

基于 GSM 短信技术的电网电压监测仪研制

潘天红, 盛占石

(江苏大学 电气信息工程学院, 江苏 镇江 212013)

摘要: 基于全球移动通信系统(GSM)技术的电网电压监测系统由多台短信电压监测仪、GSM 网络、IBM-PC586 上位机及电压监测统计管理软件 4 部分组成。介绍了短信电压监测仪的硬件(电压/电流信号的采样、滤波、信号调理、A/D 转换、显示、时钟、GSM-Modem 接口等)电路及其功能。讨论了 GSM 通信发送/接收短信息的编码规则与步骤以及短信电压监测仪的短信处理。

关键词: GSM; 短信; 电压监测; 通信; 协议描述单元

中图分类号: TM 933; TN 92

文献标识码: A

文章编号: 1006-6047(2005)07-0048-05

电网电压是衡量电网质量的重要指标。其运行状况是评价电网电压质量、生产调度管理、制订电网规划和技术改造计划的重要依据,也是考核系统运行管理水平的重要指标,无论是供电部门还是用电单位,对供电电压进行动态监测和记录势在必行^[1,2]。

近年来,全球移动通信系统(GSM)网络迅速发展^[3],使用成本也越来越便宜。GSM 的短信服务 SMS(Short Message Service)本身具备的数据传送功能^[4],使得电网电压监测出现新的模式:用 SMS 交换数据。本课题组在前期研究工作的基础上^[2],成功研制了第三代网络型电压监测仪:基于 GSM 技术的 DT 100G。

本监测仪能够实现多个回路同时监测,并根据需要实时与上位机管理软件交换数据。管理软件统计各监测点的电压最大值、最大值发生时刻、最小值、最小值发生时刻、运行时间、超上限时间、超下限时间、电压合格率、电网电压出现异常的类型(如:电网断电、超上限 10 min 等)与发生的时刻等,以及为用

户提供报表:同类电网电压的月报表、日报表、日整点电压值等,并且提供多种打印功能。

1 系统组成及原理

SMS 为 GSM 网络的一种基本业务,本系统基于该网络技术,实现数据无线传输,系统结构见图 1。

该系统由多台短信电压监测仪、GSM 网络、配置 GSM 终端的上位机(IBM-PC586),以及电压监测统计管理软件 4 部分组成。

1.1 短信电压监测仪

短信电压监测仪是系统的前端采集设备,具体负责电网电压数据的采集、显示、统计、监测、存储及无线传输。本监测仪可以监测 4 种类型的电压等级:A 类(如 220 V),B 类(如 3 kV),C 类(如 10 kV),D 类(如 220 kV)。同时,当电网电压出现异常时(如断电、电压超上限 10 min),它能主动向监控中心发送报警数据。另外,还可以接收管理中心控制命令,执行相应的数据传送与接收指令。

