

Modbus 协议及其在 MCU 与 PLC 通信中的应用

彭庆海, 胡小强

(杭州电子科技大学 自动化学院, 浙江 杭州 310018)

摘要:为解决 PLC 设备的人机交互性能差的问题,分析了已广泛应用于 PLC、变频器和自动化仪表等设备的 Modbus 协议,介绍了 Modbus 通讯数据如何在芯片中组成消息帧;并结合目前在工业领域使用较为广泛的 SIEMENS S7-200 系列 PLC 及 STC89C58RD 单片机,详细阐述了 MCU 与 PLC 之间通讯的实现。研究表明,该方法使 PLC 设备可通过系统的人机界面程序进行控制,增加了其交互性能。

关键词:Modbus 协议;人机交互;STC89C58RD 单片机

中图分类号:TP206

文献标识码:A

文章编号:1001-4551(2010)04-0052-04

Modbus protocol and application in the communication between MCU and PLC

PENG Qing-hai, HU Xiao-qiang

(College of Automation, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: In order to solve the poor man-machine exchange performance of PLC equipment, the Modbus protocol was analyzed which has been widely used in PLC, inverter and other automation instrumentation, and also it was introduced that how to composite the message frame in the chip. In addition, combined with SIEMENS S7-200 series PLC and STC89C58RD single-chip, it was elaborated that how to realize the communication between the MCU and the PLC. The results show that it lets the PLC devices be controlled by the system man-machine interface program, in order to address their shortcoming in man-machine exchange.

Key words: Modbus protocol; man-machine exchange; STC89C58RD single-chip microcomputer

0 引言

Modbus 通信协议是 Modicon 公司于 1979 年开发的,用于实现其 PLC 产品与上位机的通信。由于其简单易用,目前 Modbus 通信协议作为一种通用的工业标准已广泛应用于 PLC、变频器和自动化仪表等设备^[1-4]中。而 PLC、变频器等不具有方便、亲切的人机界面,增加了技术工人的操作难度;在很多应用领域需添加交互界面,但工业级的人机界面或工控机价格昂贵,大大增加设备的生产成本,对小型工业设备来说自然降低了产品的竞争力。

为解决此问题,本研究在分析 Modbus 协议的基础上,结合目前在工业领域应用较为广泛的 SIEMENS S7-200 系列 PLC 及 STC89C51 系列单片机,详述基于 Modbus 协议的 MCU 与 PLC 之间的通讯。

1 Modbus 通信原理

Modbus 协议是一个主-从架构的协议,采用请求-响应方式;包括一个主站,而其他使用 Modbus 协议参与通信的节点为从站,每一个从站都有一个唯一的地址;并且定义了一个控制器能够识别使用的消息结构,以此描述了一个控制器请求访问其他设备的过程,如何回应来自其他设备的请求,以及如何侦测并记录错误信息,从而使控制器可以在网络和其他设备之间完成信息和数据的交换与传送。

ModBus 协议有 ASCII 和 RTU 这两种报文传输模式,它们定义了在这些网络上连续传输的消息段的每一位,以及决定怎样将信息打包成消息域和如何校验。ASCII 模式报文中的每 8 位字节都转换为两个 ASCII 字符发送;而 RTU 模式报文中的每 8 位字节作为两个

十六进制字符,以字节为单位进行传输;所以在相同的波特率下,RTU 模式能够获得更大的数据流量。因此,工业智能仪器仪表一般采用 RTU 模式^[5]。

2 Modbus-RTU 消息帧

Modbus-RTU 消息帧由站地址、功能码、数据域和 CRC 校验域构成。Modbus-RTU 消息帧的结构如图 1 所示。

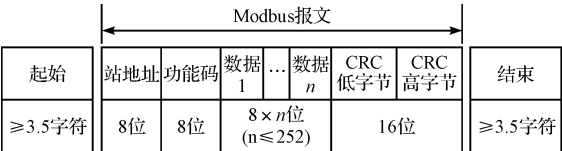


图1 Modbus-RTU 消息帧的结构

站地址:使用 RTU 模式传输的第一个域是站地址,即从站的地址用来选择相应的“从设备”。

功能码:“从站”收到的“消息”里的“功能代码”将告诉“从站”,“主站”需要它完成的动作。S7-200 系列 PLC 支持的 Modbus 从站协议功能如表 1 所示。

