A company of SIM Tech

SIM800 Series_Software Upgrade _Application Note_V1.04

Document Title:	SIM800 Series_Software Upgrade_Application Note
Version:	1.04
Date:	2016-11-17
Status:	Release
Document Control ID:	SIM800 Series_Software Upgrade_Application Note_V1.04

General Notes

SIMCom offers this information as a service to its customers, to support application and engineering efforts that use the products designed by SIMCom. The information provided is based upon requirements specifically provided to SIMCom by the customers. SIMCom has not undertaken any independent search for additional relevant information, including any information that may be in the customer's possession. Furthermore, system validation of this product designed by SIMCom within a larger electronic system remains the responsibility of the customer or the customer's system integrator. All specifications supplied herein are subject to change.

Copyright

Contents

Figure Index

Version History

Date	Version	Description of change	Author
2013-09-02	V1.00	New version	Yanhai.cheng
2013-09-04	V1.01	SIM800 Series Upgrade protocol and picture change	Yanhai.cheng
2014-06-30	V1.02	Change Linux Command parameter redefine	Yanhai.cheng
2015-10-10	V1.03	Change scope and change upgrade protocol	Zhongyu.gou
2016-11-17	V1.04	Scope	Wenjie.lai

Scope

This document describes how to use the PC or external MCU to upgrade software of SIM800 series modules by serial port.
This document can apply to SIM800 series modules with upgrade function (upgrade file name is ROM_VIVA).

1 Upgrade Process

This chapter introduces software upgrade process of SIM800 series modules. The following picture shows the upgrade process:

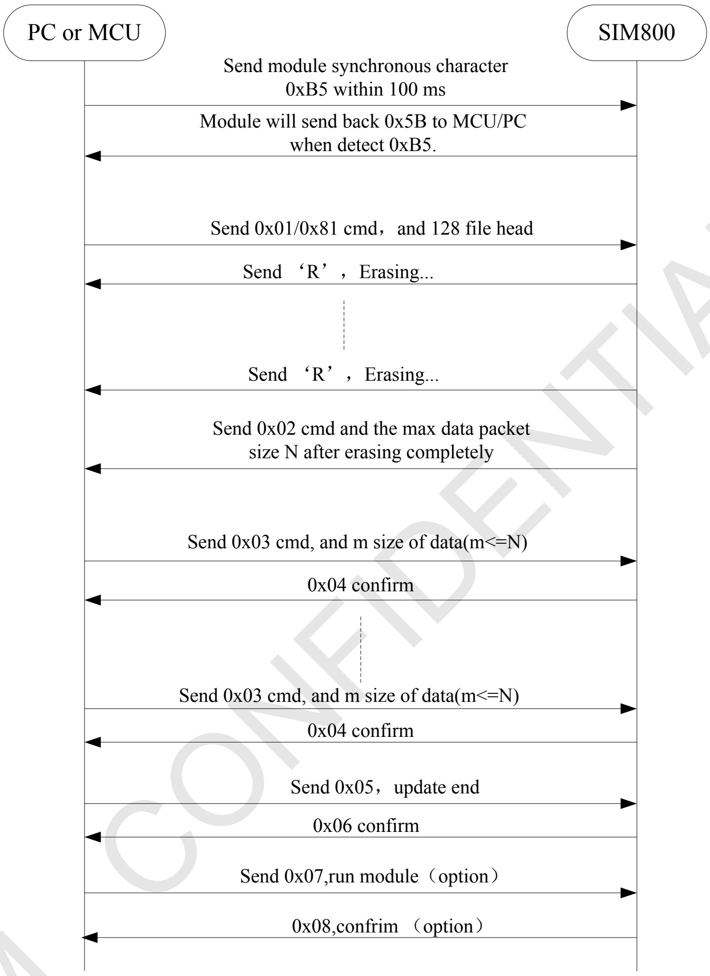
PC or MCU
SIM800
Send module synchronous character 0xB5 within 100 ms
Module will send back 0x5B to MCU/PC when detect 0xB5.
Send 0x01/0x81 cmd，and 128 file head
Send ‘R’，Erasing...
Send ‘R’，Erasing...
Send 0x02 cmd and the max data packet size N after erasing completely
Send 0x03 cmd, and m size of data(m<=N)
0x04 confirm
Send 0x03 cmd, and m size of data(m<=N)
0x04 confirm
Send 0x05，update end
0x06 confirm
Send 0x07,run module（option）
0x08,confrim （option）