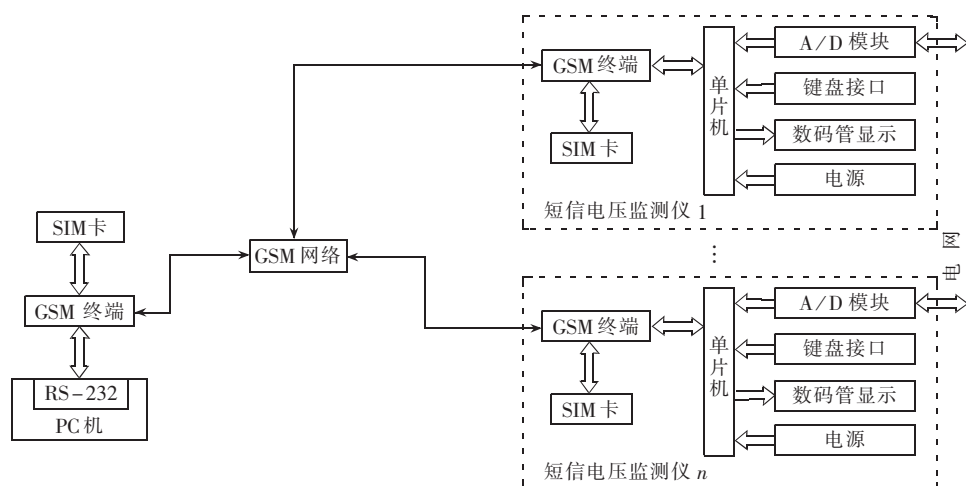


图 1 系统结构图

Fig.1 The structural diagram of system

1.2 GSM 网络

GSM 网络主要为短信电压监测仪与管理中心数据交换提供网络平台支持。该部分由移动通信维护,无需用户关心。

1.3 配置 GSM 终端的上位机

负责与分散各地的短信电压监测仪进行通信联络,接收各电压监测仪发送来的数据以及向各电压监测仪传送控制指令。

1.4 统计管理软件

负责对各监测点电网运行数据进行统计分析、查询、存储、图形显示、打印等功能。

2 短信电压监测仪的硬件结构与功能

本系统的下位机硬件结构如图 2 所示。
系统的下位机包括电压、电流信号的采样、滤波、

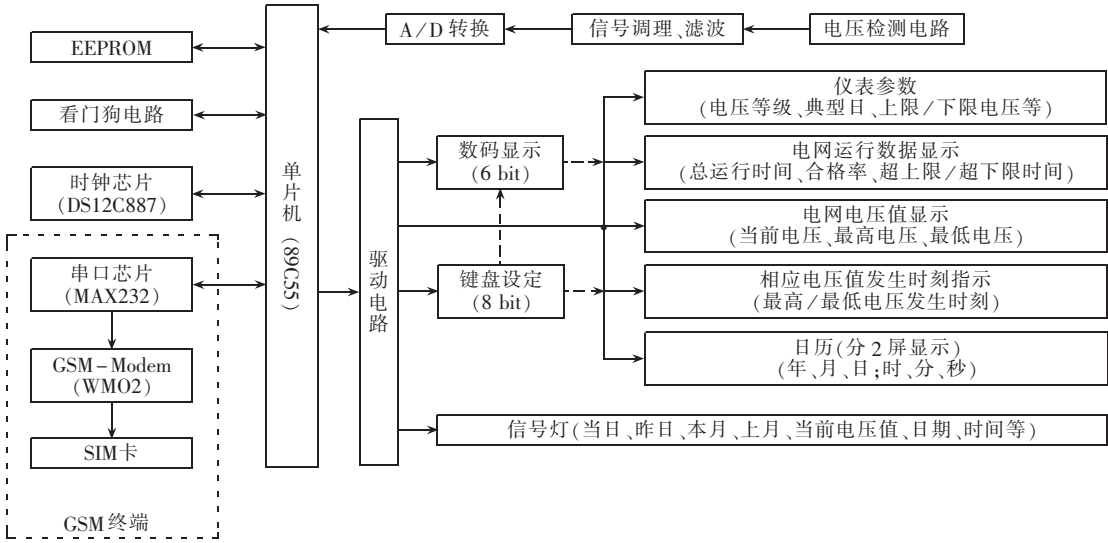
信号调理、A/D 转换、键盘显示、时钟、看门狗、GSM - Modem 接口等电路及 MCU 单元 AT89C55 等,能够完成如下功能。

a. 设定与显示仪表的当前时间:年(2 bit)、月(2 bit)、日(2 bit)、时(2 bit)、分(2 bit)、秒(2 bit),仪表第一次运行时需要校正相关的时间。

b. 实时采样监测。监测仪对被监测的电网电压采用有效值采样,其采样周期每秒 1 次,并作预处理存储。1min 作为 1 个统计单元,取 1min 内的电压预处理值的平均值,代表被监测系统实时运行电压。