表 1 S7-200 支持的 Modbus 从站协议功能

功能	描述
1	读单个或多个线圈(数字量输出)状态,返回任意数量输出点的 ON/OFF 状态
2	读单个或多个线圈(数字量输出)状态,返回任意数量输入点的 ON/OFF 状态
3	读单个或多个保持寄存器,返回 V 存储区的内容。保持寄存器在 Modbus 中以字为单位,在一个请求中最多读 120 个字
4	读单个或多个模拟量输入寄存器,返回模拟量输入值
5	写单个线圈(数字量输出),将数字量输出点置为指定的值,不是被强制,用户程序可以通过 Modbus 请求改写数值
6	写单个保持寄存器。在 S7-200 的变量存储器 V 中写入单个保持寄存器的值
15	写多个线圈(数字量输出),在 Q 映像寄存器中写入多个数字量输出值。输出的其实点必须是一个字节的最低位(例如 Q0.0 或 Q2.0),而且写入输出的点数必须是 8 的整数倍。这些点不是被强调,用户程序应 Modbus 请求改写该值
16	写多个保持寄存器。在 S7-200 的 V 存储器中写入保持寄存器的值,在一个请求中最多可以写 120 个字

数据域:“主机”发给“从机”的“数据域”中,包含了“从机”要完成“功能域”指示的动作时所必需的附加信息。如,寄存器地址等。

CRC 校验:使用 RTU 模式时,信息包括了一个基于 CRC 方法的校验域,判断数据传输的正确与否。通常工业使用的 CRC 编码方法有程序代码法和查表法。

查表法适合比较简单并且传输要求不高的通信,程序代码的编写也有很多不同的版本^[6-8]。

典型的 Modbus-RTU 消息帧没有起始位,也没有停止位,而是以至少 3.5 个字符时间的停顿间隔标志 1 帧的开始或结束。消息帧必须作为一连流的传输。如果在帧完成之前有超过 1.5 个字符时间的停顿时间,接收设备将刷新不完整的消息并假定下一字节是一个新消息的地址域。同样地,如果一个新消息在小于 1.5 个字符时间内接着前个消息开始,接收的设备将认为它是前一消息的延续^[9]。

3 硬件原理框图

S7-200 系列 PLC 的通讯口 Port0 可以支持 Modbus-RTU 协议,成为 Modbus-RTU 从站,其通信接口为 RS-485 接口。STC89C58RD 可以通过串行口与 MAX485 链接,并将操作数据在芯片中成帧,经过接口芯片电平转换发送到总线上以实现与 S7-200 系列 PLC 的串行通信。系统硬件原理框图如图 2 所示,主要包括微控制器、Modbus 接口芯片(MAX485)、人机交互电路(液晶显示、键盘输入)、声光报警等,其中 Modbus 总线可支持 247 个从站。

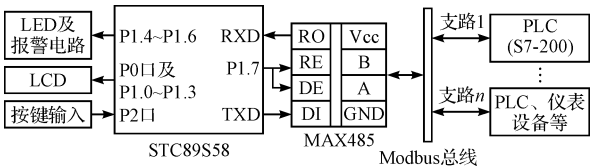


图2 系统硬件框图

在本研究中,单片机选用 STC89C58RD,它在指令集上与传统的 MCS-51 完全兼容;具有较强的抗干扰能力、高速及低功耗等特点;内部扩展了 29 KB E2PROM,可对用户数据进行断电保存,还具有支持程序在线调试和下载等特点。

人机交互电路主要由 LCD(19264)显示电路、按键输入电路、声光报警等组成,可实现对系统功能与参数的设置、显示从站设备(如 S7-200 等)的主要状态并对其进行操作等。

4 软件设计

4.1 系统软件总体规划

系统软件总框图如图 3 所示,主要包括用户人机界面程序、RS-485 异步通信程序和 Modbus-RTU 通信协议实现程序。

其中,人机界面程序包括:LCD 显示程序、键盘扫描及用户参数设置、PLC 从

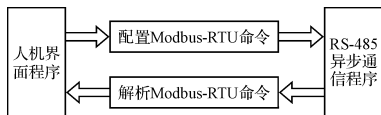


图3 系统软件总框图

站返回数据进行保存并更新显示数据;RS-485 异步通信程序包括:单片机串口接收和发送数据、波特率及数据传输格式配置;Modbus-RTU 通信协议实现程序包括:对需控制的从站点进行 RTU 请求帧的配置、确定接收到的 RTU 响应帧格式、对读取的 RTU 响应帧进行帧解析、以及消息帧传递时的 CRC 校验程序。

