一种采用曼码调制的非接触 IC 卡读写程序编制

简 介 非接触 IC 卡技术有十分良好的应用前景。本文从应用角度介绍了 e5550/U2270B 器件组构成的一种低频非接触 IC 卡系统，并对采用曼彻斯特码调制进行信息交互时的读写操作做了详尽分析，最后给出用 C 语言编写的相应源程序。

关键词 非接触 IC 卡 曼码调制 非接触 IC 卡的读写操作

导 言

非接触 IC 卡技术已广泛应用于诸如电子交易，医疗保健凭证，驾车授权凭证，车辆加油管理系统，家居、公司办公通道，各种限权进入场所的门禁，各类电、水、热能和煤气计量表具的预付费系统，乃至宠物识别等。因其使用便捷、安全，日益为有关技术领域的工程师所关注。

图 1 采用 e5550/U2270B 的非接触卡读写系统示意图非接触 IC 卡是一种接口电路。它通过卡上配置的发射机应答器振荡线圈与基站振荡线圈的耦合取得能量，通过必要的通信软件配合，保证卡与基站间实现双向数据交换，如图 1 所示。许多著名厂商，如 Simens、Philips、Temic 等半导体公司，均有各具特色、性能优异的产品。

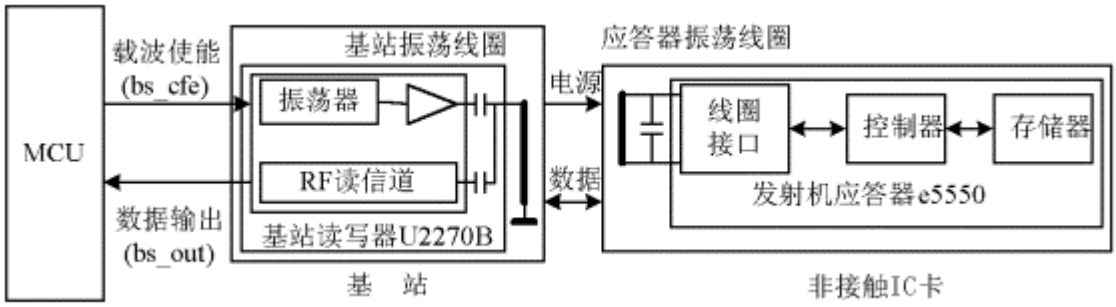


图 1 采用 e5550/U2270B 的非接触卡读写系统示意图

e5550 的全称是标准读写识别集成电路（Standard Read/Write Identification IC），实际即是一种低频发射机应答器。它与基站读写集成电路（Read/Write Base Station IC）U2270B 相匹配，构成非接触 IC 卡系统的核心器件。这两种器件统称为非接触式读写识别集成电路（其注册商标为 IDIC ,以下简称 IDIC 或非接触 IC 卡），均由德国本茨集团麾下的 Telefunken 半导体公司开发，目前已转由 Atmel 公司生产。因其工作可靠、价格低廉，不失为特定应用领域的一种优选方案。

一、 e5550/ U2270B 器件组的基本性能

e5550 发射机应答器的基本性能如下：

（1） 低供电电压、低功耗 CMOS 结构的 IDIC。
（2） 发射机应答器的电源是通过非（直接）接触的线圈耦合获得。
（3） 额定的射频（RF）振荡频率范围为：100～150kHz。

（4） 发射机应答器上带有 EEPROM，共分 8 个（存储）区，每区有 33 个位，故总共有 264 个位（见表 1）。

表 1 e5550 应答器内的存储器映射

位 序		EEPROM
0	1 …… 32	内分区
L	用户数据或口令区	第 7 区
L	用户数据区	第 6 区
L	用户数据区	第 5 区
L	用户数据区	第 4 区
L	用户数据区	第 3 区
L	用户数据区	第 2 区
L	用户数据区	第 1 区
L	工作方式区	第 0 区

注：各分区的第 0 位（表中以“L”标注的位）为非发送位。

（5） 8 个（存储）区的首位分别为该区的写保护位"L"。为"1"时，该区为只读区；为"0"时，该区为既可读又可写区。
（6） 8 个（存储）区中的第 0 区为工作方式数据存储区，通常是不发送的，而其他的 7 个区每个区中各有 32 位，即总共有 224 位供用户使用。
（7） 具备增强防护功能，以免非接触卡式 EEPROM 的误编程。
（8）每一存储区的写操作时间一般不超过 50ms。
（9） EEPROM 操作的一些其他选项：

