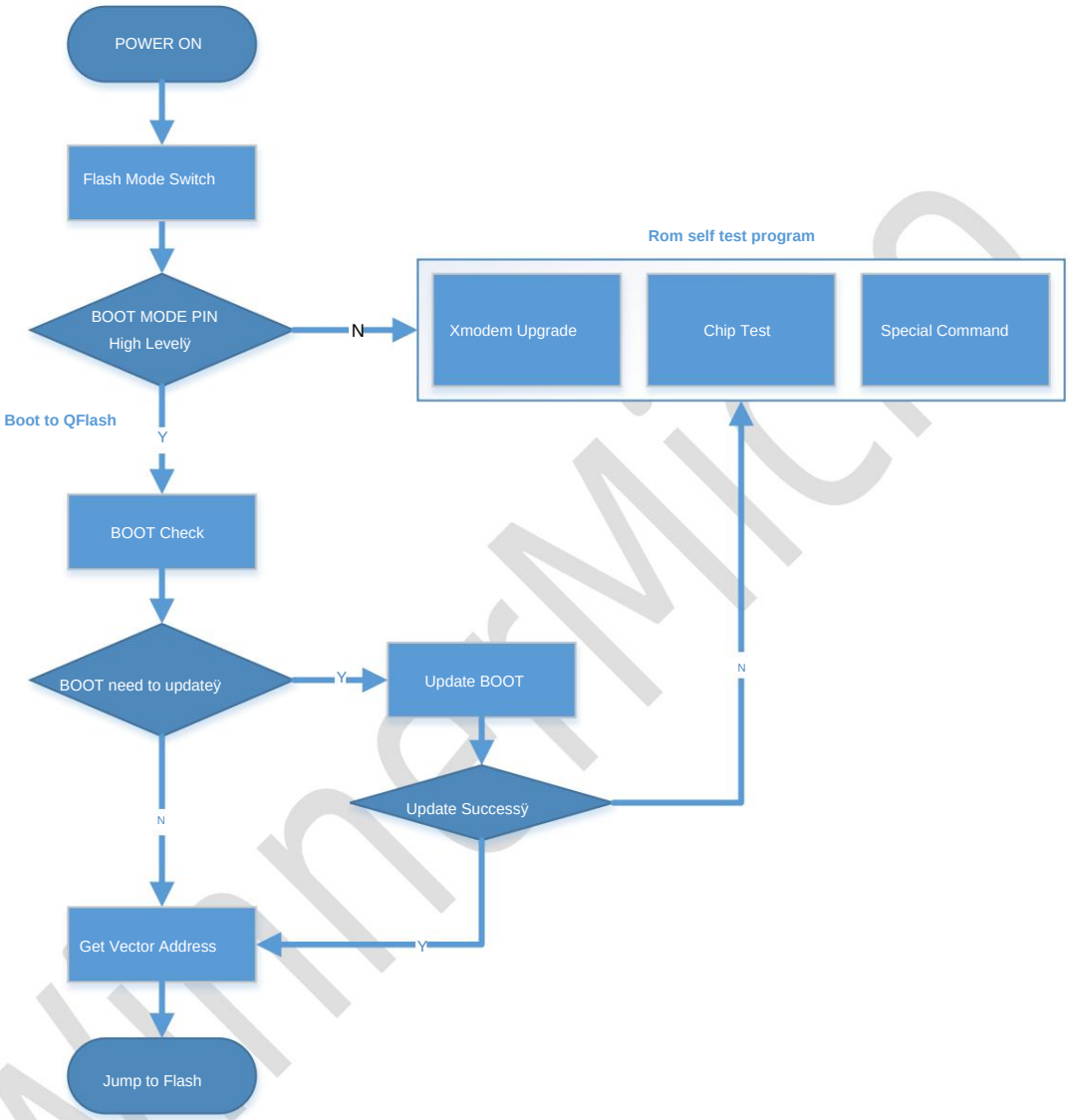


Figure 2-1

2.2 Bootloader

2.2.1 QFLASH self-test

Complete the QFLASH working status check

Machine Translated by Google

2.2.2 QFLASH mode switching

After booting from ROM, QFLASH defaults to 1-wire mode. To make the program run on QFLASH, ROM needs

To switch QFLASH to 4-wire mode.

