MODBUS 协议在单片机与触摸屏通信中的应用

张 芬

（西安航空职业技术学院，陕西 西安 710089）

【摘 要】文章介绍了自主开发的智能配电系统的硬件构成，重点讲述基于 MODBUS 通讯协议的触摸屏与单片机系统的通讯方法。该方法降低了系统设计成本，并提高了设备的通用性。目前该系统已通过用户的验收并投入使用。

【关键词】MODBUS；单片机；触摸屏

【中图分类号】TP29 【文献标识码】A 【文章编号】1008-1151(2009)07-0023-02

（一）引言

目前，计算机机房的配电系统大都使用不停电系统（UPS），保证了机房的可靠供电。UPS 系统下的每一路电流采用自动空气断路器进行过流保护，这种保护是有效的，但这种保护不具备智能，不能设置，不会报警，更没有供电及故障报警信息的纪录，与高可靠性的要求不相符，有进一步改造的必要和需求。我们为计算机机房开发的一套智能配电系统 iPDS(Intelligent Power Distribution System)很好的满足了以上要求，具有智能化、人性化两大特点。

（二）系统构成

本智能系统对机房内各路电源的电流值、漏电流值、零地电压、自动空气断路器的运行状态等信息进行实时监测、显示。具有实时报警、详细记录等功能，并可以根据用户要求灵活的配置各路监测信息。可以在显示屏上查询机房各路电源的使用情况，尽早发现和消除隐患，实时处理故障情况，进一步提高了系统的可靠性。

系统由数据处理单元、数据采集节点、LED 显示节点、触摸屏等组成，具体系统结构如图 1 所示。数据处理单元有两个 CPU，单片机 AT89C52 和 P87C591，二者通过双口 RAM 进行数据的交换，其中 AT89C52 与触摸屏通过 RS-485 通讯，处理触摸屏上的显示和设置信息，P87C591 处理 CAN 总线上的交互信息。

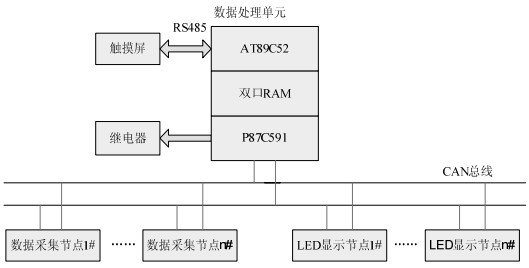

图 1 智能配电系统结构图

通常情况，触摸屏支持与多种 PLC 通讯时的相应的驱动程序，但和单片机通讯时，内部并无相应的驱动程序，需要借助 MODBUS 协议来完成二者之间的通讯。故编制程序前，首先应该对 MODBUS 协议有较深刻的理解和认识。

（三）MODBUS 协议

1.MODBUS 协议简介

MODBUS 协议是应用于 PLC 或其他控制器上的一种通用语言。该协议是一种标准的串行通讯协议，使用标准的串行接口（RS485），数据通讯采用主/从方式，主设备可单独和从设备通信，也能以广播方式和所有从设备通信。通过此协议，控制器之间、控制器通过网络和其他设备之间可以实现串行通信。该协议已经成为通用工业标准。采用 MODBUS 协议，不同厂商生产的控制设备可以互连成工业网络，实现集中监控。

2.MODBUS 协议的报文格式

MODBUS 协议的基本通讯单元，称为报文，每一条报文包括三部分：报文头（包括：站址、命令码和字节数）、数据和检验码。串行通讯时是以一个字符（加上特定附加位构成一“帧”）作为最小传送单位的，在 MODBUS 协议的报文中，每帧包括 11 位：1 个起始位、1 个校验位、1 个停止位和 8 个数据位（1 个字符）。报文头、数据和校验码由若干个字符组成。