· 比特率（位传送率 b/s）--RF/8，RF/16，RF/32，RF/40，RF/50，RF/64，RF/100,RF/128。
· 调制方式--二进制（BIN）、频移键控（FSK）、相移键控（PSK）、曼彻斯特码（Manchester）、双相位码（Biphase）。
· 其他--请求应答（AOR）、终止方式和口令方式。

U2270B 基站读写器的基本性能如下：

(1) 载波频率 fOSC 范围为 100～150kHz。
(2) fOSC 为 125kHz 时，典型的数据传送率为 5kb/s。
(3) 适用的调制方式为曼彻斯特码（简称曼码）和双相位码。
(4) 可由 5V 的稳压电源或汽车蓄电池供电。
(5) 调谐能力。
(6) 与微控制器有兼容的接口。
(7) 处于备用工作方式时，其功耗甚低。

(8) 有一向微控制器供电的输出端。

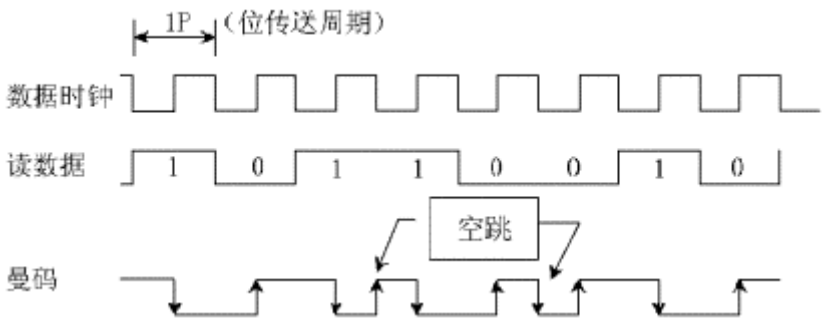
二、 非接触 IC 卡的读操作

现仅就 IDIC 通信中遇到的一些问题，并对通信的核心部分--读写操作做必要的探讨。首先申明，所谓的读写，其意分别为：基站通过 MCU 进行"读操作"；基站通过 MCU 进行"写操作"。

e5550 和 U2270B 匹配使用时，根据两者的基本特性，其调制方式只可能在曼码和双相位码中择一。不失一般性，选择曼码调制。曼码调制时数据传送的规则可用图 2 加以说明。

图 2 采用曼码调制的数据表达方式由图 2 可知，位数据的传送周期（1P）规定了每传送 1 位数据的时间是固定的，它由 RF/n 决定。其物理实质是微控制器通过基站与应答器中的存储器（EEPROM）进行数据的读写操作。若载波频率 fOSC＝125kHz，位数据传送率选 RF/32，则每传送一位的时间（周期）为振荡周期的 32 分频，故位传送周期为：

1P=1/(125kHz×32)=256μs



根据我们得到的器件，采用曼码调制的数据，位数据"1"对应着电平下跳，位数据"0"对应着电平上跳（注意：Telefunken 半导体公司提供的资料（Rev.A2,13-Oct-97）正好与此相反，故最好用前自己先测试一遍，切记！）。在一串传送的数据序列中，两个相邻的位数据传送跳变时间间隔应为 1P。若相邻的位数据极性相同，则在该两次位数据传送的电平跳变之间，有一次非数据传送的、预备性的（电平）"空跳"。

电平上跳、电平下跳和两个相邻的同极性位数据之间的预备性空跳是确定位数据传送特征的判据。本判据被定义为判据一（位数据检测指标）。

非接触 IC 卡在读操作时，另一须关注的问题是传送的位数据序列起始标志和结束标志。厂商并未提供有关的资料，通过摸索，已基本掌握了其特征，为便于说明，请参见图 3。

