

AN02001

如何使用 TC35/TC35T AT 命令收发短信息

作者：技术支持部 胡永健

一、 介绍：

本文记录的大量的 TC35/TC35T 实验数据 ,总结了使用 TC35/TC35T 收发短信的方法。

TC35 模块系 SIEMENS 公司为嵌入式设备设计的 GSM 双频通讯核心模块 ,TC35T 内含 TC35/SIM 卡座/电源/天线/RS232 接口 ,系可独立使用的通讯终端。本文中除特别说明外 ,所有关于 TC35 的说明也适用于 TC35T。TC35 不仅支持标准的 AT 命令集 ,SIEMENS 公司还将 AT 命令进行了扩展 ,以便更有效的控制 TC35。

MC2002 可选 GSM 扩展板采用了 -TC35 模块 ,用户可以通过 MC2002 Modem 接口控制内置的 TC35 或通过上位机 (如 PC) RS232 通讯口控制 TC35T 终端 ,使用 AT 命令 ,即可实现收发短信 ,以及语音以、数据拨号等相关操作。

需要说明的是 TC35 具有自动识别串行接口速率的能力 ,但要求速率范围在 1200Bps 至 115200Bps 之间 ,并且设置为 8Bit 数据 ,无校验 ,1 位停止位。

九十年代初 ,AT 命令仅被用于 Modem 操作。由于没有控制移动电话文本消息的先例 ,因此开发了一种叫 SMS(Short Message Service) Block Mode 的协议 ,通过终端设备 (TE--Terminal Equipment) 或 PC 来完全控制 SMS。几年后 ,主要的移动电话生产厂商诺基亚、爱立信、摩托罗拉和 HP 共同为 GSM 研制了一整套 AT 命令 ,其中包含对 SMS 的控制。AT 命令在此基础上演化并被加入 GSM 07.05 标准 ,以及之后的 GSM 07.07 标准。对 SMS 的控制共有三种实现途径：

- (1) 最初的 Block 模式
- (2) 基于 AT 命令的 Text 模式
- (3) 基于 AT 命令的 PDU 模式

到现在 ,PDU 已取代 Block ,后者逐渐淡出。

二、AT 命令形式及返回形式

所有的 AT 命令都以“AT”或“at”打头。

在 TC35 所支持命令集中根据命令名称可简单分为：

- (1) “ATxx”及少量“AT+xxx”为 V.25 标准命令集；
- (2) “AT+Cxxx”为 GSM 标准所扩展的 AT 命令；
- (3) “AT^Sxxx”为 SIEMENS 定义扩展的 AT 命令。

另外，根据命令形式可分为：

- (1) “AT+Cxxx=?”为测试命令 (Test Command)，执行此种命令将返回此命令所支持的参数及参数范围；
- (2) “AT+Cxxx?”为读命令 (Read Command)，执行此种命令将返回此命令当前的参数值；
- (3) “AT+Cxxx=<...>”为写命令 (Write Command)，执行此种命令将设置此命令的参数值；
- (4) “AT+Cxxx”为无参数的执行命令 (Execution Command)。

特别要注意的是这些命令的返回形式为：

<CR><LF>Response<CR><LF>

在本文数据实录中未将<CR><LF>显式地打印出来，但切记 TC35 回送时含有这些字符，这对于编写程序来比对 TC35 回送值以确定 TC35 工作是否正常非常重要。

在本文中：

<CR>	代表 ASCII 中回车字符，值为 0x0D；
<LF>	代表 ASCII 中换行字符，值为 0x0A；
<SP>	代表 ASCII 中空格字符，值为 0x20；
<CTRL+Z>	代表 ASCII 中文件结束字符，值为 0x1A；

所有 TC35 回送的字符以下画线表示，所有上位机发送给 TC35 的字符以正常字符表示。

三、准备工作：

使用 TC35 收发短信息，用户必须准备一张已开通短信息服务 SIM 卡，并将其插入 MC2002 之 TC35 扩展模块 SIM 卡座中或 TC35T 的 SIM 卡座中。

使用 PC 配合 TC35T 收发短信，用户需开启 TC35T 电源，通过串行数据线联接到 PC 机，并在 PC 端安装串口读写软件，如超级终端，Telix 等。通过终端软件发送 AT 命令，察看返回数据。