本系统使用MODBUS的RTU传输模式完成触摸屏和单片机系统的通讯功能。使用 RTU 模式，报文发送至少要以 3.5 个字符时间的停顿间隔开始。传输的第一个域是设备地址。网络设备不断侦测网络总线，包括停顿间隔时间内。当第一个域(地址域)接收到，每个设备都进行解码以判断是否发往自己的。在最后一个传输字符之后，一个至少 3.5 个字符时间的停顿标定了报文的结束。一个新的报文可在此停顿后开始。在实际应用中，一般采用 4 个字符的传输时间标志报文的起始和结束。一个典型的报文结构如表 1 所示。

表 1 RTU 报文结构

起始间隔	设备地址	功能代码	数据	CRC 校验	结束间隔
T1-T2-T3-T4	1 个字节	1 个字节	n 个字节	2 个字节	T1-T2-T3-T4

MODBUS 网络只有一个主机，所有通信都由他发起。在本系统中，单片机是主机，触摸屏是从机。

3.CRC 校验码的实现

使用 RTU 模式，报文包括了一基于 CRC 方法的错误检测域。CRC 域检测了整个报文的内容。CRC 域是两个字节，包含一 16 位的二进制值。它由发送设备计算后加入到报文中。接

【收稿日期】2009-05-08

【作者简介】张芬（1980－），女，陕西渭南人，西安航空职业技术学院教师，硕士研究生，研究方向为现场总线、运动控制、计算机控制。

收设备重新计算收到报文的 CRC，并与接收到的 CRC 域中的值比较，如果两值不同，则有误。

正常的通讯过程中由于涉及了 CRC 校验问题，而这个校验过程是需要占用软件时间的，它将影响终端的应答速度。如果采用标准的 CRC 计算公式来做接收和发送报文的 CRC 校验码，需要占用较多的时间，在使用较高速度通讯时是不允许的。本设计采用了查表法计算 CRC，速度非常快，能够满足高速通讯的需要。

（四）系统参数设置

本系统人机界面所有画面均采用 EasyBuilder500 全中文软件进行组态。系统将单片机作为主机，将触摸屏作为从机。触摸屏系统设置为：在菜单[编辑]中选择[系统参数]项，在弹出的对话框中设置 PLC 类型为 MODBUS RTU Server，通讯口类型设置为 RS-485，将波特率，数据位个数，校验位，停止位个数设置成和单片机系统一致。该设置如图 2 所示。

系统组态的画面包括主画面、参数设定、参数显示、状态信息、报警信息等，经 EWIEW 软件编译无误后，从个人电脑中下载到人机界面即可使用。由于篇幅原因组态画面不再此详细介绍。

人机界面与本系统所设计的单片机硬件系统之间通过 RS485 通讯电缆以主从方式进行连接。

（五）软件实现

1.初始化程序

本系统的应用软件采用单片机高级语言 C51。整个系统的程序实现是由很多个子程序构成的，每个子程序都完成触摸屏与单片机的信息交换，只是不同的子程序完成不同的功能。

AT89C52 初始化程序如下：

```
void initSFR(void)
{
 TH1=0xfa;
 TL1=0xfa;     //设定波特率为 9600
 TMOD=0x21;    //T1 选用模式 2
 PCON=0X80|PCON;    //数据传输率翻倍
 SCON=0x50;    // 模式 1：10 位异步串行通信
 PS=1;         //串行口中断控制位高优先级
 TR1=1;        //启动 T1
 ES=1;         //串口中断允许
 EA=1;         //允许中断总控制
}
```

图 2　触摸屏系统参数设置

2.通讯子程序

MODBUS 协议有几十个功能码，在这些功能码中较常使用的有“01”、“02”、“03”、“04”、“05”、“06”及“10”号功能码，使用它们即可实现对下位机的数字量和模拟量的读写操作。下边以功能码“03”读取模拟量寄存器为例，讲述 C51 程序的实现。其通讯流程如图 3 所示。

（1）单片机发送命令：[设备地址] [命令号 03] [起始寄存器地址高 8 位] [低 8 位] [读取的寄存器数高 8 位] [低 8 位] [CRC 校验的低 8 位] [CRC 校验的高 8 位]

例：[11][03][00][6B][00][03][CRC 低][CRC 高]

