TEMIC 系列射频卡读写器的研制

摘要:介绍了 TEMIC 系列射频卡的一种读写器,它可以对 ATMEL 公司的 TEMIC 系列射频卡 E5550、E5551 和 T5557 进行读写。通过使用这个读写器，可以对上述射频卡进行块写、块读、规则法、工作模式设置、密码设置、取消密码和更改密码等操作。

关键词：射频卡 U2270B AT89S52

射频卡是一种非接触式智能 IC 卡,是近几年发展起来的一项新技术。它没有接触式 IC 卡的电气触点，而是通过无线电波进行数据传输，相对于传统的接触式 IC 卡具有可靠性高、寿命长等明显优势，因而得到了广泛应用。当前实际应用中主要采用的是以 ATMEL 公司的 TEMIC 系列为主的 125kHz 射频卡和以 PHILIPS 公司的 MIFARE 技术为核心的 13．56MHz 射频卡。

本文采用ATMEL公司的AT89S52 单片机和该公司TEMIC系列射频卡的读写基站芯片U2270B研制开发TEMIC系列射频卡读写器。

图 1

1 TEMIC系列射频卡特性及原理

TEMIC 系列射频卡的特点为：

(1)低功耗、低电压的 CMOS 结构；

(2)无线电源供给，无线数据传输；

(3)射频频率为 100~150kHz；

(4)264bit 的 EEPROM，且有写保护功能；

(5)加密逻辑、唤醒功能，多种波特率，多种编码方式。

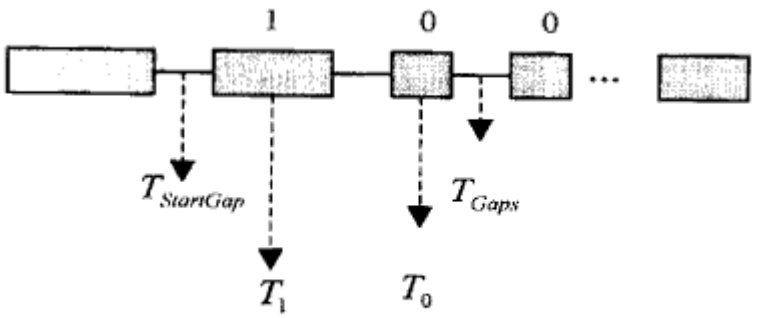

图 2 写卡数据流示意图

TEMIC 系列射频卡内有 264bit 的 EEPROM,被分成 8 块(block)，每块为 33bit，其中 bit0 是 lock 位，此位

一旦写"1"后，该块数据就不能再作任何修改。8 个 block 中，block0 是控制块，用来控制卡的各种操作特性，如同步信号、编码方式、波特率、数据流长度、加密和口令唤醒等功能的启用关闭等；blockl~bloc6 是用户块，用来存放用户数据和信启、；block7 是密码块，若加密功能不被启用，也可以作为用户块使用。

在使用射频卡之前都要先设置射频卡的工作模式，这可通过设置控制块 block0 来完成。TEMIC 系列射频卡的工作模式设置为：基站工作在 125kHz 的载波频率下，采用 RF / 32 的传输波特率和 Manchester 编码，使用 Sequence Terminator 同步信号，循环发送 blockl~block6 的数据。在这样的工作模式配置下，位时钟周期 T=32/RF=（32×10 6）/（125×10 3）μs=256μs。

TEMIC 系列射频卡的读卡过程为：射频卡先发送 Sequences Terminator 同步信号(粗线条部分)，接着依次发送经过 Manchester 编码后的 blockl~block6 的数据，发送完 block6 数据的最后一位后(bitt32)，又重新开始，不断循环发送。读卡的数据流如图 1 所示。Manchester 编码采用由低电平向高电平的跳变表示数据位为"1"，而用由高电平向低电平的跳变表示数据位为 "0"。结合 Manchester 编码的这个特点可以这样进行解码：在位时钟周期的下降沿(即半周期)处检测电平的变化情况，如果检测到电平变化发生，则继续判断变化后的电平情况，是高电平则该位解码为"1"，低电平则解码为"0"，没有跳变发生则视为信号异常，进行出错处理。