通过 MC2002 使用 TC35 扩展模块时，用户需编程选用 MODEM 端口，TC35 将自动上电，再通过编程发送 AT 命令和处理返回数据。MC2002 在关闭 TC35 电源前，首先要向其发送“AT^SMSO”命令，并确认返回为“OK”或 0（即中断与 TC35 网络连接）后，才可关闭 MODEM 端口。

四、使用 AT 命令实现收发短信

1. 收发短信及相关操作 AT 命令

ATZ	软复位；
ATE	本地回线设置；
ATV	设置返回结果码形式；
AT+CMEE	错误报告设置；
AT+CSCA	短消息中心地址；
AT+CMGR	读短消息；
AT+CMGS	发送短消息；
AT+CMGC	发出一条短消息命令；
AT+CMGL	列出 SIM 卡中的短消息；
AT+CMGF	选择短消息信息格式：0 PDU，1 文本；
AT+CSCS	设置字符集；
AT+CSMP	设置短消息文本模式参数；
AT+CMGW	向 SIM 内存中写入待发的短消息；
AT+CMNI	显示新收到的短消息；
AT+CMGD	删除 SIM 卡内存的短消息；
AT+CPBR	读取当前电话本信息；
AT+CSQ	检查信号质量；
AT+SMSO	中断网络连接。

TC35 提供 Text 和 PDU (Protocol Data Unit) 两种模式来处理短信。在 Text 模式下可进行 GSM 字符集与 8Bit 数据的收、发等操作，但不支持中文或 UCS2 字符集字符的收发操作；在 PDU 模式下可支持上述所有操作，但需要理解收发 PDU 数据格式。在 Text 模式与 PDU 模式下，上述命令使用方法会有所不同。详细的内容请参阅相关资料。

下面就根据收发不同编码类型的数据进行最简单易行的设置，用户在实际应用中需根据实际需要进行设置。

2. 发送短信实例

SMS 是由 ETSI 所制定的一个规范 (GSM 03.40 和 GSM 04.11)，规定当使用 7Bits 编码 (GSM 字符集) 时最多可以发送 160 个字符；当使用 8Bit 编码 (数据消息，如：铃音、图片) 时最多可以发送 140 个字符 (通常无法直接通过手机终端显示)；当使用 16Bit 编码 (UCS2) 时最多可以发送 70 个字符，此编码用来显示 Unicode 文本信息，可以被大多数的手机终端支持。实例：

(1) 发送英文短信

```
AT+CMGF=1      设置为 Text 模式
AT+CSMP=17,167,0,0 设置 Text 模式参数。最后一个参数是数据编码类型
                  (DCS-Data Coding Scheme)，0 表示默认字符集 (GSM)。
AT+CSCS=GSM    设置为 GSM 字符集
AT+CMGS        输入对方电话号码
><SP>为 TC35 提示，"TEST LINE!"短信息内容，<Ctrl+Z>表示结束。
```

数据实录：

><SP>为 TC35 提示 ,
"0011000B913196899074F00008AA0862116210529F4E86" 为 PDU 内容 ,
<Ctrl+Z>表示结束.其中," 62116210529F4E86 " 为 " 我成功了 " 中文字符
串的 Unicode.

数据实录 :

```
AT<CR>
OK
AT+CMGF=0<CR>
OK
AT+CSCS=GSM<CR>
OK
AT+CSMP=17,167,0,8
OK
AT+CMGS=22<CR>
<SP>0011000B913196899074F00008AA0862116210529F4E86<CTRL+Z>
//PDU 内容
+CMGS: 89
OK
```

3. 接收短信实例

(1) 接收英文短信

AT+CMGF=1 设置为 Text 模式
AT+CSCS=GSM 设置为 GSM 字符集
AT+CMGL=ALL 列出所有短信息

请注意其中第一条及第三条为中文短信,它们在 Text 模式下无法显示出正确的内容,只能列出其中的英文字符; +CMGL 后的数字(如 1)表示记录号,"REC READ"表示已读,(未读为"REC UNREAD"),"+8613699809470"表示发方号码,"02/05/19,22:17:31+00"表示时间邮戳。

AT+CMGL=UNREAD 可以列出所有未读短信息,注意:未读短信一旦列出一次即变为已读短信

数据实录 :

```
AT<CR>
OK
AT+CMGF=1<CR>
OK
AT+CSCS=GSM<CR>
OK
AT+CMGL=ALL<CR>
+CMGL: 1,"REC READ","+8613699809470",,"02/05/19,22:17:31+00"
```