意义如下：

1）设备地址和上面的相同。

2）命令号:读模拟量的命令号固定为 03。

3）起始地址高 8 位、低 8 位：表示想读取的模拟量的起始地址。比如例子中的起始地址为 107。

4）寄存器数高 8 位、低 8 位：表示从起始地址开始读多少个模拟量。例子中为 3 个模拟量。注意，在返回的信息中一个模拟量需要返回两个字节。

图 3　发送子程序

（2）设备响应：[设备地址] [命令号 03] [返回的字节个数] [数据 1] [数据 2]...[数据 n] [CRC 校验的低 8 位] [CRC 校验的高 8 位]

例：[11][03][06][02][2B][00][00][00][64][CRC 低][CRC 高]

意义如下：

1）设备地址和命令号和上面的相同。

2）返回的字节个数：表示数据的字节个数，也就是数据 1，2...n 中的 n 的值。例子中返回了 3 个模拟量的数据，因为一个模拟量需要 2 个字节所以共 6 个字节。

3）数据 1...n：其中[数据 1][数据 2]分别是第 1 个模拟量的高 8 位和低 8 位，[数据 3][数据 4]是第 2 个模拟量的高 8 位和低 8 位，以此类推。例子中返回的值分别是 555，0，100。

4）CRC 校验同上。

（3）发送程序如下：

```
void Send03(uchar Radrh,Radrl,Rnumber)
{
 td_dat3[0]=1; //从机地址;
 td_dat3[1]=3; //功能码 03：读取保持寄存器的数据
td_dat3[2]=Radrh; //起始地址高字节
td_dat3[3]=Radrl; //起始地址低字节
td_dat3[4]=0; //读取模拟量数量的高字节
```

（下转第 14 页）

面进行杜绝：（1）可靠性与线路安全；（2）对端路由器的身份认证和路由信息的身份认证；（3）访问控制对于路由器的访问控制，需要进行口令的分级保护；基于 IP 地址的访问控制；基于用户的访问控制。

信息隐藏：与对端通信时，不一定需要用真实身份进行通信。通过地址转换，可以做到隐藏网内地址、只以公共地址的方式访问外部网络。除了由内部网络首先发起的连接，网外用户不能通过地址转换直接访问网内资源；数据加密；在路由器上提供攻击检测，可以防止一部分的攻击。

4.IP 地址欺骗防范

（1）抛弃基于地址的信任策略：阻止这类攻击的一种非常容易的办法就是放弃以地址为基础的验证。不允许 r 类远程调用命令的使用；删除 .rhosts 文件；清空 /etc/hosts.equiv 文件。这将迫使所有用户使用其它远程通信手段，如 telnet、ssh、skey 等等。

（2）使用加密方法：在包发送到网络上之前，我们可以对它进行加密。虽然加密过程要求适当改变目前的网络环境，但它将保证数据的完整性和真实性。

（3）进行包过滤：可以配置路由器使其能够拒绝网络外部与本网内具有相同 IP 地址的连接请求。而且，当包的 IP 地址不在本网内时，路由器不应该把本网主机的包发送出去。

路由器虽然可以封锁试图到达内部网络的特定类型的包。但它们也是通过分析测试源地址来实现操作的。因此，它们仅能对声称是来自于内部网络的外来包进行过滤，若你的网络存在外部可信任主机，那么路由器将无法防止别人冒充这些主机进行 IP 欺骗。

5.WinNuke 攻击防范

对于 WinNuke 的防御方法主要是先判断数据包目标端口是否为 139、138、137 等，并判断 URG 位是否为 1，同时通过防火墙或者路由器对所涉及 IP 或者端口号进行阻断，在设备支持的情况下开启审计功能，对时间发生的时间、源主机和目标主机 IP 地址和 MAC 地址进行记录。