Figure 1: Upgrade process

1.1 Command Summary

CMD	Description	Direction
0xB5	Sync byte	PC->MODULE
0x5B	Sync byte confirm	MODULE->PC
0x01/0x81	Send head information	PC->MODULE
0x02	Head information confirm	MODULE->PC
0x03	Send Upgrade data	PC->MODULE
0x04	Upgrade data confirm	MODULE->PC
0x05	Upgrade end	PC->MODULE
0x06	Upgrade end confirm	MODULE->PC

‘P’	Write flash fail	MODULE->PC
‘C’	Checksum error	MODULE->PC
‘R’	Erasing	MODULE->PC
‘E’	Erase error	MODULE->PC
‘S’	File size error	MODULE->PC
‘M’	Command error	MODULE->PC
‘T’	Time out	MODULE->PC
‘N’	Data package num error	MODULE->PC
‘F’	Time out between two commands	MODULE->PC
0x07	reset module	PC->MODULE
0x08	Reset module confirm	MODULE ->PC

Note:

1. ***The host computer should continue to transmit the synchronization word (0xB5) and the interval time of two synchronous word instructions should be less than 50 milliseconds, until the module has a synchronous word response (0x5B).***
2. ***The instruction sequence order: synchronization word: (0xB5) -> settings and erase address space (0x01/0x81) -> send up Packet level (0x03) -> data packet is sent (0x05) - >boot module (0x07).***

   The host computer can only send an upgrade data packet instruction (0x03) after setting the address and erase space (0x01/0x81). If the instruction sequence is wrong, the module will respond to the error code 'M', and enter an error state, you need to restart the PC module and upgrade again.
3. ***There are two exception error types in the upgrade process: recoverable error and irrecoverable error. The error code has been reported once when recoverable and reported continuously when irrecoverable. You must restart the module and upgrade again to recover the irrecoverable error. Only reported 'T' and 'C' of the error state can be recovered, the other errors are irrecoverable.***
4. ***The maximum time of module waiting for the instruction from host computer is 30 seconds. The module has been started to count when got confirm instruction. If the waiting time is longer than 30 seconds, the module enters the exception handling process and gets an irrecoverable error, you must restart the module and upgrade again.***
5. ***The document referred to the restart module or reset module is the switch to restart or use reset pin to restart, be sure not to use the powerkey shutdown. In the case of the bootloader phase or the module code is not complete, the powerkey shutdown is invalid.***

1.2 Start Upgrade Process

1) Make sure the normal power supply, and the serial port of the host computer and the UART1 port of the module are connected correctly.
2) Reset module.

Note:

The serial port of the host computer must be set as follows: 115200 bps, 8 bit, No parity bit, 1 stop bit, no flow control.

1.3 Synchronization Word Detection（0xB5）

When the module Bootloader program starts, if it receives the 0xB5 byte synchronization word within 100 ms, it will reply with a 0x5B byte word then the module go into the upgrade mode.

Within 100 ms, if the module does not receive 0xB5 synchronization word, the module will enter normal mode.

