PLC及PC与RFID射频识别读写器串行通讯实现

Realization of Serial Communication between RFID Reader/Writer and PLC/PC

王 宏
Wang,Hong

摘要：本文以 EMS(Escort Memory Systems)的 RFID 射频识别读写器 LRP830 为例，分别介绍了可编程控制器及微机与 RFID 射频识别读写器进行串行通讯，从而读取标识数据的具体实现方法：PLC 通过串行 I/O 通讯协议与 RFID 读写器实现串行通讯，PC 通过 Windows 多线程技术与 RFID 读写器实现串行通讯。文中给出了实例。RFID 射频识别在我国的应用才刚刚开始，前景非常广阔。本文所述方法具有一定代表性，对于推动 RFID 射频识别技术在工业自动化等领域的应用，具有一定的积极意义。

关键词：射频识别 可编程控制器 微机 串行通讯

技术创新

Abstract: This paper introduces the method of serial communication between PLC/PC and RFID systems in order to capture data from tags, by taking the RFID Reader/Writer from EMS (Escort Memory Systems) as an example. The serial communication between PLC and RFID Reader/Writer is achieved by GE Fanuc Serial I/O protocol, while the communication between PC and RFID Reader/Writer is achieved by Windows multi-thread technique. The application of RFID is promising and there is still a long way to go in this field in China. The method presented in this paper is representative and constructive for RFID applications in the field of Industrial Automation and others.

Keywords: RFID PLC PC Serial Communication

1 RFID 射频识别系统简介

RFID 的全称是 Radio Frequency Identification，即射频识别，它利用无线电射频实现可编程控制器(PLC)或微机(PC)与标识间的数据传输，从而实现非接触式目标识别与跟踪。

一个典型的 RFID 射频识别系统包括四部分：标识、天线、控制器和主机(PLC 或 PC)，系统结构图见图 1。

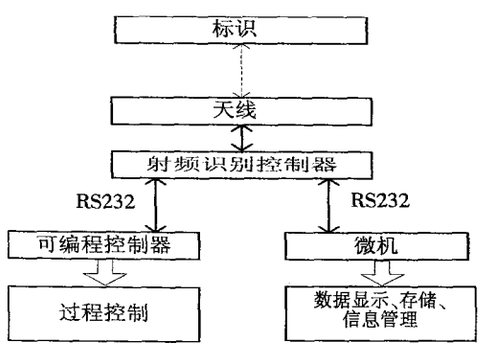

图 1 RFID 射频识别系统结构图

标识一般固定在跟踪识别对象上，如托盘、货架、小车、集装箱，在标识中可以存储一定字节的数据，用于记录识别对象的重要信息。当标识随识别对象移动时，标识就成为一个移动的数据载体。以 RFID 在计算机组装线上的应用为例，标识中可以记录机箱的类型(立式还是卧式)、所需配件及型号(主板、硬盘、CD-ROM 等)、需要完成的工序等。又如在邮包的自动分拣和跟踪应用中，可以在标识中存储邮包的始发地、目的地、路由等信息。

天线的作用是通过无线电磁波从标识中读数据或写数据到标识中。天线形状大小各异，大的可以做成货仓出口的门或通道，小的可以小到 1mm。

控制器用于控制天线与 PLC 或 PC 间的数据通信，有的控制器还带有数字量输入输出，可以直接用于控制。控制器与天线合称读写器。

PLC 或 PC 根据读写器捕捉到的标识中的数据完成相应的过程控制，或进行数据分析、显示和存储。

本文即以具有代表性的美国 EMS (Escort Memory Systems) 公司的 13.56MHz 无源 RFID 射频识别读写器 LRP830 为例，介绍了 PLC 及 PC 与 RFID 读写器进行串行通讯，从而获取标识数据，用于控制或数据处理的具体实现方法。

2 RFID 射频识别读写器的命令集及串行通讯协议

以 LRP830 读写器为例，LRP830 是 EMS 13.56MHz 无源系列射频读写器中的一种，它的标识和天线可以在水下或高温腐蚀环境中正常工作，可以一次读写 99 个标识，最大读写距离 63.5cm。它带有两个串口，一个 DeviceNet 接口，4 个 DI 隔离输入，4 个 DI 隔离输出，保护等级 IP66，NEMA4 封装，非常适合于在工业自动化中应用。

LRP830 读写器上的串口是合在一起的，通过专用电缆可以分接出 COM1 和 COM2 两个串口，两个串口作用不同，COM1 用作通讯口，从 PLC 或 PC 接收命令并返回响应数据，可以配置为 RS232、RS422 或 DeviceNet 接口。COM2 用于配置系统参数(如读写模式、波特率等)或下载系统升级程序。