6.ARP 攻击防范

（1）对重要设备或者网关 MAC 地址和对应的 IP 地址进行绑定，也可以通过写脚本的形式实现；

（2）在交换机上做端口与 MAC 地址的绑定，采用端口保护，同时配置 ACL 对于一些非合法 IP 或者 MAC 地址进行过滤，并定义访问规则；

（3）使用 ARP 服务器，通过该服务器查找自己的 ARP 转换表来响应其他设备的 ARP 广播；

（4）对于某些网络环境可以考虑禁止网络接口的 ARP 解析或者使用代理 ARP；

（5）使用其他硬件例如防火墙等监控网络，尽量避免使用集线器等设备；

（6）管理员定期对主机 ARP 缓存进行检察。

7.路由协议攻击防范

为防止路由信息泄露，路由协议例如 RIP、OSPF 等都支持对等体之间的认证，只是采用的加密方式是密文还是明文的形式，通过启用 MD5 的方式可以提供较高的安全性，对对等体进行认证和校验，同时在接口公告时采用反掩码尽量精确公告，对于一些没有必要接收路由的端口启用 Passive interface 命令，这样既能够保证该接口网段路由照常发布但又不会再收发协议报文，不会与其它路由设备建立邻居的同时也避免了路由泄露。

（三）结束语

互联网络正以惊人的速度改变着人们的生活方式和工作效率。从商业机构到个人都将越来越多地通过互联网处理银行事物、发送电子邮件、购物、炒股和办公等等。这无疑给社会、企业乃至个人带来了前所未有的便利，所有这一切都得益于互联网络的开放性和匿名性特征。然而正是这些特征决定了互联网不可避免地存在信息安全隐患。但只要我们处处做好防范，提高综合素质，提高网络安全防范意识问题总会迎刃而解。

【参考文献】

[1] 甘刚,等.网络攻击与防御[M].北京:清华大学出版社,2008,3:110-217.

[2] 谭毓安.网络攻击防护编码设计[M].北京:北京希望电子出版社,2002,3:177-324.

[3] 牛少彰,等.网络的攻击与防范——理论与实践[M].北京：北京邮电大学出版社,2006,12:90-289.

[4] (美)马里克（Malik,S）.网络安全原理与实践[M].王宝生,朱培栋,白建军,译.北京:人民邮电出版社,2006,11:270-401.

[5] 周继军,等.网络与信息安全基础[M].北京:清华大学出版社,2008,8:168-299.

（上接第 24 页）

```
td_dat3[5]=Rnumber;//读取模拟量数量的低字节
crc16Val=crc16(td_dat3,6);//进行 CRC 校验
td_dat3[6]=(uchar)(crc16Val>> 8);  //*CRC 校验低字节    td_dat3[7]=(uchar)(crc16Val& 0x00ff); //*CRC 校验高字节
for(j=0;j<3500;j++) //根据波特率延时 4 个字符时间，大约 4ms
  _nop_();
 for (i=0;i<8;i++)  //发送数据
{   ES=0;       //串口中断关闭
   ACC=td_dat3[i];
   SBUF=ACC;
   while(TI==0)
     {      _nop_()};
   for(j=0;j<255;j++) //延时
  _nop_();
    TI=0;
 }
ES=1;     //串口中断允许
}
```

（六）结束语

Modbus 协议是一个仅有物理层和数据链路层的现场总线协议，特别适合结构简单、成本低的应用场合。触摸屏通过支持 Modbus 协议，实现了与单片机进行通信，降低了系统设计成本，并提高了设备的通用性。目前该系统已通过用户的验收并投入使用。

【参考文献】

[1] 李惊蛰,师向东.MODBUS 协议在不可靠信道中的应用[J].电气传动自动化,2003,25(5):51-52.

[2] 何立民.单片机应用技术选编 8[M].北京航空航天大学出版社,2000:200-230.

MODBUS协议在单片机与触摸屏通信中的应用

作者： 张芬
作者单位： 西安航空职业技术学院,陕西,西安,710089
刊名： 大众科技
英文刊名： DAZHONG KEJI
年，卷(期)： 2009，(7)

参考文献(2条)

1. 李惊蛰.师向东 MODBUS协议在不可靠信道中的应用[期刊论文]-电气传动自动化 2003(5)

2. 何立民 单片机应用技术选编8 2000

相似文献(10条)

1. 期刊论文 路平.薛树琦.Lu Ping.Xue Shuqi Modbus协议下单片机与eView触摸屏的通信方法 -单片机与嵌入式系统应用2007(4)
Modbus协议由于其具有开放性、透明性、成本低、易于开发等特点,已成为当今工业领域通信协议的首选.本文介绍了一种基于Modbus通信协议的eView触摸屏与常用的51单片机的通信方法.该方法通过C51编程实现Modhus通信,在51系列单片机上具有通用性,有一定的借鉴作用.