c. 按查询功能,显示总运行时间、合格时间、合格率、超上限/超下限时间等。同样,仪表保存本月与上月,今日与昨日的此类相关数据。

d. 按查询功能,显示当前电压值、电压最大值及发生时刻、电压最小值及发生时刻等。同样,仪表



保存本月与上月,今日与昨日的此类相关数据。
e. 按键可读出昨日 24 h 整点的电压平均值。
f. 具有瞬时值超限报警(超上限/超下限 LED 闪烁报警)。
g. 自动日历系统,统计与自然月份吻合。
h. 按键设定仪表参数:仪表号、电压等级、超上限/下限电压值、典型日日期、仪表校正系数、仪表密码、日期与时间等。
i. 自动 SMS 数据交换。仪表出现异常情况(超上限 10 min、超下限 10 min、断电、来电 10 min 等),自动向短信中心发送异常数据;接收管理中心发送的操作命令,并返回相应内容。

3 GSM 通信接口的工作原理与编码实现

GSM 通信控制终端的接口一般采用目前在市场上提供的可供二次开发的标准 GSM 模块,如:FalcomA2D 系列、Wavecome 的 WMO2 系列、西门子的 TC35 系列、爱立信的 DM 10/DM 20 系列、中兴的 ZXGM 18 系列等。

这些模块的功能、用法差别不大,提供标准的 UART 串行接口,支持 GSM 07.05 所定义的 AT 命令集的指令^①。因此,微控制单元(MCU)能非常方便地通过 UART 接口与 GSM 模块连接,并直接使用 AT 命令就可以方便简洁地实现短信息的收发、查询和管理^[5]。本监测仪采用 GSM 通信模块为 Wavecome 的 WM 02 系列,硬件框图如图 2 所示。

GSM 短信终端通过异步通信接口实现对 SMS 的控制共有 3 种接入协议:Block Mode;基于 AT 命令的 Text Mode;基于 AT 命令的协议描述单元(PDU) Mode。其中以 PDU 模式应用最为广泛,基本上全国所有的电信局都提供支持 PDU Mode 的短消息业务,并已取代 Block Mode,为了保证系统具有广泛的适用性,本文采用 PDU 模式收/发 SMS。

与 SMS 有关的 GSM AT 指令(from GSM 07.05)如表 1 所示。

① AT command set for GSM Mobile Equipment(GSM 07.07 version 7.4.0 Release 1998).

表 1 相关的 GSM AT 指令
Tab.1 The relevant AT commands

AT指令	功 能
AT+CMGC	Send a SMS command (发出一条短消息命令)
AT+CMGD	Delete SMS message (删除 SIM 卡内存的短消息)
AT+CMGF	Select SMS message format (选择短消息信息格式;0-PDU;1-文本)
AT+CMGL	List SMS message from preferrrd store(列出 SIM 卡中的短消息 PDU/text;0/3 “REC UNREAD”-未读,1/“REC READ”-已读,2/“STO UNSENT”-待发,3/“STO SENT”-已发,4/“ALL”-全部的)
AT+CMGR	Read SMS message (读短消息)
AT+CMGS	Send SMS message (发送短消息)
AT+CMGW	Write SMS message to memory (向 SIM 内存写入待发的短消息)
AT+CMSS	Send SMS message from storage (从 SIN /M 内存中发送短消息)
AT+CNMI	New SMS message indications (显示新收到的短消息)
AT+CPMS	Preferred SMS message storage (选择短消息内存)
AT+CSCA	SMS service center address(短消息中心地址)
AT+CSCB	Select cell broadcast messages (选择蜂窝广播消息)
AT+CSMP	Set SMS text mode parameters (设置短消息文本模式参数)
AT+CSMS	Select Message Service (选择短消息服务)

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 Byte,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。单片机与 GSM 终端首先要建立联接,传送一些初始化指令,然后发送短消息内容,单片机发送和接收(GSM 终端回答)均为 ASCII 码。

3.1 发送短信息的编码规则与步骤

以一个例子说明其编码规则与发送过程:要向号码为“+8613218383701”发送 1 条短信息(号码转换为 683112383807F1),其内容为“你好”(变成 Unicode 为“4F60597D”,长度是 04)。