S
+CMGL: 7,"REC READ","+8613902909595",,"02/05/17,16:23:31+00"
1234567890ABC
+CMGL: 10,"REC READ","+8613902909595",,"02/05/17,16:41:19+00"
1234567890ABC

OK

(2) 接收中文短信

AT+CMGF=0<CR> 设置为 PDU 模式

AT+CMGL=4<CR> 列出所有短信息

+CMGL 后的首个数字(如 7)表示记录号;第二个数字表示短信状态(0—未读短信;
1—已读短信);其后一个数字(如 28)表示 PDU 长度,最后为该条短信的 PDU
数据。

数据实录:

AT<CR>
OK
AT+CMGF=0<CR>
OK
AT+CMGL=4<CR>
+CMGL: 1,1,,28
0891683108705505F0040D91683196899074F0000820509122711300085
3D17ED981EA5DF1
+CMGL: 7,1,,32
0891683108705505F0240D91683109929095F50000205071613213000D3
1D98C56B3DD703958503804
+CMGL: 10,1,,50
0891683108705505F0240D91683109929095F50008205071611491001E0
0310032003300340035003600370038003900300041004200438FD84E2A

OK

4. 删除短信实例

接收的 SMS 存储在 SIM 卡中,如不及时删除则在 SIM 卡存储满后无法接收新的短信,建议用户将短信列出/读回并转存储在上位机(MC2002 或 PC)后,及时将 TC35 中内容删除。删除的命令为:AT+CMGD=<index>。其中,index 为记录号。要说明的是即使在 index 处无记录,此命令也会返回 OK。

数据实录:

AT<CR>
OK
AT+CMGD=1
OK

五、收发 PDU 的数据格式

接收与发送的 PDU 数据串不仅仅包含了短消息内容，而且还包含其它信息，如：发送者的信息、短信中心地址、时间标志等等。这些都是以 8 位字节的 16 进制数或者半 8 位字节的十进制数下的字符。

1. 收 PDU 的数据格式

在这里给出一个例子：接收到源地址为“13677328099”发来的内容为“Hi”的 PDU，其数据为：08 91 683108701305F0 00 0D 91 683109929095F5 00 00 20507161321300 02 C834

下面进行详细分析：

- (1) 08—短信息中心地址字节长度。指“(91)+(683108701305F0)”的长度，其中两个数字计为一个字节长度；
- (2) 91—短信息中心号码类型 (Type of Number)。91 是表示遵守 International/E.164 标准。此外还有其它数值，但 91 最常用；
- (3) 683108701305F0—短信息中心号码，注意其每两位是位置颠倒的。实际号码应为：8613800731500。由于电话号码为奇数(11 位)，因此加入 F 来保证其为 8 字节；
(1)、(2)、(3)通称短消息中心地址 (Address of the SMSC)；
- (4) 00—SMS_DELIVER 的第一个 8 位；
- (5) 0D—发送方号码长度；
- (6) 91—发送方号码类型 (同 2)；
- (7) 683109929095F5—发送方号码，实际号码为“8613902909595”；
(6)、(7)、(8)通称目的地址 (TP-Destination-Address)；
- (8) 00—协议标识 TP-PID (TP-Protocol-Identifier)；
- (9) 00—数据编码方案 TP-DCS (TP-Data-Coding-Scheme)
Bit No.7 与 Bit No.6：一般设置为 00；
Bit No.5：0 — 文本未压缩，
1 — 文本用 GSM 标准压缩算法压缩；
Bit No.4：0 — Bit No.1、Bit No.0 为保留位，不含类型信息，
1 — Bit No.1、Bit No.0 含有类型信息；
Bit No.3 与 Bit No.2：
00—默认的字母表，
01—8bit，
10—USC2 (16bit)
11—预留；
Bit No.1 与 Bit No.0：
00—Class 0，
01—Class 1，
10—Class 2 (SIM 卡特定信息)，
11—Class 3；
- (10) 20507161321300—时间戳 TP-SCTS (TP-Service_Centre-Time-Stamp)；
- (11) 02—用户数据长度 TP-UDL (TP-User-Data-Length)；
- (12) C834—用户数据 TP-UD (TP-User-Data) “Hi”；