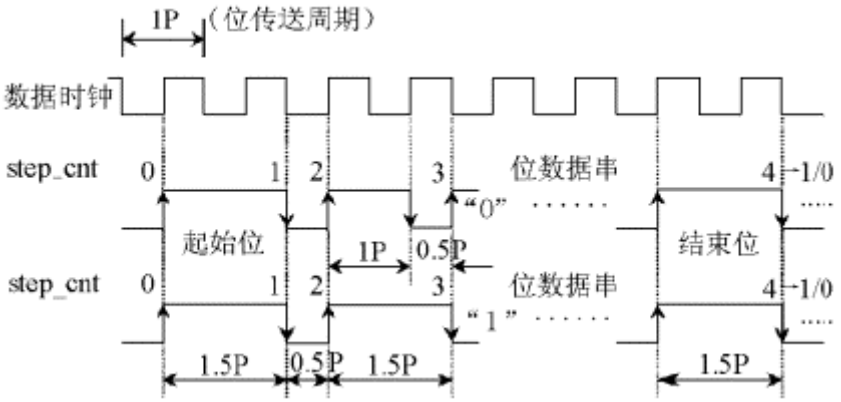


图 3 曼码调制的数据串起始/结束标志的时序特

图 3 曼码调制的数据串起始/结束标志的时序特征图 3 中，stepcnt 为读操作步序，其确切含义见表 2。

表 2 参数 step _ cnt 的含义

含 义	置 step _ cnt
尚未进入读操作	0
测到上跳后，经 1.5P 后又测到下跳	1
置 step _ cnt＝1 后，经 0.5P 测到上跳	2
根据图 3 的条件判据，已开始接收数据	3
收到第二个 1.5P，前一个上跳存入的位指针 bit _ ptr＝0，则为结束数据的接收	4

假定非接触 IC 卡的存储器内存放的位数据序列为一非空集，则在若干位数据的跳变后，检测到一电平上跳，经过 1.5P 发生电平下跳，再经过 0.5P 又发生电平的上跳，则该上跳即为起始标志。
起始标志即为结束标志。这意味着非接触 IC 卡的存储器内存放的数据包括起始标志（即结束标志）和位数据序列。读操作时，是首尾相接、循环执行的。

识别数据起始标志和数据结束标志，是通过参数 stepcnt 进行的顺序化判别，故 stepcnt 为读操作的判据二（首尾检测指标）。

非接触 IC 卡在读操作时，第三个须要关注的问题是，如何确定 1.5P、1P 和 0.5P 三个特征判据？e5550 和 U2270B 的射频振荡频率范围在 100～150kHz，当位传送率选择 RF/32 时，即 fOSC 经过 32 分频后，上述的三个参数在不同的 fOSC 时，处于什么样的范围内呢？请见表 3。

表 3　1.5P、1P 和 0.5P 三个特征判据对应的 2μs 为单位的计数值

f_{osc}/kHz	100	110	125	140	150
t_{osc}/μs	10	9	8	7	6.67
32 分频后的位传送周期/μs	320	288	256	224	213
时间间隔参数	μs/2μs 为单位的计数值				
0.5P	160/80	144/72	128/64	112/56	106/53
1.0P	320/160	288/144	256/128	224/112	213/107
1.5P	480/240	432/216	384/192	336/168	319/160

由上可知，只要 1.5P、1P 和 0.5P 的间期是不重叠的。根据采用 100～150kHz 和 110～140kHz 两组数据的对比可见，使用后者更合适。另一个办法是：通过试验，找到合适的间期指数，即可依此作为电平跃变的判别阈。这样，在确保识别能力的前提下，又从工艺上降低了对于振荡回路的频率精度要求。

根据上述振荡频率的变化范围 110～140kHz，将编码变化的不同间隔转化成相应的间期指数，具体如表 4 所列。

表 4　振荡频率在 110～140kHz 范围时，delta 的变化范围对应的间期指数

delta	delta 的变化范围（2μs 为单位的计数值）	间期指数 prd _ cnt
0.5P	$56<\tau<72$	0
1P	$112<\tau<144$	1
1.5P	$168<\tau<216$	2
>1.5P	$\tau\geqslant216$　或　$\tau<56$	3

1.5P、1P 和 0.5P 是识别数据起始标志、位数据序列和数据结束标志的间期特征值。通过试验，它可用间期指数 prdcnt 反映，故为读操作的判据三（间期检测指标）。

借助于上述的位数据检测指标、首尾检测指标和间期检测指标，非接触 IC 卡读操作程序的撰写便易如反掌。

三、 非接触 IC 卡的写操作

基站产生固定间隙的射频振荡，并通过控制两个间隙之间的振荡时间对位数据"1"和位数据"0"进行编码，持续地发送位数据流，完成写操作。写操作射频振荡波形示意如图 4 所示。

