

用单片机控制手机收发短信息

摘要：介绍用 MCS-51 系列单片机控制手机收发短信息的原理、硬件电路、PDU 数据格式和符合 GSM07.05 协议要求的短信息发送/接收程序，同时给出了一个应用实例。

关键词：单片机 短信息 PDU GSM 接口

GSM (Global System for Mobile communication) 系统是目前基于时分多址技术的移动通讯体制中比较成熟、完善、应用最广泛的一种系统。目前已建成的覆盖全国的 GSM 数字蜂窝移动通信网，是我国公众移动通信网的主要方式。主要提供语音、短信息、数据等多种业务。基于 GSM 短消息功能可以做成传输各种检测、监控数据信号和控制命令的数据通信系统，能广泛用于远程监控、定位导航、个人通信终端等。由于公众 GSM 网络在全球范围内实现了联网和漫游，建立上述系统不须再组建专用通信网络，所以具有实时传输数据功能的短消息应用将得到迅速普及。

目前，人们设计的各类 DTE 设备基础上以微处理器为核心，带有 RS232/RS485 等通信接口，在物理层上很容易实现与 GSM 设置（如手机等）的连接。但对 SMS 协议的研究文献却较少，特别是用单片机控制手机的 SMS (Short Message Service) 收发的研究更少。笔者在用单片机设计基于 GSM 的 SMS 数据采集器时，对怎样用单片机控制手机收发短信息进行了探讨。