2.2.3 IMAGE verification

Complete IMAGE header verification and IMAGE content verification

2.2.4 Vector Table Redirection

The W800 program will eventually run in QFLASH (code base address: 0x8000000), so it needs

Redirect the vector table.

Redirect address rule: (exception vector + interrupt) is a total of 64 words, according to the requirements of the VBR register, to

The gauge address must be an integer multiple of 0x400.

2.3 Upgrade procedure

Use Xmodem protocol to upgrade IMAGE to QFLASH or memory area, and upgrade to memory area

After the image is upgraded, it jumps to the memory for execution, and the upgraded FLASH needs to be restarted and then jumps to execute.

Upgrade IMAGE format:

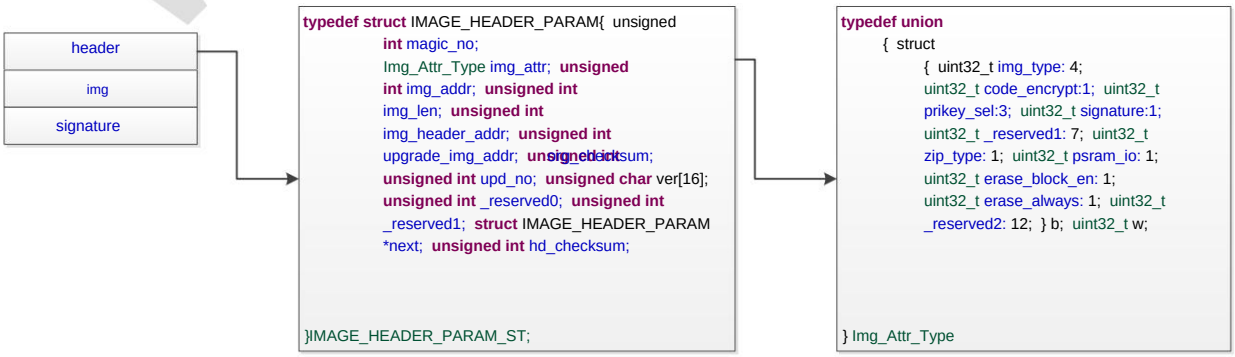


Figure 2-2

Machine Translated by Google

The IMAGE of W800 includes three parts: header, image area and signature. Header contains magic_no, img_attr, etc., where img_attr is a Uint32 type, including img_type, code_encrypt and other fields.

IMAGE header field description of W800:

field	describe
magic_no	magic word, fixed value 0xA0FFFF9F
img_attr	Img_Attr_TypeÿIMAGE Attribute
img_addr	The position of the Image area in the flash, the running position
img_len	The length in bytes of the Image area
img_header_addr	IMAGE header position in flash
upgrade_img_addr	upgrade area address, upgrade IMAGE header storage location in flash
crc32	result of org_checksum Image area
upd_no	Upgrade version number, a larger value indicates a newer version; when the version number is 0xFFFFFFFF , any version number firmware can be upgraded
to see	Image version number, string
next	The location of the next image header in flash
The crc32 value of the above field of hd_checksum	Image header

IMAGE Attribute field description of W800:

field	Bit	describe
img_type	4	0x0ÿSECBOOTÿ 0xE: ft test program; Other values: user defined

Machine Translated by Google

code_encrypt	1	0: The firmware is stored in plain text; 1: The firmware is encrypted and stored by the customer
pricey_sel	3	The chip has 8 sets of RSA private keys built-in to decrypt the secret key encrypted by the firmware, and the user can choose A group of use, the value range is 0~7
signature	1	0: IMAGE does not contain signature; 1: IMAGE contains 128bytes signature
zip_type	1	0: no compression; 1: image area part is a compressed file
Reserved	1	not currently in use
erase_block_en	1	0: does not support 64KB block erase; 1: supports block erase
erase_always	1	0: Check whether the flash is all F before erasing the Sector or Block, and the Sector with all F Or Block does not perform erase operation; 1: Always erase first and then write