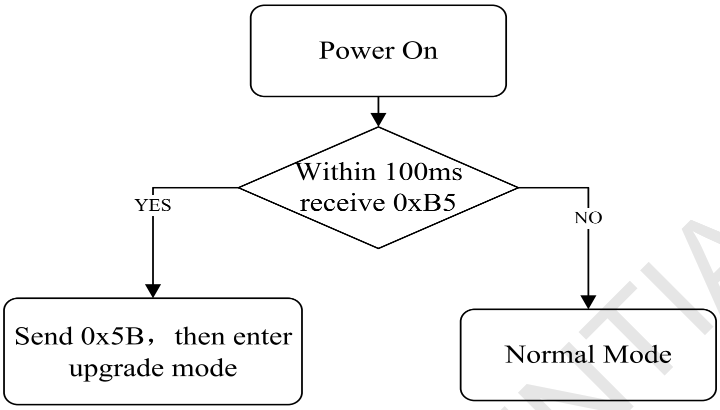

Figure 2：Waiting for synchronization word

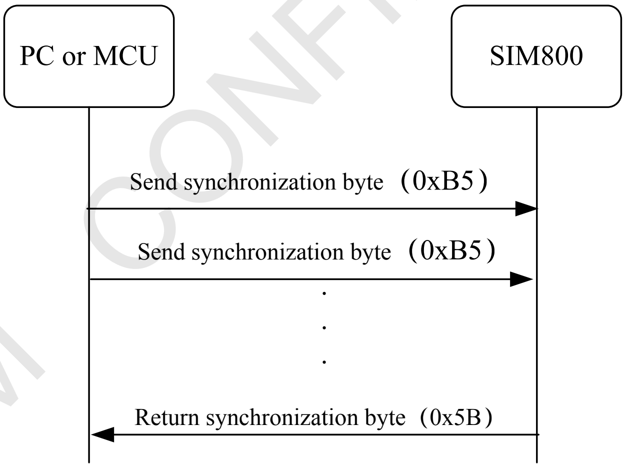
PC or MCU
SIM800
Send synchronization byte （0xB5）
Send synchronization byte （0xB5）
Return synchronization byte （0x5B）

Figure 3：Synchronization word detection

Note:

In order to make sure that the module can receive the synchronization byte 0xB5, the proposed upper computer continuously sends the synchronization byte 0xB5 until the module is powered up, until the module has a 0x5B instruction confirm, and the interval time of the two synchronization word should be less than 50 millisecond.

1.4 Send Head Information (0x01/0x81)

Command word 0x01 means there is no need to erase the file system of the module, while 0x81 means it needs to erase the file system of the module. In the version upgrade, such as upgrading from B01 to B02 version, you should erase the file system. The upgrade does not need to erase the file system if the version is special edition for customers. Data head contains 128 bytes information that included in the front part of upgrade file.

In the erase process, it will continue to return to the ASCII character 'R', that is, 0x52 in hexadecimal format, that means module is being erased internal Flash. The interval time of two characters is 30 milliseconds and the maximum timeout period is 1 second.

Data head format:

command	data
0x01/0x81	128 bytes head information

Module confirm：

confirm	Maximum data length N
0x02	2 bytes with low in the front and high in the post

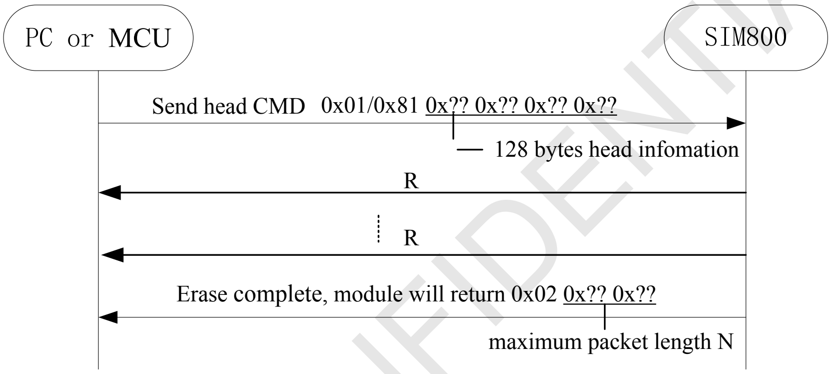
PC or MCU
SIM800
Send head CMD 0x01/0x81 0x?? 0x?? 0x?? 0x??
128 bytes head infomation
R
R
Erase complete, module will return 0x02 0x?? 0x??
maximum packet length N

Figure 4：Send head information

1.5 Upgrade ROM_VIVA File to the Module (0x03)

To upgrade ROM_VIVA file to the module, the frame should include four parts: the frame head (0x03), 3-bytes data frame length (maximum length is no more than N bytes returned with 0x02), 1-byte data frame number, data fields and 4-bytes data checksum. Checksum calculation method is as following: add all data bytes of the number and the value of last 4 bytes of the number is the checksum.