3.1.1 第 1 步

单片机发送:41 54 2B 43 4D 47 46 3D 30 0D(AT+CMGF=0,设置短消息格式为 PDU)。

GSM 终端应答:41 54 2B 43 4D 47 46 3D 30 0D 0A 4F 4B 0D 0A(返回“OK”)。

3.1.2 第 2 步(在收到“OK”后进行)

单片机发送:41 54 2B 43 4D 47 53 3D 30 31 39 0D(AT+CMGS=019,设置短信长度,19 为十进制数=15+2×中文短信长度)。

GSM 终端应答:41 54 2B 43 4D 47 53 3D 30 31 39 0D 0D 0A 3E 20(返回“>”)。

3.1.3 第 3 步(在收到“>”后进行)

单片机发送:30 30 31 31 30 30 30 44 39 31 36 38 33 31 31 32 33 38 33 38 30 37 46 31 30 30 30 38 30 31 30 34 34 46 36 30 35 39 37 44 1A(以“CTRL^Z”结束)。

GSM 终端应答:30 30 31 31 30 30 30 44 39 31 36 38 33 31 31 32 33 38 33 38 30 37 46 31 30 30 30 38 30 31 30 34 34 46 36 30 35 39 37 44 1A 0D 0A 2B 43 4D 47 53 3A 20 39 37 0D 0A 0D 0A 4F 4B 0D 0A(返回“+ CMGS:97 OK”)。

这组单片机发送 PDU 格式的字符串,其对应的内容为

0011000D91683112383807F1000801044F60597D

下面对信息内容进行分析:

001100 ① + 0D ② + 91 ③ + 683112383807F1 ④ + 000801 ⑤ + 04 ⑥ + 4F60597D ⑦

注解:① 001100:固定内容。

② 0D:短信息中心地址(号码)长度。

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

④ 683112383807F1:对方(接收方)的手机号码 13218383701。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。

⑤ 000801

a. 00 是协议标识 TP-PID,一般为 00,各位阐述如下:

No.7	No.6	No.5	No.4	No.3	No.2	No.1	No.0
------	------	------	------	------	------	------	------

No.7 与 No.6:一般设置为 00;

- No.5:0——文本未压缩,
1——文本用 GSM 标准压缩算法压缩;
- No.4:0——表示 Bit No.1,bit No.0 为保留位,不含信息类型信息,
1——表示 Bit No.1,bit No.0 含有信息类型信息;

No.3 与 No.2:00——默认的字母表,
01——8 bit,
10——USC2(16 bit),
11——预留;

No.1 与 No.0:00——Class 0,只显示,不储存,
01——Class1,储存在 ME 内存中,
10——Class2(SIM 卡特定信息)储存在 SIM 卡中,

11——Class3 直接传输到 TE。

b. 08:数据编码方案 TP-DCS,USC2 编码(汉字编码)。

c. 01:有效期 TP-VP。

VP value(&h)	相应的有效期
00 to 8F	(VP+1)*5 min
90 to A7	12 h+(VP-143)*30 min
A8 to C4	(VP-166)*1 d
C5 to FF	(VP-192)*1周

⑥ 04:短信长度(2×中文短信长度)。

⑦ 4F60597D: 短信内容 —— 你好,7D —— 累加和。

3.2 接收短信息的编码规则与步骤

根据设置不同,GSM 终端将收到的短消息保存在缓存单元或存入 SIM 卡,单片机从 GSM 终端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+CMGL2 条指令完成。以读取 1 条未读短信说明接收过程。

3.2.1 第 1 步

单片机发送:41 54 2B 43 4D 47 46 3D 30 0D(AT+CMGF=0,设置短消息格式为 PDU)。

GSM 终端应答:41 54 2B 43 4D 47 46 3D 30 0D 0A 4F 4B 0D 0A(返回“OK”)。

3.2.2 第 2 步(在收到“OK”后进行)

