(9)

单片机扩展标准微机键盘的技术

山东省潍坊医学院计算机中心(261042) 荣 振
山东省潍坊第二人民医院(261041) 梁 华 王春生

26-28 TP364.23 TP368.1

摘 要：一种只利用单片机1根通信线就可实现对标准微机键盘扩展，并可实现单片机与标准微机键盘之间进行异步通信的方法。

关键词：标准微机键盘 单片机 异步通信

用单片机扩展键盘一般有2种方式，一种是并行方式，即利用单片机的并行I/O口，如要扩展16(4*4)键，需要8位I/O线；另一种是串行方式，即利用串转并集成电路164以及单片机的2位串行口线和若干位I/O线，如要扩展16键，需要1片集成电路164及2位串行线和2位I/O线，并且不管是分立元件的键盘还是薄膜键盘，其键数、颜色和面积一但增加，成本均在几十元以上(还不包括制板费，键盘壳等其它费用)。

标准微机键盘的技术及工艺成熟、可利用的键码数多达近百个，随着制造工艺的进步，其价格不断下降，现在一般键盘的零售价在40元左右，新的老式键盘只需20~30元即可买到。特别是对于那些希望占用单片机的系统资源少而需要扩展的键数又多、仪器整体需要美观大方的设计者，其性能价格比显得更为优越。

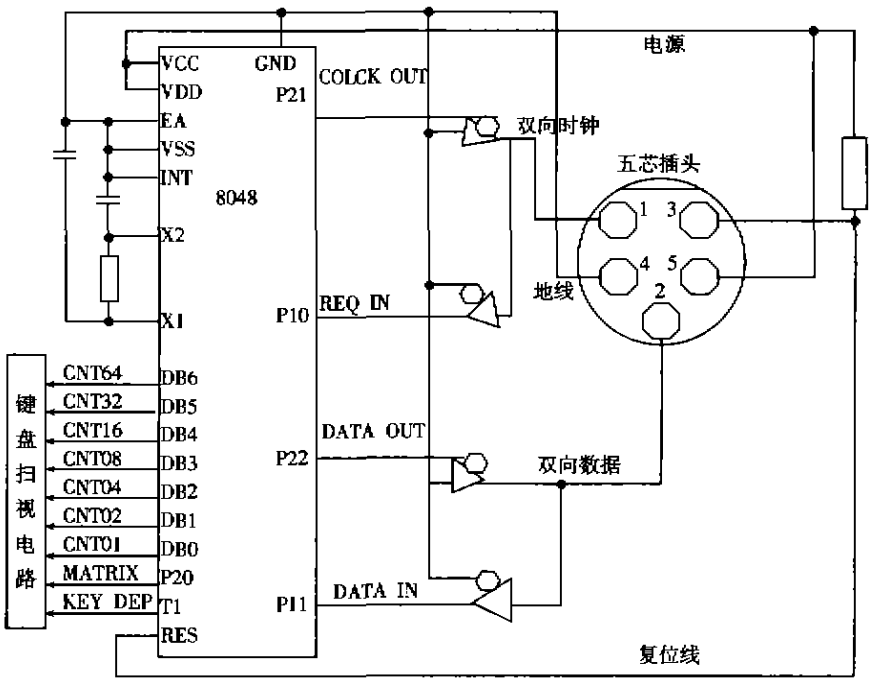

图1 键盘处理器发送扫描码逻辑

1 工作原理与硬件结构

如图1所示，微机键盘上的单片微处理器在加电自动复位后，就开始扫描监视键盘电路，一旦有键被按下，键盘处理器就按照复位时的异步通信波特率缺省值，通过串行数据DATA OUT端和时钟定位CLOCK OUT端，将按下键的扫描码发送出去。同样，系统机CPU也可通过这2根双向线向键盘串行传送数据，以控制键盘的动作。键盘处理器发送的扫描码为1字节码，与键位或ASC码并非同值，部分键的扫描码如表1所示。这里要特别指出的是，当某键被按下后，键盘处理器发出的是连续3个字节的数据，第1个字节是接通扫描码，其后是2个字节的断开扫描码，在这3个字节中，第1和第3字节相同，为键的扫描码，中间字节为固定值F0H。如“A”键为1CH、F0H、1CH。键盘扫描码的发送完全按串行异步通信格式进行，其规定如图2所示。

表1 部分键值与键值扫描码对照表

键	1	2	3	4	5	6	7	8	9	0	Q	W	E	R	T	Y	U
码	16	1E	26	25	2E	36	3D	3E	46	45	15	1D	24	2D	2C	35	3C
键	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B
码	43	44	4D	1C	1B	23	2B	34	33	3B	42	4B	1A	22	21	2A	32