2. 期刊论文 姜凤武.王杭.JIANG Feng-wu.WANG Hang 基于MODBUS协议实现单片机与变频器的通信 -自动化技术与应用2006,25(4)
本文介绍采用MODBUS协议中的ASCII模式实现单片机与变频器的通信.单片机做作为上位机,变频器作为下位机,通过RS485接口实现单片机与变频器的通信,有效且经济地实现单片机对交流电机的控制.

3. 期刊论文 尤慧芳.You Huifan 用MODBUS实现触摸屏与单片机的通信 -工业控制计算机2008,21(12)
讲解如何利用MODBUS通信协议,实现触摸屏与单片机的通信和控制.详细介绍了触摸屏与单片机的硬件连接、软件设置及编辑、MODBUS通信协议的使用方法等内容.

4. 期刊论文 李明伟.郭广峰.黄鸽 PIC单片机与触摸屏串行通信的MODBUS协议实现 -电子技术应用2005,31(9)
介绍一种在PIC单片机与触摸屏之间采用Modbus协议实现异步串行通信的方法.简单介绍了Modbus通信协议,给出了硬件电路连接图、程序流程图以及用PIC单片机C语言编写的部分通信程序.实际使用证明该方法数据传输稳定可靠,并提供了良好的人机交互环境.

5. 学位论文 邓元生 基于单片机的MODBUS总线协议实现技术研究 2009
现场总线是当今自动化领域发展的热点之一，被誉为自动化领域的计算机局域网。它作为工业数据通信网络的基础，沟通了生产过程现场设备之间的联系。当今现场总线有许多标准，MODBUS协议就是其中重要的标准之一，它已经是全球工业领域最流行的协议之一，很多工业设备，诸如PLC、DCS，智能仪表等都使用MODBUS协议作为它们之间的通信标准。
本文为创建单片机组网的平台，实现PC机和单片机的通信，达到用PC机控制单片机的目的，构建了以PC机为主机，MODBUS协议为联络载体，单片机为从机的“主-从”式装置；设计了RS-232和RS-485的电平转换器，实现了PC串口和单片机串口的电平的兼容；采用CRC校验方法，保证了通信数据的准确性。装置中的主机采用通用微机，从机采用AT89S52单片机为核心器件，并配备了ADC0809和DAC0832等辅助元件，以及Intel8155芯片作为装置扩展接口。 本文在分析研究MODBUS协议的基础上，针对MODBUS信息帧的特点，采用VC++6.0编程实现了主机和单片机以MODBUS协议的串行通信，从机系统采用C51编程实现了通信数据的提取、解析和发送。本文以单片机实现MODBUS协议通信，具有广泛的实际应用前景。

6. 期刊论文 许文辉.Xu Wenhui STC单片机实现的ModBus-RTU协议无线通信服务器 -自动化与信息工程2007,28(1)
介绍一个基于STC单片机构建的Modbus-RTU主站协议的无线通信服务器.着重介绍其使用的芯片,原理及电路.从低成本的角度,有效地解决了AB的PLC主站与远方多处的Modicon MicroPLC之间的无线通信问题.为实现异种类型PLC之间的无线数据交换提供了一个切实可行的方法.

7. 期刊论文 温建明.鲁五一.袁庆国 基于MODBUS协议的触摸屏与单片机通信的实现 -起重运输机械2008(7)
介绍1种在Winbond单片机W77E516与触摸屏之间采用Modbus协议实现异步串行通信的方法.首先介绍系统实现的硬件结构,系统选用具有标准Modbus通信协议接口的SOLCN S534T型触摸屏,同时给出了基于单片机W77E516的简单硬件电路连接图,然后介绍了Modbus通信协议,最后给出了详细的通信程序实现方法和程序流程图,并举例说明触摸屏及单片机的实际通信数据格式.实际使用证明该方法数据传输稳定可靠,并可提供良好的人机交互环境.

