SIM800系列_
软件升级协议_应用文档

GPRS 模组

芯讯通无线科技(上海)有限公司
上海市长宁区金钟路633号晨讯科技大楼B座6楼
电话：86-21-31575100
技术支持邮箱：support@simcom.com
官网：www.simcom.com

名称：	SIM800 系列_软件升级协议_应用文档
版本：	1.05
日期：	2020.06.15
状态：	已发布

版权声明

芯讯通无线科技(上海)有限公司
上海市长宁区金钟路 633 号晨讯科技大楼 B 座 6 楼
电话：86-21-31575100
邮箱：simcom@simcom.com
官网：www.simcom.com

了解更多资料，请点击以下链接：
http://cn.simcom.com/download/list-230-cn.html

技术支持，请点击以下链接：
http://cn.simcom.com/ask/index-cn.html 或发送邮件至 support@simcom.com

关于文档

版本历史

版本	日期	作者	备注
V1.00	2013-05-30	程延海	第一版
V1.01	2013-09-04	程延海	适用型号增加 SIM800
V1.02	2014-06-30	程延海	修改 Linux 命令行参数定义
V1.03	2015-10-10	勾中余	适用型号描述更改
V1.04	2016-11-17	来文洁	适用范围
V1.05	2020-06-15	曾福梅/来文洁	修改风格样式