起始	D0	D1	D2	D3	D4	D5	D6	D7	奇偶	停止

图2 键扫描码发送格式

单片机内的串行口可以提供4种工作方式，其中方式2、方式3的串行异步通信格式与键盘的通信格式完全相同。但这里存在一个关键问题，即键盘的串行通信和单片机的串行通信均以控制对方的通信时钟为前提，二者

之间进行通信必须使其通信时钟相同。对于单片机的应用，主要以接收和识别来自键盘的扫描码为目的，因此利用单片机串口的方式3(波特率可变)，使单片机串口的通信时钟满足键盘发送的通信时钟频率。图3为键盘接口与单片机之间的硬件连接图，其中虚线部分的P3.4与CLOCK OUT连线是为了预先测量键盘通信时钟频率而临时设置的，实际电路也可将此连接去掉。

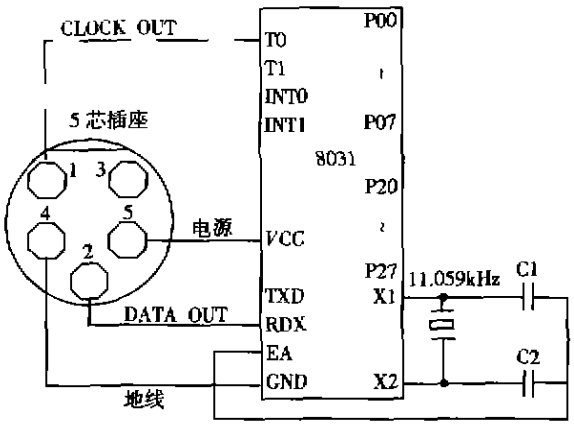

图3 单片机与微机键盘插座连接图

2 软件设计原理

首先利用P3.4与CLOCK OUT连线测量键盘通信时钟频率。即利用P3.4接收键盘发出的通信时钟方波、并利用定时器1以单片机自己的主振频率为基准对该方波的周期进行测定。若1个方波对应于M个机器周期，则根据M可计算出由定时器1作波特率发生器时，要产生与键盘相同的波特率，TH1应预置多大的值。为了提高换算的精度和便于计算，可以测8个或16个方波的机器周期数。

在模式2时，定时器1的溢出率为：

T1溢出率=T1计数速率/[256-(TH1)]

TI计数速率=$f_{OSC}/12$ (1)

因此：

BR=(2smod/32)×(f_{osc}/12)/(256-(TH1)) (2)

f_{OSC}为单片机主振频率，BR为波特率。

MCS-51 1个机器周期的时间为t=12/fosc，由于1个方波的周期T等于2位串行数据的时间、则传送1位数据所需的时间为$0.5\times M\times t=6M/f_{osc}$，根据式(1)和式(2)、且令SMOD=1，可算得：

TH1=256-M/32 (3)

如果测定8个方波的机器周期数，则式(3)改为

TH1=256-8M/256 (4)

根据式(4)，给出方波测定子程序ST及如图4的框图。

```
ST: MOV R4,#8          ;测8个方波
    MOV TMOD,#01H      ;TI为模式1
    MOV TH1,#0         ;T1清零
    MOV TL1,#0
H1: JNB P3.4,H1
H2: JB  P3.4,H2        ;第1个方波下跳
    SETB TR1           ;启动T1
H3: JNB P3.4,H3
H4: JB P3.4,H4
    DJNZ R4,H3
    CLR TR1            ;停止T1
    MOV A,TL1          ;开始计算TH1
    RR A
    ADDC A,TH1         ;A=8M/256
    MOV R0,#255
    XCH A,R0
    CLR C
    SUBB A,R0          ;A=255-(8M/256)
    DEC A
    DEC A              ;误差调整
    MOV TH1,A          ;串口方式3时定时器1
    MOV TLI,A          ;应设置的值
```

我们选用晶振为11.059kHz的单片机对键盘进行测试，其串口为方式3、定时器1应设置的值为"0FBH"。下面介绍单片机扩展标准微机键盘的驱动程序(即异步通信程序)、第一种方法是利用上面程序ST测试出的值(假设为TT)编制的程序KEY1及如图5所示的框图。