基站给射频卡发送数据时也要对数据进行编码，使数据信号加载到天线的发射信号中。TEMIC系列射频卡的基站芯片使用一种改变发射天线负载的方式对信号进行编码。这可以通过打开、关断天线(即把CFE(2)管脚设置为高、低电子)产生短暂的RF信号间隔(gap)来把RF信号分割成不同长短的区间的方法对数据进行编码。起始间隔(Start Gap)一般比数据间的间隔略长、用来与射频卡同步。一般起始间隔TStartGap =330μs，数据间间隔TGaps=300μs。在发送数据时，一个时间长度大约为To=1001xs的RF区间表示数据为"0"，一个时间长度大约为T1=350μs的RF区间表示数据为"1"。在编写程序时可以使用延时中断RF区域的方法进行发送数据。写卡时基站发送给卡片的数据流(RF区域状态)如图 2 所示。

图 3

阴影部分为打开RF信号的时长，连接线部分为关断RF信号的时长。TEMIC系列射频卡各段区间的时间长度为：

2 系统的硬件构成

本系统选用 AT89S52 单片机作为主控模块，与 TEMIC 系列射频卡读写模块、串口通信模块和声光提示电路共同构成了一个 TEMIC 系列射频卡读写器系统。系统硬件原理图如图 3 所示。

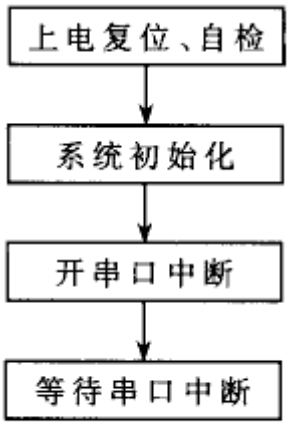

图 4 主程序框图

2．1 主控模块--AT89S52 单片机

AT89S52 单片机是一种低功耗、高性能的 CMOS 8 位单片机，它具有 MCS-51 系列单片机的优点，并且在指令和管脚封装上与 MCS-51 系列单片机相兼容，同时片内具有 Watchdog 功能，当程序由于某种干扰而死机时，系统可以可靠复位，保证系统的正常运行。

2．2 TEMIC 系列射频卡读写模块

其作用是完成同 TEMIC 系列射频卡之间的数据通信。该读写模块以 ATMEL 公司 TEMIC 系列射频卡的读写基站芯片 U2270B 为核心，如图 3 中右侧所示。

天线：基站天线需要用户自己绕制。一般用铜制漆包线绕直径为 3cm 的圈 150 圈即可，电感值为 1.35mH。

载波频率 fOSC：典型值为 125kHz，也可以由用户自己设定。此频率是由流入 RF(15)管脚的电流值决定的，所以通过调节 RF(15)和 VS(14)管脚之间的限流电阻 Rf1 和 Rf2 的值就可以改变此频率。具体的计算公式如下：

Rf1+Rf2=(14375/fosc)-5

CIN 和 CHP：基站从射频卡读人的是经过 125kHz 载波调制后的信号，它通过 CIN 电容耦合输入到 INPUT(4)管脚，经过低通滤波器、放大器、施密特触发器等几个环节后，在 OUTPUT(2)管脚输出解调后的信号。低通滤波器的截止频率由 fOSC 决定，一般为 fOSC / 18。INPUT 管脚的耦合电容 CIN 以及 HIPASS(16)管脚的去耦电容 CHP 的值决定了解调电路的高通特性，有利于更进一步滤除无用及干扰信号。CIN 和 CHP 的值依射频卡的数据传输波特率的不同而不同，波特率为 fOSC / 32 时分别为 680pF 和 100nF。CHP 与下限截止频率的关系如下：

fcut=1/(2×π×CHP×Ri)