适用范围

本手册描述了如何使用 PC 或者外部的 MCU 的串口升级 SIM800 系列模块的软件。

本手册适用于带串口升级功能（软件包里的 ROM_VIVA 文件）的 SIM800 系列版本。

目录

1 介绍

1.1 文档目的

本章节主要介绍 SIM800 系列模块的软件协议升级。

1.2 参考文档

[1] SIM800 Series_AT Command Manual

1.3 术语和缩写

术语	描述
MCU	微控制单元
PC	个人计算机
UART	通用异步收发传输器
ROM	只读存储器

2 升级流程

本章节主要介绍 SIM800 系列模块软件升级流程。
升级流程如图 1 所示。

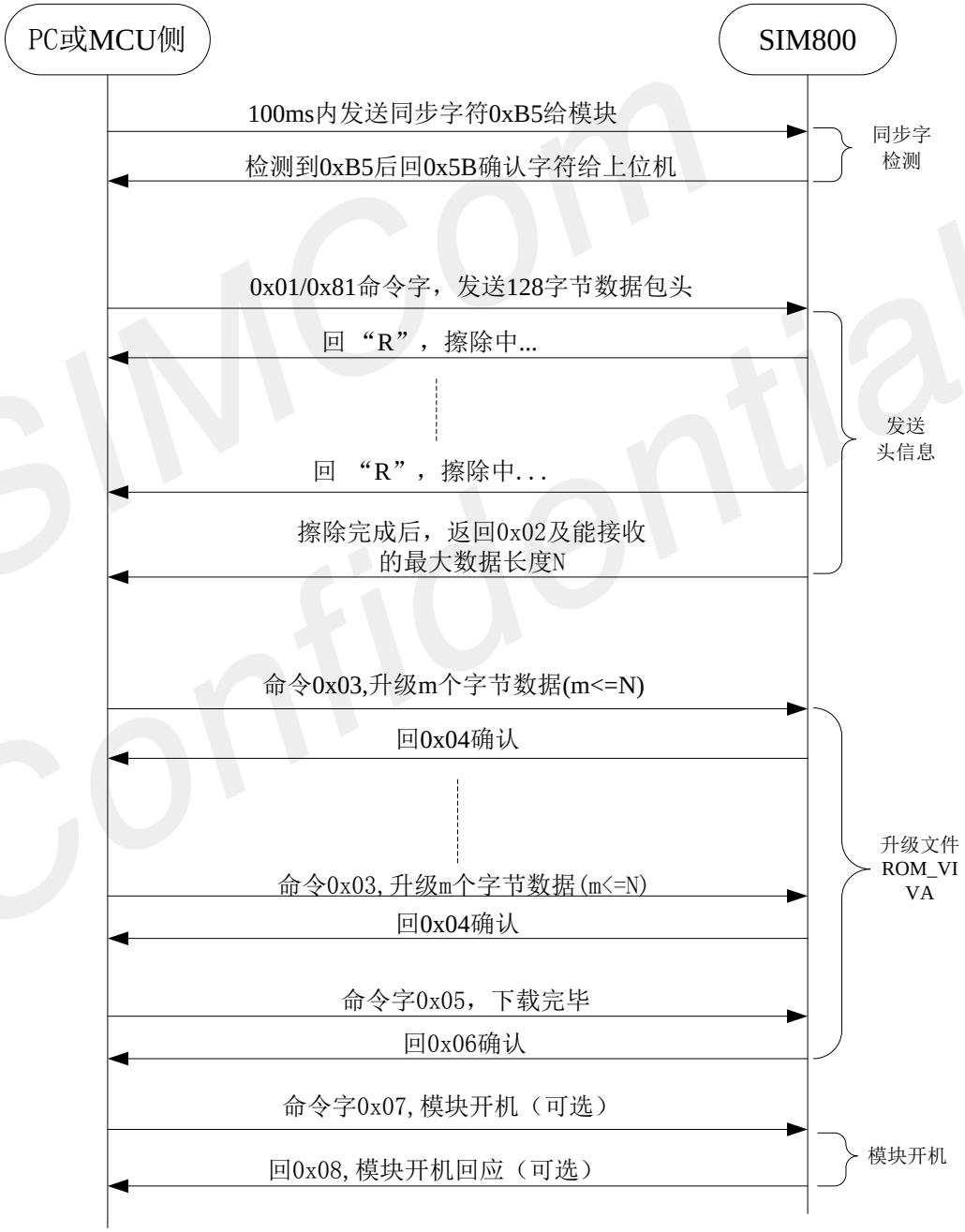

图 1：升级流程图

2.1 命令字

命令字	描述	方向
0xB5	同步字	PC->MODULE
0x5B	同步字回应	MODULE->PC
0x01/0x81	设定地址及擦除空间	PC->MODULE
0x02	设定地址及擦除空间回应	MODULE->PC
0x03	发送升级数据包	PC->MODULE
0x04	发送升级数据包回应	MODULE->PC
0x05	数据发送结束	PC->MODULE
0x06	数据发送结束回应	MODULE->PC
‘P’	写 flash 失败	MODULE->PC
‘C’	校验位错误	MODULE->PC
‘R’	擦除中	MODULE->PC
‘E’	擦除失败	MODULE->PC
‘S’	文件传输大小出错	MODULE->PC
‘M’	命令错误	MODULE->PC
‘T’	超时	MODULE->PC
‘N’	数据包序号错误	MODULE->PC
‘F’	指令之间时间超时	MODULE->PC
0x07	升级完模块开机	PC->MODULE
0x08	升级完模块开机回应	MODULE ->PC

※ 特别注意

1. 上位机应持续发送同步字（0xB5），两个同步字指令间隔应小于 50 毫秒，直到模块有同步字回应（0x5B）。
2. 指令有顺序要求，顺序为：同步字(0xB5)->设定地址及擦除空间(0x01/0x81)->发送升级数据包(0x03)->数据包发送完毕(0x05)->模块开机(0x07)。
3. 设定地址及擦除空间（0x01/0x81）后只能发送升级数据包指令(0x03)。如果指令顺序错误的话，模块会回应错误码‘M’，并进入不可恢复错误状态，需要上位机重启模块并重新进行升级流程。
4. 升级过程中有两种异常错误类型，可恢复错误和不可恢复错误。可恢复错误上报一次错误码，不可恢复错误状态一直上报错误码。发生不可恢复错误时，就必须重启模块并重新升级。只有上报‘T’和‘C’的错误状态是可恢复错误以外，其他都为不可恢复错误。
5. 模块等待上位机指令的最大时间是 30 秒，在模块回应指令后开始计时，如果等待时间大于 30 秒，则模块进入异常处理流程，上报错误码，进入不可恢复错误状态，需要上位机重启模块并重新进行升级流程。
6. 该文档提到的重启模块或复位模块是指开关断电重新开机或者使用 reset 复位脚重启，务必不要使用 powerkey 关机。在 bootloader 阶段或者模块代码不全的情况下，powerkey 关机无效。

2.2 启动升级流程

1 确保模块正常供电，及上位机串口与模块 UART1 端口正确连接。
2 复位模块。

※ 特别注意

上位机的串口必须是如下设置：115200bps，8 bit，No parity bit，1 stop bit，no flow control。

2.3 同步字检测(0xB5)

当模块的 bootloader 程序启动后，模块如果在 100ms 内接收到了同步字 0xB5，模块将会回复一个 0x5B，此时模块就进入了升级模式。
如果模块在 100ms 内，没有接收到同步字 0xB5，模块将进入正常的启动模式。