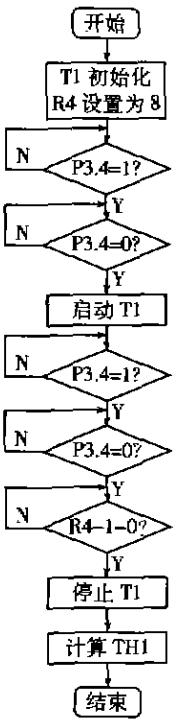

图4 键盘时钟测定子程序ST框图

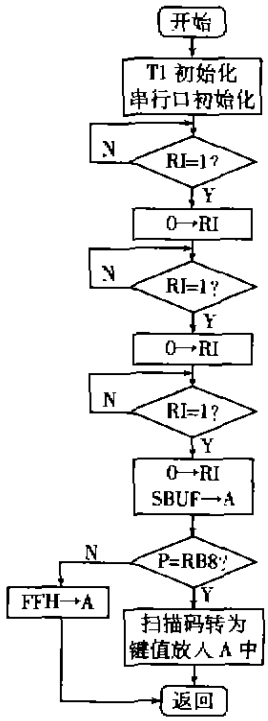

图5 键盘驱动子程序KEY1框图

```
KEY1: MOV TMOD,#20H    ;T1编程为方式2定时
      MOV TH1,#TT      ;用ST测出的值初始化T1
      MOV TL1,#TT
    SETB TR1           ;启动TI
```

TCP 代码的安全性分析

西安交通大学硕 810(710049) 蒋旭宪 张德运 张 勇

摘 要：从分析 TCP 状态的转化图入手，讨论了 TCP 代码实现中可能存在的安全性方面的问题，并给出相应的改善措施。

关键词：TCP/IP 网络安全 TCP 状态转化图 TCP 代码

在诸多网络协议中，最重要的也是应用最广泛的协议是 TCP/IP 协议簇。TCP/IP 协议簇包括许多协议：如 ICMP、IP、TCP、UDP 等。但各协议中潜在着安全漏洞(exploits)：TCP 序列号攻击、IP 地址欺骗、IP 源路由的使用以及应用 ICMP 协议进行 DoS (Deny of Service) 攻击等。由于许多重要的应用程序都是面向连接，即基于 TCP 的、如简单邮件传输协议 SMTP、telnet 终端服务、r-命令(rlogin，rsh 等)、FTP 等。TCP 代码实现中如果存在安全漏洞、就会带来巨大的安全隐患。

本文通过分析 TCP 协议实现的状态转化图和定时器(Timers)的应用，指出可能存在的安全漏洞，并说明黑客是如何利用这些漏洞来进行攻击的，同时提出相应的改善和补救措施。

1 TCP 的状态转化和定时器的应用

TCP 连接状态的初始化、建立和终止是随着 TCP 状态的变化而变化的。TCP 状态转化图如图 1 所示。具体的 TCP 状态的定义和转化可参考文献[2]。

从图 1 中可以看出，状态的改变是与定时器密切相关的。TCP 连接的建立、终止、流控和数据的重传都与定时器有关。下面是一些比较关键的、对系统性能有很大影

(接上页)

```
        MOV 87H,#80H  ;设波特率系数(SMOD)为 1
        MOV SCON,#0D0H  ;串行口为方式 3 接收
WAIT:   JBC RI,W1     ;等待键盘按下后发出的
        JMP WAIT      ;第 1 字节数据
W1:     JBC RI,W2     ;放弃第 1 字节数据
        JMP W1        ;等待第 2 字节数据
W2:     JBC RI,PRI    ;放弃第 2 字节数据
        JMP W2        ;等待第 3 字节数据
PRI:    MOV A,SBUF    ;接收键盘扫描码
        JNB PSW.0,PNP ;奇偶校验
        JNB RB8,PER
        SJMP RIGHT
PNP:    JB RB8,PER
        SJMP RIGHT
PER:    MOV A,#0FFH   ;奇偶校验出错
        RET           ;返回值为"FF"
RIGHT:  MOV B,A       ;利用查表法将扫描码
        MOV R2,#0H    ;转化为具体键值
LOOP:   MOV A,#7
        ADD A,R2
        MOVC A,@A+PC
        INC R2
        CJNE A,B,LOOP
        DEC R2
        MOV A,R2      ;返回的键值在 A 中
        RET
TAB:    DB 45H,16H,1EH,26H,25H,2EH,36H,3DH
                                  0,1,2,3,4,5,6,7
        DB 3EH,46H,1CH,32H,21H,23H,24H,2BH
                                  8,9,A,B,C,D,E,F
        DB
```

运行此程序后：(1)单片机等待键盘有键按下，根据键盘某键按下即连续发出 3 个字节数据的特点、放弃前 2 个，取最后 1 个字节的扫描码，经奇偶校验后，将正确的扫描码转化为具体键值；(2)单片机利用键按下后发出的第 1 个字节测量键盘通信时钟频率，以初始化串口方式 3 时定时器 1，并以此为基准、接收第 3 字节的键盘扫描码，可根据程序 ST 和 KEY1 来编制此程序 (此方法需要借助 P3.4 与 CLOCK OUT 之间的联接)。

在此技术中，由于微机键盘的通用性、可靠性及性能价格比等优点，在我们所设计并已投入市场的"心功能检测诊断仪"中得到了较好的应用。

(收稿日期：2000-02-31)