2. 发 PDU 的数据格式

在这里同样给出一个例子：向目的号码为“ 46708251358 ”的终端发送内容为“ hellohello ” PDU 数据。PDU 内容为：

00 11 00 0B 91 6407281553F8 00 00 AA 0A E8329BFD4697D9EC37

下面进行详细分析：

- (1) 00-短信息中心地址长度。在这里为 0，表示使用存储在 SIM 卡中的短信息中心地址；
- (2) 11-SMS_SUBMIT 的第一个 8 位；
- (3) 00-发送方地址信息。在这里为 0，表示使用本机号码；
- (4) 0B-接收方号码长度；
- (5) 91-接收方号码类型(Type of Number)；
- (6) 6407281553F8-接收方号码.实际号码为 46708251358；
- (7) 00-协议标识 TP-PID (TP-Protocol-Identifier)；
- (8) 00-数据编码方案 TP-DCS (TP-Data-Coding-Scheme)
 - Bit No.7 与 Bit No.6：一般设置为 00；
 - Bit No.5： 0 — 文本未压缩，
1 — 文本用 GSM 标准压缩算法压缩；
 - Bit No.4： 0 — Bit No.1、Bit No.0 为保留位，不含类型信息，
1—表示 Bit No.1、Bit No.0 含有类型信息；
 - Bit No.3 与 Bit No.2：
 - 00—默认的字母表，
 - 01—8bit，
 - 10—USC2 (16bit)，
 - 11—预留；
 - Bit No.1 与 Bit No.0：
 - 00—Class 0，
 - 01—Class 1，
 - 10—Class 2 (SIM 卡特定信息)，
 - 11—Class 3；
- (9) AA-有效期 TP-VP (TP-Valid-Period)；
- (10) 0A-用户数据长度 TP-UDL(TP-User-Data-Length).若发送 7Bit 编码数据，则 TP-UDL 为实际字符个数；若为 8Bit 数据或 16Bit 编码的 Unicode，则 TP-UDL 为数据字节 (8 位) 的个数。
- (11) E8329BFD4697D9EC37-用户数据 TP-UD(TP-User-Data)"hellohello"；

3. PDU 模式发送 7Bit 数据编码过程

在 PDU 模式下发送 7Bit 编码数据前首先要将数据编码为 8Bit，在进行发送。还是以发送“hellohello”为例来分析编码过程：

“hellohello”包含了 10 个字符，他们必须一个个将用 7-bits 来代表。

H	e	l	l	o	h	e	l	l	o
104	101	108	108	111	104	101	108	108	111
1101 000	1100 101	1101 100	1101 100	1101 111	1101 000	1100 101	1101 100	1101 100	1101 111

1101 000	1100 10 <u>1</u>	1101 1 <u>00</u>	1101 <u>100</u>	110 <u>1</u> <u>111</u>	11 <u>01</u> <u>000</u>	1 <u>100</u> <u>101</u>	<u>1101</u> <u>100</u>	1101 100	1101 11 <u>1</u>
-------------	---------------------	---------------------	--------------------	----------------------------	----------------------------	----------------------------	---------------------------	-------------	---------------------

上表中首行为 7BIT 数据的 ASCII 表示，次行为 ASCII 值，第三行为 ASCII 值的二进制表示，第四行中有下画线的二进制数字表示将要在编码时移到前字节。

首先将字符转换为 7 位的二进制，然后，将后面字符的位调用到前面，补齐前面的差别。例如：h 翻译成 1101000，e 翻译成 1100101，显然 h 的二进制编码不足八位，那么就将 e 的最后一位补足到 h 的前面。那么就成了 11101000 (E8)。剩余地编码看下表（表中有下画线的部分表示其为编码时移来的数据，第八字节时为 0 表示编码后节省出一个字节地址）：

<u>1</u> 1101 000	<u>00</u> 110 001	<u>100</u> 11 011	<u>1111</u> 1 101	<u>01000</u> 110	<u>10010</u> <u>111</u>	<u>11011</u> <u>001</u>		<u>1</u> 1101 100	11011 1
E8	32	9B	FD	46	97	D9		EC	37

那么就变成了 9 个十六进制数 E8 32 9B FD 46 97 D9 EC 37。

六、参考资料

- (1) <<Technical Product Information TC35>>;
- (2) <<AT Command Set -- Siemens Cellular Engines >>
- (3) <<GSM Technical Specification - GSM07.05 >>
- (4) <<GSM Technical Specification - GSM07.07 >>

相关网站：...

- (1) [Http://www.etsi.org/](http://www.etsi.org/)
- (2) [Http://www.dreamfabric.com/sms/](http://www.dreamfabric.com/sms/)
- (3) [Http://www.nobbi.com/sms_pdu.html](http://www.nobbi.com/sms_pdu.html)