LRP830 可以与所有 EMS 的 FastTrackTM 系列无源标识结合使用，每个标识中可以存储 48 个字节的数据，另外还有 8 个字节用于存储只读的唯一的序列号(出厂前由厂方设定)。

LRP830 提供了单标识读写命令集(见表 1)，多标识读写命令与此类似。

表 1 单标识命令集

命令	功能	命令	功能
04H	写同一字节数据到标识的连续地址	05H	读块地址
06H	写连续地址块	07H	读标识序列号
08H	搜寻标识	0DH	连续读块地址
10H	设置数字量输出	11H	数字量输入状态

每种命令可以有三种通讯协议：ABxS 、ABxF 、ABx ASCII。表 2 是 ABxS 通讯协议持续读单标识命令的一个例子，其它命令与此类似。

3 RFID 读写器与 PLC 串行通讯

以 EMS RFID 读写器 LRP830 与 GE Fanuc VersaMax PLC 的串行通讯为例。VersaMax PLC 的 RS232 串口与 LRP830 的 COM1 接线对应关系见表 3。

表 2 ABxS 协议持续读单标识命令举例

高字节	低字节	说明
AAH	ODH	命令字，上表一、表二中命令字节前加 AAH
O0H	00H	起始地址，2 个字节，指定从标识中第一个字节开始读
00H	08H	读地址长度，2 个字节，指定读 8 个字节数据
00H	02H	以秒为单位，指定同一标识重复被读写间隔时间为 2 秒
FFH	FFH	通信终止标志，以 FFFFH 标志命令结束

表 3 VersaMax 与 LRP830 读写器的串口接线对应关系

VersaMax RS232 口	LRP830
TXD 2	J RXD
RXD 3	N TXD
GND 5	K GND

通过 PLC 控制 RFID 读写器读写标识数据的实现流程如图 2 所示。

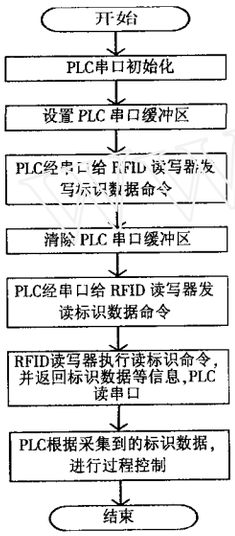

图 2 PLC 读写 RFID 标识数据的程序结构框图

以下是具体实现时要注意的技术细节：

1） LRP830 与 VersaMax PLC 的串口相连时，信号线要错线，即 VersaMax RS232 口的 TXD/RXD 要接 LRP830 的 COM1 的 RXD/TXD，LRP830 与 PC 连接时则是直通的。

2) PLC 使用串行 I/O 通讯协议与 RFID 读写器通讯。串口初始化、设置缓冲区、清除缓冲区、写串口、读串口状态等操作都是先通过一组 BLKMOV WORD 指令给 COMMREQ 的数据块赋值，然后执行 COMMREQ 指令完成的。例如，以下语句(见图 3 (略可向作者索取))通过 RFID 读写器写 10 个 FF(46H)到标识中，从第一个字节写起。

3） 要注意 PLC 写标识数据只需要执行写串口命令就可以了，而 PLC 读标识数据的过程则包含两步：一是 PLC 执行写串口命令，即写读标识命令到 RFID 读写器；二是 PLC 执行读串口命令，捕捉 RFID 读写器返回的数据。这是由于 RFID 读写器在接到读标识命令后，会返回读命令的响应信息到串口缓冲区，其中包含了读到的标识数据。

4) 使用 ABxS 协议时，要注意命令字的 MSB 和 LSB 的顺序问题。RFID 读写器与 PLC 通讯时，要将读写器指令的 MSB 和 LSB 颠倒一下，即 LSB 在前，MSB 在后。例如图 3 中，第二个 BLKMOV WORD 指令的第三个输入 IN3 应为 16#4AA，而非 16#AA04。

5） 利用读写器指示灯的变化辅助 PLC 程序调试。LRP830 读写器的面板上有两排 LED 指示灯，其中，当“ANT”亮时，表示天线在执行读写操作；“COM1”亮时，表示串口 1 执行了写命令，“RF”亮时，表示有标识被读写且仍在读写范围内。

4 RFID 读写器与 PC 串行通讯

仍以 EMS RFID 读写器 LRP830 为例。与 PC 机相连时，LRP830 的 COM1/COM2 与 PC 机的 9 针串口 COM1/COM2 的连接对应关系见表 4。