8. 期刊论文 魏占永.潘振克.殷文.屠秋恩.计晨.WEI Zhan-yong.PAN Zhen-ke.YIN Wen.TU Qiu-en.JI Chen 单片机Modbus-TCP协议栈设计及其在低压配电系统中的应用 -低压电器2005(8)
充分利用单片机资源,建立TCP/IP协议栈,并嵌入Modbus应用协议完成Modbus到TCP的协议转换.利用Modbus-TCP协议栈在低压配电系统中组建工业以太网.测试表明,该系统运行稳定.

9. 学位论文 严惠 基于ARM7与51单片机的电梯控制器通信及人机界面的研究与开发 2007
电梯通信作为电梯运行的主脉络，负责传递电梯的各个通讯指令以及各种控制信息，因此，提高电梯的性能在很大的程度上取决于电梯信息量的传输品质。同时，为保证电梯运行的可靠性以及提高电梯的使用寿命，必须对电梯进行合理的维护。而电梯的远程监控技术是一种合理有效的维护手段，通过它可以对电梯实行有效的未知维护。 本文从上述两个点出发，结合电梯控制器设计的实际项目，重点研究了电梯控制系统中的通讯和电梯控制器远程监控上位机界面的设计。整个系统的通讯布局以CAN总线为主干网，485总线为主体板和扩展板之间的通讯桥梁。 电梯控制系统分为楼层控制器、轿厢控制器、轿顶控制器、主板控制器以及相应的扩展板。本文主要从以下几个方面进行研究。 1. 楼层控制器的设计。采用51单片机为楼层微控制器，MedWin为软件开发平台，实现楼层控制器的硬件和软件设计；将CAN总线运用于楼层控制器通讯中，结合MODBIJS协议以及CAN信息帧结构自定义通讯协议，实现了独立CAN控制器下的CAN通讯；通过功能调试验证了方案可行性。 2. 轿顶控制器的设计。采用ARM单片机为轿顶主控制器，ADS1.2为软件开发平台，进行轿顶控制器硬件和软件设计；将CAN总线应用于轿顶控制器通讯，实现了非独立CAN控制器的CAN总线通讯功能；并对轿顶功能进行调试验证。 3. 轿厢扩展板的设计。进行轿厢扩展板的软硬件设计；采用MODBUS通讯协议，将485总线应用于轿厢扩展板中，实现了轿厢扩展板与主体板通讯；通过调试验证了方案的可行性。 4. 远程监控上位机设计。以Delphi为开发平台，RS485为通讯总线，实现电梯参数的获取与显示的软件功能；在以太网环境中，采用Visual Stdio 6.0为开发平台，结合MODBUS-TCP通讯协议实现客户端、服务器的软件设计；并在模拟环境中验证了上位机功能。 通过研究表明，CAN总线可以用于电梯控制系统的通讯中，而且性能可靠，实时性好，能充分满足电梯控制器对通讯性能的要求；RS485总线能充分实现电梯主体板和扩展板之间的通讯目的，能准确有效的实现上位机对电梯参数的获取；采用融合客户端/服务器模式的对等网络技术设计电梯远程监控上位机软件，在模拟环境中实现了位于不同环境的客户端电梯与维护方之间的连接，确保了维护方对电梯的远程监控。

10. 会议论文 刘暾东.潘江虎.周文博 基于ModBus通讯的液晶型断路器智能控制器研制 2008
针对断路器的电流保护和四遥功能要求,开发一智能断路器控制器.该控制器利用MSP430处理器芯片强大的处理能力和丰富的片内集成模块,使得控制器具有较好的实时性和电磁兼容性;同时,采用电力系统常用MODBUS通信协议,实现控制器与上位机的便捷通信,完成"四遥"功能;另外,利用液晶显示和按键修改技术,使用户方便调整断路器保护参数.实验测试结果表明,该智能控制器保护效果良好、成本低、易于实现.