Flash area division of W800:

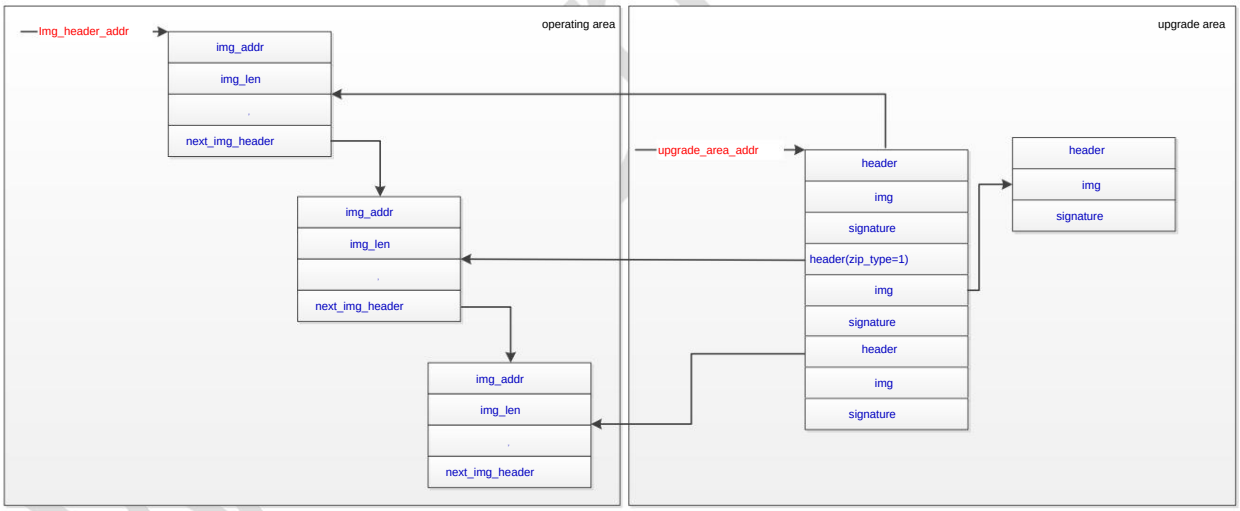


Figure 2-3

The ROM program judges whether the img_type of the first header is

sec boot, if yes, verify the crc and signature of the header and img, compare the version number, if the verification passes and

and the version is updated, move the header to the address of img_header_addr, and move the img and signature to

The address of img_addr.

The ROM program finds the img header of the SECBOOT program according to the img_header_addr parameter, and checks

Machine Translated by Google

After img header and img's crc and signature are successful, jump to img_addr and execute SECBOOT.

The SECBOOT program traverses the headers in turn according to the upgrade_area_addr parameter until img_type

It is the header of img, and then similar to the ROM program, move the header to the address of next_img_addr, move

The address of img and signature to img_addr.

The upgrade area can support multiple img upgrades including SECBOOT, you only need to put the programs to be upgraded end to end

Just the address of upgrade_area_addr.

For the img with zip_type=1 in the header, the img part is the original img

Header+img+signature is the compressed result of three parts, decompress it before moving. SECBOOT does not support compression.

2.4 OTP parameter area

The OTP parameter area of W800 stores some parameters related to firmware upgrade and signature verification.

2.5 Test procedure

The test program of W800 for the chip test stage is not placed in ROM, and it needs to pass uart before testing

The xmodem is upgraded to run in memory or Flash.

2.6 Operation instructions

The ROM program of W800 supports some operations in the module production stage: baud rate switching, QFLASH ID and capacity acquisition

Fetch, get ROM version, system reboot, etc.