表 4 LRP830 的串口与 PC 串口连接对应关系

	PC（DE9）	LRP830	描述
COM1	TXD 2	N TXD	发送数据
	RXD 3	J RXD	接收数据
	GND 5	K GND	信号地
COM2	RXD 2	R TXD	发送数据
	TXD 3	P RXD	接收数据
	GND 5	M GND	信号地

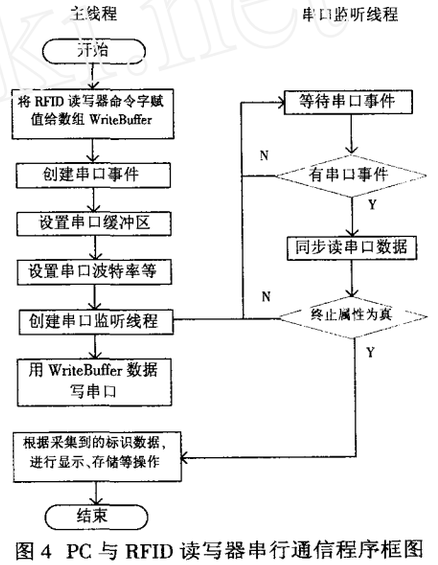

图 4 PC 与 RFID 读写器串行通信程序框图

在 PC 机上开发串口通讯程序，可以使用现有的通讯控件(如 VB 的 Mscomm)，也可以使用高级编程语言结合 Windows API 实现。本文用 Delphi 6 在 Windows2000 环境中，应用多线程技术实现了 PC 与 RFID 读写器间的串行通信。使用 Delphi 的优点是，Delphi 对许多 Windows 底层 API 函数作了封装，简化了程序代码。使用多线程的优点是，程序编写比较灵活，而且串口监听线程不影响主线程其它任务执行。程序结构框图见图 4.

在具体实现上述思路时，要注意以下技术细节：

1） 根据 RFID 读写器通讯协议的特点，读写器每执行一个主机发来的指令，无论是读标识还是写标识，都会返回一定字节的响应数据，用以确认命令已执行或返回标识中存储的数据。因此，主机读或写标识数据都需要先写(串口命令)后读(返回的串口数据)。2) 为了使程序体现模块化的设计思想，易于调试和维护，可以把各种 RFID 命令预先存入命令数组中，而把主机对 RFID 串口的命令和捕捉 RFID 读写器命令响应编制成单独的子程序，在调用它之前，先调用命令字赋值子程序。3) 对主线程的说明：在主线程中用 CreateFile 函数建立串口事件，设置缓冲区和通信参数，创建串口监听线程。用 WriteFile 写串口函数完成通过 RFID 读写器写数据到标识中。部分程序如下：

```
……
hcom := CreateFile(pchar(Whichcom), GENERIC_WRITE Or GENERIC_READ,
  0, 0, OPEN_ALWAYS, FILE_ATTRIBUTE_NORMAL, 0); //产生串口事件
setupcomm(hcom,TOTALBYTES,TOTALBYTES);//设置缓冲区
getcommstate(hcom,lpdcb);
lpdcb.BaudRate:=BAUDRATE; //波特率
lpdcb.StopBits := STOPBIT; //停止位
lpdcb.ByteSize := BYTESIZE; //每字节有几位
lpdcb.Parity :=PARITY; //奇偶校验
setcommstate(hcom,lpdcb); //设置串口
Mycomm := Tcomm2.Create(False); //创建串口监听线程
WriteFile (hcom, WriteBuffer,sizeof (WriteBuffer),lpBytesSent, 0);//写标识命令
……
```

4）对串口监听线程的说明：

程序中用到的方法主要有 Synchronize 和 Terminate。Synchronize 是 Delphi 提供的一种安全调用线程的方法，它把线程的调用权交给了主线程，从而避免了线程间的冲突，这是一种最简单的线程间同步的方法，可以省去用其它语言编程时需要调用的多个 Windows API 函数，例如 createEvent（创建同步事件），Waitforsingleobject（等待同步事件置位），resetevent（同步事件复位），PostMessage（向主线程发送消息）等。用 Delphi 编写多线程通讯程序的优点是显而易见的。例如以下语句即可实现串口监听线程：

```
……
While (not Terminated) do //如果终止属性不为真
Begin
  dwEvtMask:=0;
  Wait := WaitCommEvent(hcom,dwevtmask,lpol); //等待串口事件
  if Wait Then
  begin
    Synchronize(DataProcessing); //同步串口事件
  end;
end;
```