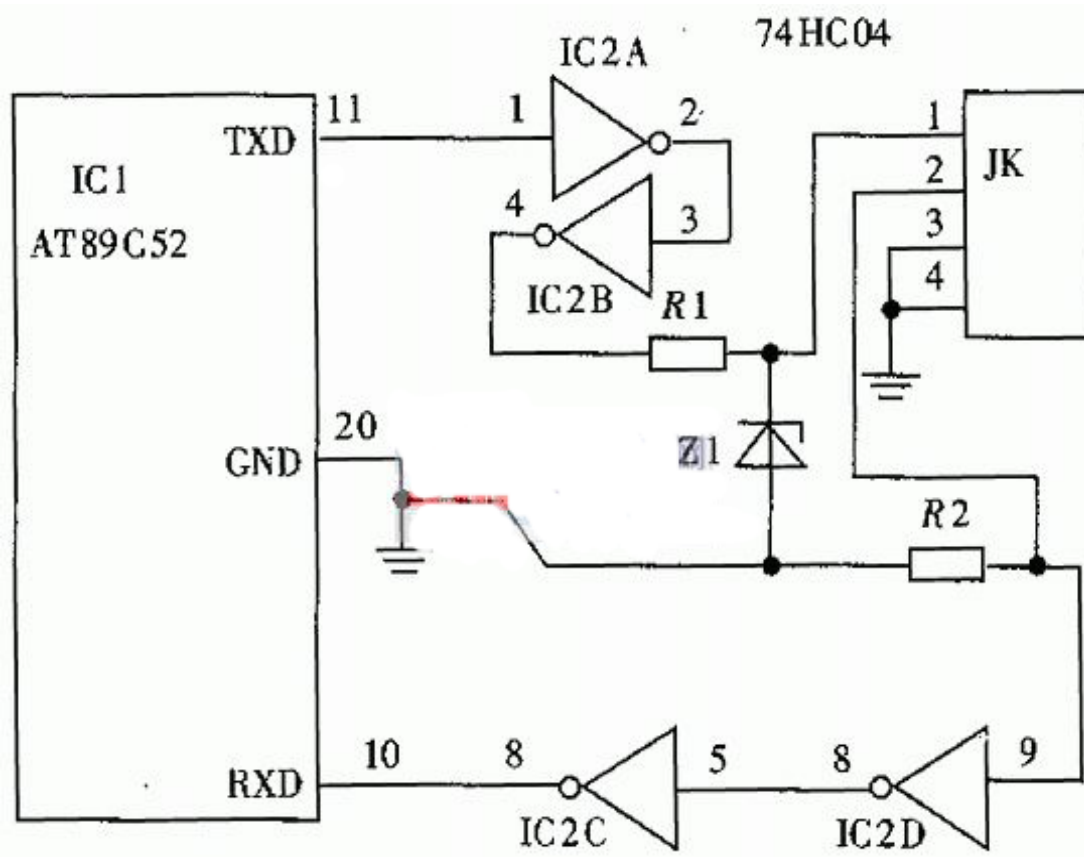


图 1 接口电路原理图

单片机与手机一般采用串行异步通信接口，具有红外和通信电缆两种连接方式，通信速度可设定，通常为 19200bps。采用红外接口的优点是单片机系统与手机电气隔离，相互不干扰，接口各自独立，使用方便；缺点是通信距离较短，红外传播的方向性对接口相对位置有要求。采用电缆连接时，数据传输的可靠性较好；其主要缺点是接口的电气参数不兼容，设计不当时会对手机的通信质量产生影响。笔者经过实践设计的接口电平转换电路如图 1。

GSM 的短信息业务 SMS 利用信令信道传输，这是 GSM 通信网所特有的。它不用拨号建立连接，把要发的信息加上目的地址发送到短信息中心，经短消息服务中心完成存储后再发送给最终的信宿。所以当目的 GSM 终端没开机时信息不会丢失。每个短消息的信息量限制为 160 字节。

现在市场上大多数手机均支持 GSM07.05 规定的 AT 指令集。该指令集是 ETSI（欧洲通信技术委员会）发布的，其中包含了对 SMS 的控制。利用 GSM 手机的串行接口，单片机向手机收发一系列的 AT 命令，就能达到控制手机收发 SMS 的目的。ETSI 的 GSM07.05 中用于 SMS 收发控制的主要 AT 命令见表 1。

表 1 常用 AT 指令

GSM07.05 Function(功能)

ATE0 RESET

AT+CSMS 选择短信息服务

AT+CPMS 选择短信息内存

AT+CMGF 选择短信息格式

AT+CSCA 短信息中心地址

AT+CNMI 显示新收到的短信息

AT+CMGR 读短信息

AT+CMGS 发送短信息

AT+CMGL 列出 SIM 卡中短信息

AT+CMSS 从 SIM 内存中发短信息

AT+CMGW 向 SIM 内存中写入待发短信息

AT+CMGD 删除 SIM 内存中的短信息

AT+CSCB 选择蜂窝广播信息

GSM 手机通过异步通信接口实现对 SMS 的控制共有三种接入协议：**Block Mode**；基于 AT 命令的 **TextMode**；基于 AT 命令的 **PDU Mode**。**PDU 模式**是发送或接收手机 SMS 信息的一种方法，短信息正文经过十六进制编码后被传送。目前，**PDU Mode** 应用最为广泛，基本上全国所有的电信局都提供支持 **PDU Mode** 的短消息业务。有些地址则不支持 **Text Mode** 和 **Block Mode**，这就限制了这两种接入协议的应用，而且 **PDU Mode** 已有取代 **Block Mode** 的趋势。为了保证系统具有广泛的适用性，本文采用 **PDU 模式**收发 SMS。

PDU 相当于一个数据包，它由构成消息（SMS）的信息组成。作为一种数据单元，它必须包含源/目的地址、保护（有效）时间、数据格式、协议类型和正文，正文长度可达 140 字节，它们都以十六进制表示。**PDU** 结构根据短消息由移动终端发起或以移动终端为目的而不同。

当由移动终端发起时，**PDU** 的格式为：

SMSC PDU 类型 MR DA PID DCS VP UDL UD (0~140octed)

当以移动终端为目的时，**PDU** 的格式为：

SMSC PDU 类型 OA PID DCS SCTS UDL UD (0~140octed)

其中，**SMSC** 为短消息业务中心地址，**DA/OA** 为源/目的地址，**PID** 为协议识别，**DCS** 为数据编码，**UDL** 为用户数据长度，**UD** 为用户数据，**VP** 为有效时间，**MR** 指明是发出信息，**SCTS** 指明短消息到达业务中心的时间。

2 PDU 格式下短信息的接收

根据设置不同，手机将收到的短消息保存在缓存单元或存入 SIM 卡，单片机从手机中接收短消息实质上就是从 SIM 或缓存中读出信息。这主要利用 AT+CMGR 和 AT+CMGL 两条指令来完成，其工作过程见图 2。