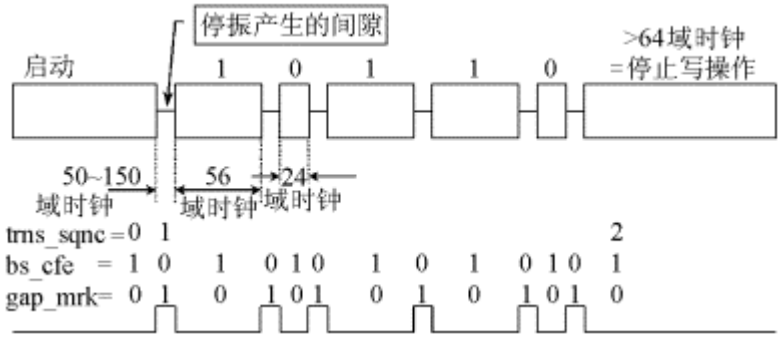


图 4 写操作时的信号流

注：域时钟（TEMIC 公司提供的资料用 fC 表示）为一时间间隔，若频率为 125kHz,fC=1/125kHz=8μs。

图 4 写操作时的信号流非接触 IC 卡插入基站后，射频线圈的耦合产生载波振荡，利用两次相邻停振之间的不同时间间隔，区分位数据"1"和位数据"0"的编码。停振间隙约在 50～

150 域时钟；位数据"0"的持续振荡时间间隔为 24 域时钟；位数据"1"的持续振荡时间间隔为 56 域时钟。当停振间隙结束后，持续振荡的时间间隔高于 64 域时钟，则 IDIC 退出写操作方式。

考虑到写操作启动（start）时，有一频率稳定过程，写操作停止（stop）时，有一 EEPROM 的写入过程约 16ms，于是将 start 和 stop 两个阶段均以 20ms 计。图 4 中标注的 trnssqnc 为发送顺序编号，启动阶段为 0，位数据流发送阶段为 1，发送结束阶段为 2。

基站读写器上有三个引脚：bsout、bscfe 和 bsin，它们的含义见表 5。

表 5 基站读写器三条引脚的含义

引脚名称	功　能
bs_out	基站信息输出引脚；有电平"上跳"和"下跳"及间隔确定
bs_cfc	基站信息输入引脚；="1"为起振，="0"为停振
bs_in	基站的供电引脚；="1"为得电，="0"为失电

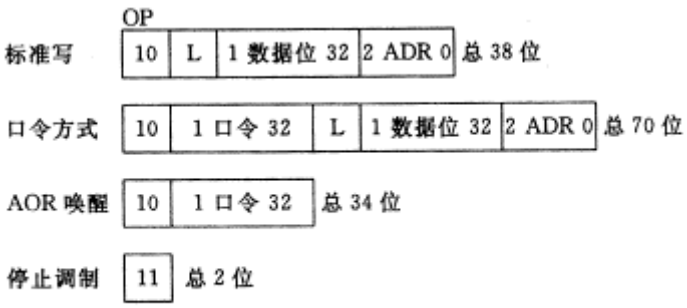


图5　合法的写数据序列

向 e5550 写位数据时，有四种合法的数据流，具体如图 5 所示。其中，OP 为操作类型码，包含两位，"10"表示即将进行的是写操作，"11"为终止 IDIC 操作码。多 IDIC 操作情况下，用这一特性可逐一控制应答器，使待控应答器逐一产生稳定的射频振荡。当方式数据区的第 28 位（usePWD）为"1"时，在写操作码"10"之后，即须将 32 位的口令（password）写入 EEPROM 的第 7 区。位数据流有 33 位，是按区写入的。其中的第一位为锁定位 L，L="1"表示该区为只读区，L="0"表示该区为读写区，其余的 32 位为位数据。ADR 为该位数据流的存放数据区，取值范围为 0～7。

根据上述的载波振荡特性，利用 carriercnst 参数进行界定（见表 7），读操作即不难实现。读写操作过程中，均使用了 2μs 为单位的计数值作为定时单位，目的是要使用 MCS-51 系列的微控制器的定时器。

表6　载波振荡特征判据对应的 2μs 为单位的计数值

振荡特性	bs _ cfe	carrier _ cnst	kHz	100	110	125	140	150
			域时钟	μs /2μs 为单位的计数值				
gap	0	1	X	150/75		100/50		50/25
“0”	1	2	24	240/120	218/109	192/96	171/86	160/80
“1”	1	3	56	560/280	509/255	448/224	400/200	374/187
start /stop	1	4	＞64	640/320	582/291	512/256	457/229	428/214

结束语

通过以上说明，再认真地研读有关的技术资料，采用曼码调制的非接触 IC 卡读写程序便不难编制。当然，实现 IDIC 的完整功能，还需要其他的一些程序模块，如数据存储格式、编码的加密算法，一次读/写操作中若出错，则须重复进行读/写操作、究竟重复几次、读/写操作过程在超时后退出等，这些均可根据应用对象的需求予以相应的解决。