单片机发送:41 54 2B 43 4D 47 4C 3D 30 0D(AT+CMGL=0,读取未读短信)。

GSM 终端应答:41 54 2B 43 4D 47 4C 3D 30 0D 0D 0A 2B 43 4D 47 4C 3A 20 32 2C 30 2C 2C 32 34 0D 0A 30 38 39 31 36 38 33 31 31 30 33 30 34 31 30 35 46 30 32 34 30 44 39 31 36 38 33 31 36 35 31 34 31 31 32 30 46 37 30 30 30 38 35 30 32 30 34 32 32 32 38 35 34 32 30 30 30 34 34 46 36 30 35 39 37 44 0D 0A 0D 0A 4F 4B 0D 0A。

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。其对应的字符串内容为

```
AT+CMGL=0
+CMGL:1,0,,24
0891683110304105F0240D916831651
41120F7000850204222854200044F60
597D
```

下面对信息内容进行分析:

a. +CMGL 1,0,,24(1 表示信息位置,0 表示未发信息,24 表示信息总容量);

b. 08①+91②+683110304105F0③+24④+0D⑤+91683165141120F7⑥+0008⑦+502042228542⑧+

0004⑨+4F60597D⑩。

注解:① 08:短信息中心地址长度,指(91)+(683110304105F0)的长度。

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

③ 683110304105F0:SMSC 短信息所使用的服务中心号码 13010314500。号码是奇数的添 F,构成一个 HEX Byte。

④ 24:为基本参数(TP-MTI/MMS/RP)。

⑤ 0D:号码长度(2×中文短信长度)。

⑥ 91683165141120F7:对方的手机号码+8613564111027。

⑦ 0008 中 00 是协议标识,08 为 UCS2 编码。

⑧ 502042228542:消息发送的日期,05-02-24 22:58:24。

⑨ 0004:短信长度。

⑩ 4F60597D:短信内容 —— 你好,7D —— 累加和。

4 短信电压监测仪短信处理

本电网电压监测仪 GSM 模块接收到的短信息保存到 SIM 卡的 EEPROM 中,不同 SIM 卡所能保存短信的条数不一样(10 条或 20 条)。及时判断 SIM 卡是否有数据中心发来的短信内容非常重要。在设计中,定时向 GSM 模块发查询内容:AT+CMGF=4,根据返回的信息,读取 SIM 卡中是否有短信。如果有,则读取短信内容,并删除 SIM 卡中的已读取的短信,保证 SIM 卡有足够的控件接收下 1 条短信。另外 MCU 的通信口处于监听状态,如果有新短信来临,则触发串行口中断,及时读取上位机传送的命令与内容。

短信收发流程图如图 3 所示。

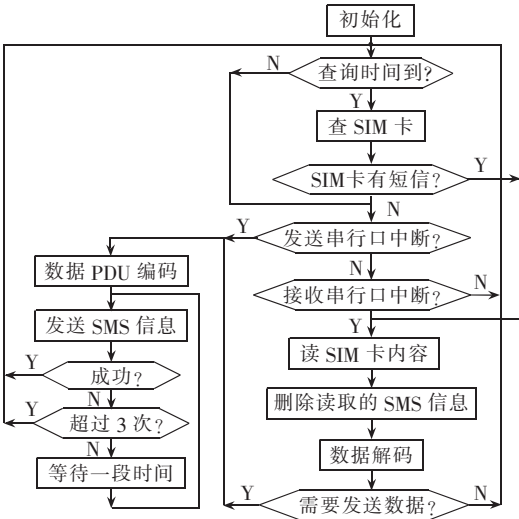


图 3 监测仪收发短信流程图

Fig.3 The flowchart of short message receiving and transmitting by instrument

为了保证上位机管理软件与短信监测仪数据交换的有效性,防止恶意短信的干扰,在通信中,设计了固定的数据报文格式^[6]:

长度(1 Byte)+命令(1 Byte)+内容(n Byte)+校验和(1 Byte)