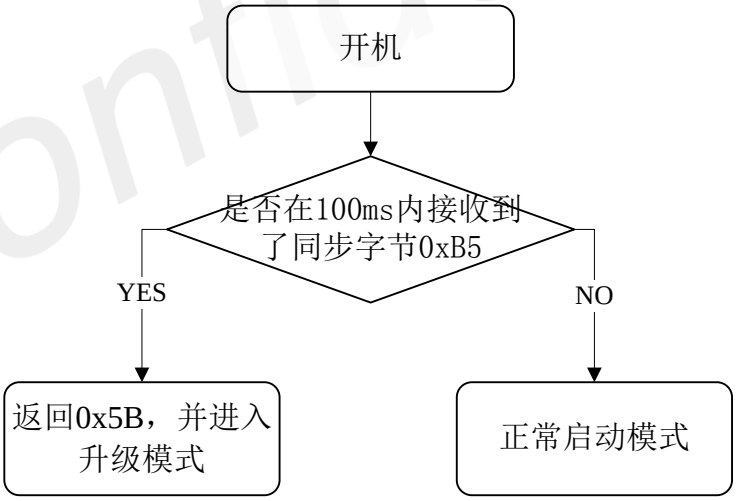

图 2：等待同步字

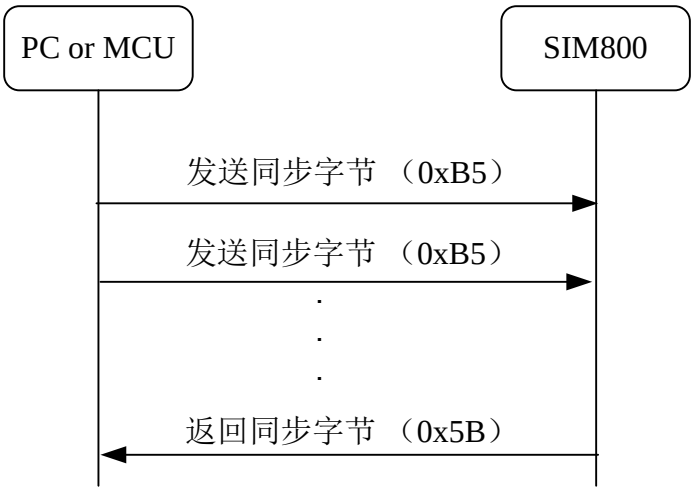

图 3：同步字检测

※ 特别注意

为了确保模块能够收到同步字节 0xB5，建议上位机从模块上电之前就持续发送同步字节 0xB5，直到模块有 0x5B 指令回应，两个同步字间隔时间应小于 50 毫秒。

2.4 发送头信息（0x01/0x81）

命令字 0x01 表示 MCU 不需要对模块的文件系统进行擦除，而 0x81 则表示需要对模块的文件系统进行擦除。在版本升级时，比如从 B01 升级到 B02 时，要选择对文件系统进行擦除。给客户的特殊版本，升级时不需要擦除文件系统。头信息为升级包的前面 128 字节。

在擦除过程中，会持续返回 ASCII 字符‘R’，即十六进制的 0x52，表示模块正在擦除内部 Flash，两个字符间隔 30 毫秒左右，最大超时时间为 1 秒。
擦除结束后，会返回指令 0x02。

发送头信息帧格式：

命令	数据
0x01/0x81	升级包前 128 字节数据

模块回应：

命令回应	允许的最大数据长度 N
0x02	2 字节，低位在前，高位在后

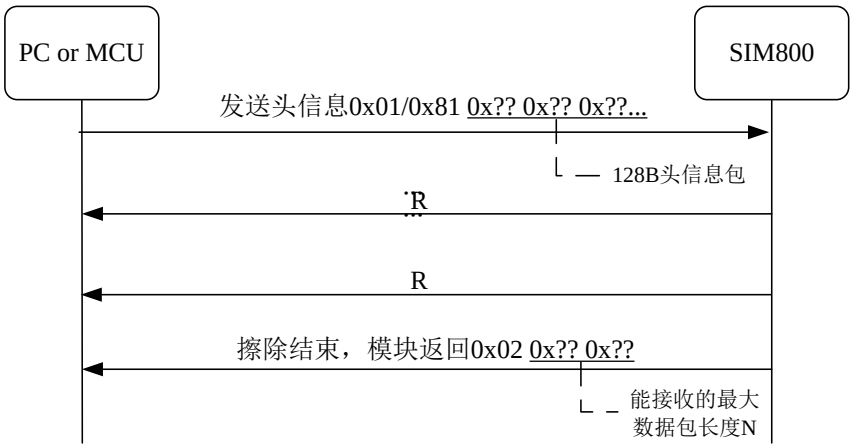

图 4：发送头信息数据包图

2.5 升级 ROM_VIVA 文件到模块（0x03）

升级 ROM_VIVA 文件到模块端，该帧主要包括 4 个部分，它们是帧头（0x03），3 字节的帧数据长度（最大值不能超过模块返回的 0x02 指令中的 N），以及 1 字节的序列号，数据域以及 4 字节的数据校验位。校验位的计算方法为：将数据域的所有字节相加得到的一个 4 字节值就是校验值。