由于不同的厂商对 AT 指令集的解释代码和响应信息不一样，所以单片机首先要确认能否与手机建立起通信，一般用 ATE 指令完成此确认；然后用 AT+CMGF 指令选定短消息的数据格式；在收到手机的正确回答反以 AT 指令完成读出功能。一般用 AT+CMGL 读取以前的信息，在收到手机的 RING（振铃）数据时，用 AT+CMGR 读取实时信息。

以下是笔者设计的物流数据采集系统中用到的接收 SMS 的一个实例，它说明了 PDU 模式的应用。单片机发送和接收（手机回答）均为 ASCII 码。所用手机为 SIEMENS S3508i。

操作过程如下（{}内为注释）：

发送：ATE

手机回答：OK {已建立联接}

发送：AT+CMGF=0 {选用 PDU 格式}

手机回答：OK {允许选择 PDU 格式}

发送：AT+CMGL=2 {列出已有的短信息}

手机回答：+CMGL: 1, 2, , 24{1 表示信息个数，2 表示未发信息，24 表示信息总容量}

0D71683108370105F004000D81683179133208F10000026080410033802632184CF682D

95E0DC2B36D3D170A0243106933D97A0243106933D97A02451068B1983492608

OK

以上这组 PDU 格式的十六进制字符串，不但包含了短消息的内容，同时包含了发送者的手机号码、短信息中心号码、短消息发送时间等。

下面对信息内容进行分析：

0D: 短信息中心地址（号码）长度。

91: 短信息中心号码类型，91 是 TON/NPI。TON/NPI 遵守 International/E.164 标准，指在号码前需加 '+' 号；此外还可直有其他数值，但 91 最常用。

683108370105F0: SMSC 短信息所使用的服务中心号码 13807310500。它经过十六进制以字节为单位的高低半字节换位处理，号码是奇数的添 F，构成一个 HEX 字节。

04: PDU 类型，文件头字节。

0B: 主叫号码长度。

81: 主叫号码类型。

3179133208F1: 0A 主叫号码，也经过了处理，实际号码为 13973123801。

00: PID，为协议标识。

00: DCS 短信息编码类型是 GSM Default Alphabet，即由 7 位 ASCII 码移位组成 8 位十六进制码（octet），其方法见表 2。

1sthex B0 A6 A5 A4 A3 A2 A1 A0

2ndhex C1 C0 B6 B5 B4 B3 B2 B1

3rdhex D2 D1 D0 C6 C5 C4 C3 C2

4thhex E3 E2 E1 E0 D6 D5 D4 D3

5thhex F4 F3 F2 F1 F0 E6 E5 E4

6thhex G5 G4 G3 G2 G1 G0 F6 F5

6thhex H6 H5 H4 H3 H2 H1 H0 G6

02608041003380:SCTS 短信息发送时间，02/06/08/14: 00: 33.08。

26: UDL 经处理后的 8 位码（octet）短信息字节长度，它小于消息 ASCII 码的长度。

32184CF682D95E30DC2B36D3D170A0243106933D97A0243106933D97A02451068B1983492608: UD 编码后的 PDU 数据, 短信息内容“2002/06/08/13:48ID102OKID103OK ID201FAIL”。

3 短信息的发送

与接收短信息一样, 发送时也要先建立联接, 传送一些初始化指令, 然后发送短消息内容。下面是用 SIEMENS S3508i 发送一个短信息的例子, 内容为: “2002/06/08/13:48ID102OK ID103OK ID201FAIL”。其 ASCII 码为:

“32030322F30362F30382F31333A34382049443130324F4B2049443130334F4B2049443230314641494C20”。

发送: ATE {请求建立联接}

手机回答: OK {已建立联接}

发送: AT+CMGF=0 {选择 PDU 模式}

手机回答: OK

发送: AT+CSMS=0{检测手机是否支持 SMS 命令}

手机回答: OK

发送: AT+CMGS=52{发送短信息, 52 octets (不包括最初 9 个短信息元字节)}

手机回答: >{允许上传数据, ASCII 码是 (\$20H, \$2EH)}

发送: 0891683108701305F011000B813179133208F10000AA2632184CF682D95E30DC2B36D3D170A0243106933D97A0243106933D97A02451068B19834926081

A

不计最初 9 个短消息信元字节, 本短信息有 52 字节 (104 个字符)。AT+CMGS 仅说明了 SMSC 信息内容的长度, 在收到手机回答的 > 符号后才发送 PDU 数据串, 并以 (CTRL^Z) 结束。