Command sending method: hexadecimal

WinnerMicro

Machine Translated by Google

2.6.1 Command List

Function	child instruction ÿSubCmdÿ	data content ÿ Data Segmentÿ	illustrate
Baud rate switching	0x31	ÿ2000000	The baud rate supports up to 2M If the setting is greater than 2M, report S (the command parameter is wrong)

QFlash Erase	0x32	4bytes	struct{
			uint16_t index;
			uint16_t count;
			};
			index: starting position (the highest bit of index is 1 to indicate Block Erase, 0 means Sector erase)
			count: number of blocks to erase

Set BT MAC address 0x33		6bytes~8bytes	
Get BT MAC address 0x34		none	
Set the GAIN parameter	0x35	84bytes	Gain parameter used when transmitting on Wi-Fi (use with caution)
Get GAIN parameters	0x36	none	Read the Gain value of the set length.
set MAC address	0x37	6bytes~8bytes	
get MAC address	0x38	none	
Get last error 0x3B		none	Get the last error message until the next operation clears remove.
Get QFLASH ID and content 0x3C		none	For example, GD 32MB returns: FID:C8,19

WinnerMicro

Machine Translated by Google

quantity			PUYA 8MB Returns: FID:85,17
Get ROM version	0x3E	none	
system restart	0x3F	none	

2.6.2 Common instruction set

Baud rate change:

2M setting command: 21 0a 00 ef 2a 31 00 00 00 80 84 1e 00

1M setting command: 21 0a 00 5e 3d 31 00 00 00 40 42 0f 00

921600 Setting command: 21 0a 00 5d 50 31 00 00 00 00 10 0e 00

460800 Set command: 21 0a 00 07 00 31 00 00 00 00 08 07 00

115200 Set command: 21 0a 00 97 4b 31 00 00 00 00 c2 01 00

BT MAC address acquisition: 21 06 00 D8 62 34 00 00 00

WiFi MAC address acquisition: 21 06 00 ea 2d 38 00 00 00

Get last error: 21 06 00 36 B6 3B 00 00 00

QFLASH ID and capacity acquisition: 21 06 00 1b e7 3c 00 00 00

Get ROM version: 21 06 00 73 0a 3e 00 00 00

System restart: 21 06 00 c7 7c 3f 00 00 00

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

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

WinnerMicro

Machine Translated by Google

2.7 ROM error codes

During the ROM startup process, if an exception is encountered, it will enter the infinite loop program on the right side of the ROM, and then print a

Error code, indicating the error message currently encountered, for the user to analyze the problems encountered.

Error codes are defined as follows:

error code	illustrate
C	normal
Upgrade procedure (XMODEM protocol)	
D	host canceled
F	timeout no data received
G	wrong package number
'	IMAGE too large
J	IMAGE burning address is illegal
K	IMAGE programming address page is not aligned
L	IMAGE header validation error
M	IMAGE content validation error
P	IMAGE content is incomplete or signature is missing
Boot process	
N	FLASH ID self-test failed
Q	wrong firmware type
L	SECBOOT header check error
M	SECBOOT parity error
Y	Decryption read SECBOOT failed

WinnerMicro

Machine Translated by Google

FROM	Signature verification failed
functional module	
R	command check error
S	wrong command parameter
T	Failed to get FT parameters (Mac and Gain etc.)
IN	Failed to set gain
IN	Failed to set MAC

3 QFLASH and RAM usage

3.1 QFLASH layout

W800 supports four-address mode, up to 128MB Flash, but the ROM program only supports three-address mode

mode, and supports a maximum address access of 16MB.

QFLASH layout from ROM perspective:



Figure 3-1

WinnerMicro

Machine Translated by Google

3.2 Use of RAM

The memory of W800 is divided into two blocks: 160Kbyte and 128Kbyte. The distribution in ROM is as follows:

Memory block	function	start address	end address	size	illustrate
160Kbyte	Stack&Heap	0x20000000	0x20003FFF	Use 16Kbyte ROM	
	NC	0x20004000	0x20027FFF	144Kbyte NC	
128Kbyte	NC	0x20028000	0x20047FFF	128Kbyte NC	

WinnerMicro