帧格式如下：

命令	帧的数据长度	帧序号	数据域	校验位
0x03/0x05	3 字节，低位在前高位在后	1 字节，发送数据帧的序号	按照数据帧的长度决定	4 字节，低位在前高位在后

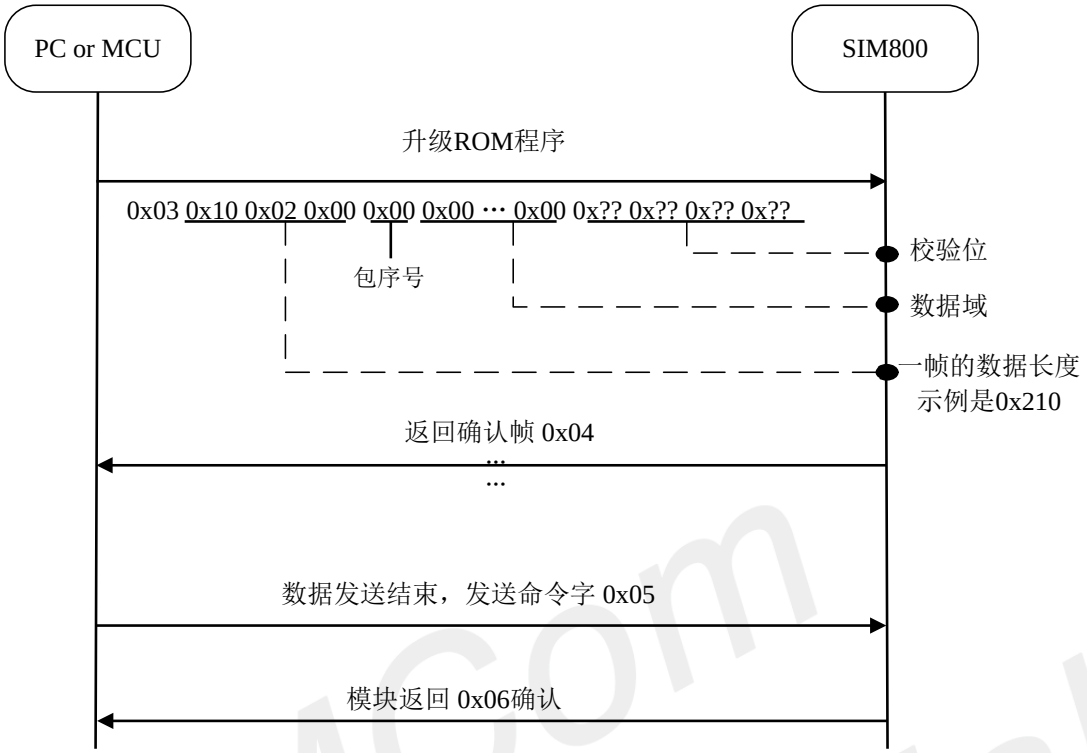

图 5：升级 ROM_VIVA 程序

※ 特别注意

1. 帧序号取值范围为 0x00～0xff。
   如果为 0，则不检测帧序号，否则从 0x01 到 0xff 循环，0x01->……->0xff->0x01->……->0xff->0x01->……。
2. 模块在接收数据期间的最大响应时间是 2 秒，如果 2 秒模块没有任何响应，则应该重启模块，重新开机升级流程。
3. 一帧数据发送最长时间为 500 毫秒，如果在 500 毫秒内模块没有收到完整数据帧，则模块会返回错误码，丢弃该次不完整数据包，等待该帧重新发送。
4. 数据发送结束的指令为 0x05。

3 Linux 源码

SIMCom 提供 SIM800 升级工具的 Linux 源码 mtkdownload.c 文件，以及在 Ubuntu 11.10 64bit 系统下已经编译好的二进制文件。在该系统上客户可以直接运行，在其它 Linux 系统，或者客户 MCU 系统上，用户需要自行编译源码并运行。

3.1 Linux 源码编译

直接运行下列命令即可完成编译。
gcc -o mtkdownload mtkdownload.c

3.2 Linux 系统上运行

直接运行下列命令即可。
./mtkdownload <com> ROM_VIVA <format>

3.3 命令行参数说明

<com>可选参数:/dev/ttyS0,/dev/ttyS1,/dev/ttyS2,/dev/ttyS3,/dev/ttyUSB0
分别代表:COM1,COM2,COM3,COM4 以及 USB 串口
ROM_VIVA 要升级的 ROM_VIVA 文件名。
<format>可选参数 Y，N
表示是否格式化文件系统。

例如：
./mtkdownload /dev/ttyUSB0 ROM_VIVA Y
表示在 USB 转串口上升级 SIM800 的 ROM_VIVA 文件，并且格式化文件系统。