The frame format is as follows:

CMD	Frame Length	Frame No.	Data Field	Checksum
0x03	3 bytes, Low byte in the front	1 byte, Data frame No.	data frame	4 bytes, Low byte in the front

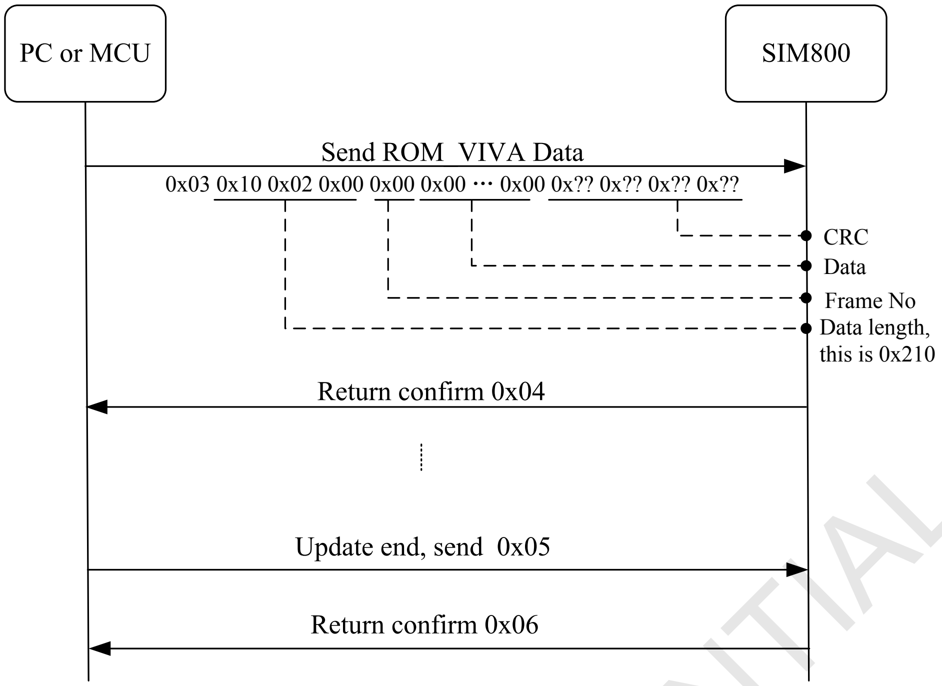

Figure 5: Upgrade ROM_VIVA file

Note:

1.The frame serial number ranges from 0xff to 0x00.

If it is 0, the frame number is not detected, otherwise it will loops from 0x01 to 0xff, 0x01->...... ->0xff->0x01->...... ->0xff->0x01->.......

2. The maximum response time of the module in the receiving data is 2 seconds, if no response is received in 2 seconds, it should restart module and upgrade again.

3. The longest time of seding one frame data is 500 milliseconds, if the module does not receive the full data frame in 500 milliseconds, Then the module returns an error code, and discarded the incomplete data packet to wait for the frame to be sent again.

4.The instruction for the ending of update is 0x05.

2 Linux Source Code

SIMCom offers SIM800 upgrade Linux source code mtkdownload, as well as the binaries compiled by Ubuntu 11.10 64 - bit system. Customer can run it directly under this system, in other Linux systems, or client MCU system, users need to recompile the source code and run their own code.

2.1 Compile the Source Code on Linux System

Run the following commands to complete the compiler directly.

```
gcc -o mtkdownload mtkdownload.c
```

2.2 Run on the Linux System

Run the following commands directly.

```
./mtkdownload <com> ROM_VIVA <format>
```

2.3 Command Line Parameters

<com>:/dev/ttyS0,/dev/ttyS1,/dev/ttyS2,/dev/ttyS3,/dev/ttyUSB0

Represent the:COM1,COM2,COM3,COM4 and the USB serial port

ROM_VIVA filename to upgrade

< format > parameter Y or N

Indicate whether or not format file system.

for example：

```
./mtkdownload /dev/ttyUSB0 ROM_VIVA Y
```

Indicate to upgrade SIM800 ROM_VIVA file, and format the file system by the USB serial port.

Appendix

A Related Documents

SN	Document name	Remark
[1]	SIM800 Series_AT Command Manual	
[2]		

B Terms and Abbreviations

Abbreviation	Description
MCU	Microcontroller Unit
PC	Personal Computer
UART	Universal Asynchronous Receiver/Transmitter
ROM	Read-only Memory

Contact us:

Shanghai SIMCom Wireless Solutions Co.,Ltd.

Address: Building A, SIM Technology Building, No. 633, Jinzhong Road, Shanghai, P. R. China 200335
Tel: +86 21 3252 3300
Fax: +86 21 3252 3020
URL: www.simcomm2m.com