上述程序一旦检测到串口事件，就调用 DataProcessing 方法读串口数据，并写入数组，供程序其它部分调用，另外还要检测何时退出线程，程序如下：

```
procedure Tmainform.DataProcessing
begin
  clear := CLEARCOMMERROR(hcom,lperrors,@comms); //清除串口错误
  if Clear Then
    Begin    //处理接收数据
      ReadFile (hcom,ReadBuffer,Comms.cbInQue, LPReadNumber,0);
      ReceBytes[I+ArrayOffset] := ReadBuffer[I];
        //读串口缓冲区数据并写入数组
      gameover := (ReceBytes[I+ArrayOffset-1]=Byte($FF))
        and (ReceBytes[I+ArrayOffset]=Byte($FF)); //终止条件
      if gameover then terminate; //退出线程
      ……
      End;
End;
```

其中，Terminate 将线程的 Terminated 属性设置为 True。线程一旦检测到 Terminated 属性为 True，就会结束线程，去执行 Onterminate 事件，在 Onterminate 事件中对采集到的 RFID 标识数据进行处理。由于 RFID 读写器的 ABxS 协议的命令响应的最后两个字节都是 FF，所以可以将收到连续的两个 FF 作为终止线程的条件之一。

程序应用举例：

以持续读标识中所有 48 字节数据命令为例，在程序中用 WriteBuffer 数组保存该命令，对 WriteBuffer 数组的各个元素赋值如下：

```
WriteBuffer[0] := Byte($AA); WriteBuffer[1] := Byte($0D); //连续读标识命令字头
WriteBuffer[2] := Byte($00); WriteBuffer[3] := Byte($00); //从第一个字节开始读
WriteBuffer[4] := Byte($00); WriteBuffer[5] := Byte($30); //读 48 个字节数据
WriteBuffer[6] := Byte($00); WriteBuffer[7] := Byte($02); //延时 2 秒
WriteBuffer[8] := Byte($ff); WriteBuffer[9] := Byte($ff); //连续读标识命令字
```

执行持续读标识命令后，程序以 WriteBuffer 数组写串口，RFID 读写器执行此命令，并返回响应数据（见图 5）。

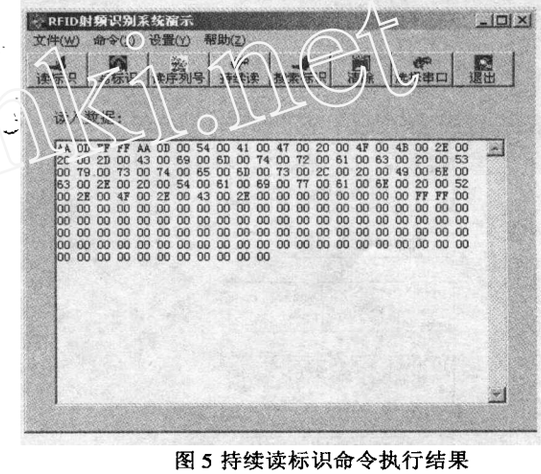

图 5 持续读标识命令执行结果

从图 5 窗口中可以看到，前 4 个字节 AA OD FF FF 就是 LRP830 读写器对持续读命令的确认信息，然后是数据报文头 AA OD 和标识中 48 个字节的数据（每字节数据前加 00），最后是数据报文尾 FF FF。

5 结束语

本文介绍了可编程控制器及微机与 RFID 射频识别读写器进行串行通讯，从而获取标识中的数据的具体实现方法：PLC 通过串行 I/O 通讯协议与 RFID 读写器实现串行通讯，PC 通过 Windows 多线程技术与 RFID 读写器实现串行通讯。本文所述方法具有通用性，对于其它厂家的 PLC 和 RFID 系统也有一定的参考价值。RFID 射频识别技术在我国工业自动化等领域的应用才刚刚开始，前景非常广阔。本文对于促进该技术的推广应用具有一定的积极意义。

参考文献：

[1]Marco Cantù, Mastering Delphi 6, SYBEX Inc.(USA), 2001.

作者简介：王宏，男，1973 年 2 月出生，工程师，工学硕士。原籍河南洛阳，1995 年、1998 年于东北电力学院自动控制系生产过程自动化专业分别取得工学学士、工学硕士学位。主要从事 PLC 及人机界面软件应用、DCS 及其仿真研究。Tel: 0755-26551199, 26235582, 13530041159. E-mail: wanghongcn@21cn.com

（518057 深圳市清华大学研究院 B203 室 华利通科技有限公司）王宏

（收稿日期：2002.7.26）