其中,长度=命令+内容(字节数相加);校验和=长度+命令+内容。

如果短信内容不符合上述要求,则认为是无效的短信,直接从SIM卡中删除该条短信,否则按照约定的格式拆包,并执行相应的操作。

5 结论

利用GSM模块,研制了DT100G型电网电压监测仪,测试使用表明,该监测仪各项指标达到设计要求,符合DL500-92电压监测仪技术条件,成本较低,利于系统集成。特别在偏远地区、海岛等架设通信线路困难或不经济的地方,工程服务设施可以自由灵活地设置,不再受地形条件的限制,具有良好的应用前景。

参考文献:

- [1] 漆文辉,银 晖.智能电压监测仪的研制[J].电网技术,2001,25(3):59-63.
QI Wen-hui,YIN Hui. Development of an intelligent voltage monitoring instrument[J]. **Power System Technology**,2001,25(3):59-63.
- [2] 陈 山,潘天红,盛占石,等.分布式电网电压监测系统的研制[J].电力自动化设备,2003,23(2):58-60.
CHEN Shan,PAN Tian-hong,SHENG Zhan-shi,*et al.* Design of distributed electrical net voltage monitoring system [J]. **Electric Power Automation Equipment**,2003,23(2):58-60.
- [3] 熊 胜. GSM网络结构现状及其发展[J].湖北邮电技术,1999,3(3):12-17.

- XIONG Sheng. The frame status and development of GSM[J]. **Hubei Post & Telecommunications Technology**,1999,3(3):12-17.
- [4] 朱光喜,张耀华.如何解析GSM短消息[J].通信技术,2003,135(3):54-56.
ZHU Guang-xi,ZHANG Yao-hua. How to solve the GSM short messages[J]. **Communication Technology**,2003,135(3):54-56.
- [5] 李 鸿.用单片机控制手机收发短信息[J].电子技术应用,2003,29(1):24-26.
LI Hong. The SMS controlled by single-chip computer[J]. **Application of Electronic Technique**,2003,29(1):24-26.
- [6] 任 侠,陈国虎.基于VB的远程通讯程序[J].计算机应用,1999,19(2):61-62.
REN Xia,CHEN Guo-hu. The communication program based on VB[J]. **Computer Application**,1999,19(2):61-62.
- [7] 李正明,盛占石,谭延良.基于公用电话交换网的电压监测系统软件设计[J].微型机与应用,2001,20(9):45-47.
LI Zheng-ming,SHENG Zhan-shi,TAN Yan-liang. The software design of voltage monitor system based on PSTN [J]. **Microcomputer & Its Application**,2001,20(9):45-47.
- [8] 沈 正,李正明,盛占石.基于Modem的电压监测系统软件平台设计与实现[J].江苏理工大学学报(自然科学版),2001,22(3):79-83.
SHEN Zheng,LI Zheng-ming,SHENG Zhan-shi. The software design of voltage monitor system based on modem [J]. **Journal of Jiangsu University of Science and Technology(Natural Science)**,2001,22(3):79-83.

(责任编辑:汪仪珍)

作者简介:

潘天红(1974-),男,安徽泾县人,讲师,博士研究生,现从事信号监测与微型机控制方面的工作(E-mail:thpan@ujs.edu.cn);

盛占石(1958-),男,江苏大丰人,副教授,硕士,现从事信号监测与微处理器应用方面的工作。

Design of power network voltage monitoring instrument based on SMS technique of GSM

PAN Tian-hong,SHENG Zhan-shi

(School of Electrical and Information Engineering,Jiangsu University,Zhenjiang 212013,China)

Abstract: The power network voltage monitoring system based on GSM(Global System for Mobile communication) consists of several SMS(Short Message Service)-based voltage monitoring instruments, GSM network,IBM-PC586 superordinate computer and statistical management software for voltage monitoring. Its hardware is introduced,such as circuits of voltage/current signal sampling,filtering,conditioning,A/D converter,display,clock,GSM-modem interface and so on,and its functions are described as well. The coding rules and steps of receiving/transmitting short messages through GSM and the further processing by voltage monitoring instrument are discussed.

Key words: GSM; SMS; voltage monitoring; communication; protocol data unit