式中，Ri=2．5kΩ。需要注意的是，OUTPUT 管脚输出的信号只是经过了解调，并没有解码。解码任务要通过单片机编程完成。

2．3 串口通信模块

主要由 MAX232CPE 构成，用作 AT89S52 的串行通信接口(SCI)的 TTL 电平和计算机串口的 RS232 电子之间的转换。计算机通过该串口通信模块可以给 AT89S52 发送读、写卡等命令，AT89S52 通过该串口通信模块把读卡结果回送给计算机。

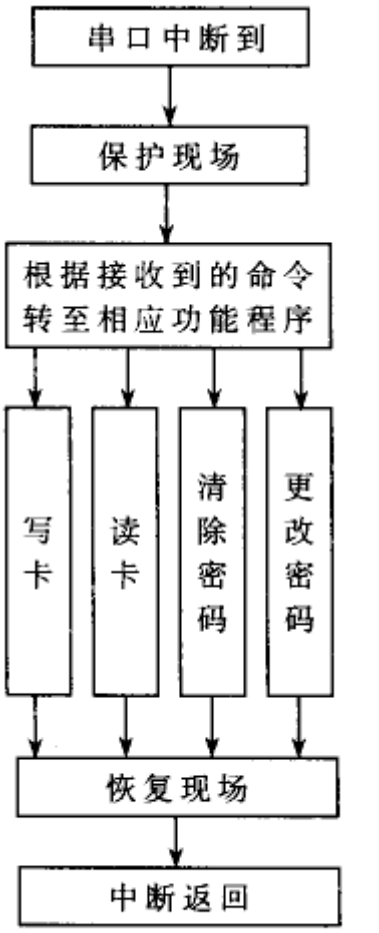

图 5 串口中断程序框图

2．4 声光提示电路

它由发光二极管和蜂鸣器构成。如果读写卡成功，发光二极管会闪一下，而且蜂鸣器也会响一声，用于提示用户。

3 系统的软件设计

假定基站工作在 125kHz 的射频频率下，采用 RF／32 的传输波特率和 Manchester 编码，使用 Sequence Terminator 同步信号，循环发送 block1~block6 的数据。

软件采用 MCS-51 系列汇编语言按照模块化结构进行编写，主要由主程序、串口中断程序两大模块组成。

主程序框图如图 4 所示。首先进行系统初始化，包括初始化 I／O 口、设置串口波特率等，然后开串口中断并进入"等待串口中断"，不断等待串口中断的到来。

串口中断程序模块执行的功能主要是根据计算机发出的命令进行相应的操作(读卡、写卡、取消密码和更改密码等)。串口中断程序框图如图 5 所示。

读卡协议描述:计算机通过串口给读写器发送 Ry 命令,Y 为 0~6 之一。当 y=0 时,读卡的 blockt~block6 的 6 块数据，当 y 为 1~6 之一时，读卡的相应块的数据。读卡成功则把相应数据通过串口回送给计算机。

写卡协议描述：计算机通过串口给读写器发送 WyPPPPPPPPXXXXXXXX 命令，y 为 0~7 之一，指定要写的块；PPPPPPPP 为卡的密码；XXXXXXXX 为要写入指定块的数据。在加密方式下，只有密码 PPPPPPPP 正确才闭以成功把数据写入卡中。在非加密方式下，密码 PPPPPPPP 可为任意数字。

取消密码和更改密码：它们的命令分别为 QPPPPPPPP 和 MPPPPPPPPpppppppp。取消密码实际上就是把卡从加密方式改为非加密方式，通过更改控制块 block0 的数据即可实现。更改密码实际上是先取消密码，然后往密码块 block7 写入新密码，并把卡设为加密方式。

本文设计的 TEMIC 系列射频卡读写器能够读写多种 TEMIC 系列射频卡，如 E5550、E5551 和 T5557 等，读写距离在 2～10cm 范围内。该读写器操作方便灵活，只要通过计算机串口按规定协议发送命令给它即可完成读卡、写卡、取消和更改密码等操作。本读写器已经实际应用在温州某非接触式 IC 卡预付费电度表的售电系统中，系统运行良好、可靠性高。