4.2 人机界面程序

人机界面程序流程图如图4所示:其主要实现用户对 PLC 设备的控制。首先,用户根据界面提示通过键盘输入对 PLC 设备的操作指令;其次,系统接收用户指令并配置 Modbus 命令,通过通信程序实现系统对从站设备的操作,如改变 PLC 寄存器的某个值、控制或者读取一个或多个 I/O 端口等。当从站设备接收到 Modbus 命令后其自动发送 Modbus 响应帧,如回送一个或者多个寄存器中的数据;主站设备获取响应帧,通过帧解析程序得到响应数据,将数据显示在人机界面对应位置上。

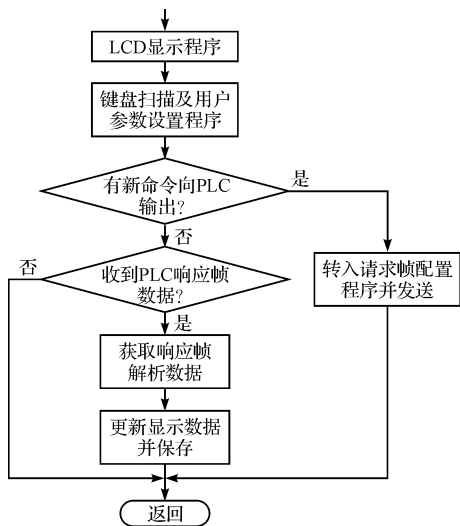


图4 人机界面流程图

4.3 RTU 响应帧格式的确定

Modbus-RTU 通信协议程序实现的重点部分是确定接收到的 RTU 响应帧格式,其主要包括:单片机对响应帧消息连续性的判断、将接收到的 RTU 消息转为有起始和结束的响应帧。

响应帧的连续性是通过测量字符间隔时间来界定的,由串行口中断响应程序取定时器 0 的值和给定值进行比较实现,程序流程图如图5所示。

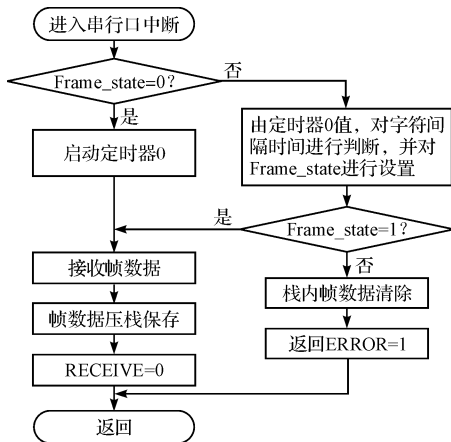


图5 响应帧连续性判断流程图

消息帧状态为 Frame_state,当 Frame_state 为 0 时,表明数据帧接收结束,再次接收时就是另一帧的起始帧;Frame_state 为 1 时,表明接收到的字符是前一消息的延续;Frame_state 为其它值时,表明接收响应帧出错。

响应帧的起始和结束判断是由定时器 0 中断程序实现的,定时器 0 初始为一个特定值(根据异步通信频率进行调整),当定时器 0 发生中断则说明字符传输时间间隔大于 3.5 个字符,响应帧传输结束,程序流程图如图6所示。响应帧接收状态 RECEIVE,当 RECEIVE 为 0 时说明响应帧正在传输,RECEIVE 为 1 时说明响应帧完成传输,并进入帧解析程序。

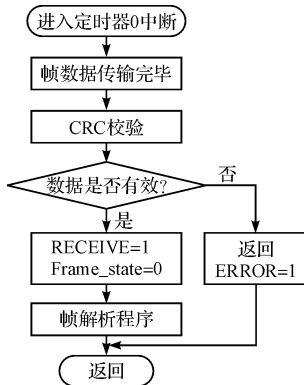


图6 响应帧接收状态判断流程图

5 实验结果

MCU 对 PLC 的 Q 0.0 口操作的 Modbus 通讯数据波形如图7所示;其包括了 MCU 对 PLC 的 Q 0.0 口进行置位请求帧,及 PLC 返回的响应帧。请求帧各部分的值依次为:站地址 1, Q 0.0 的 Modbus 地址为 16# 0000,置位操作字为 16# FF00, CRC 校验码为 16# 3A8C,其响应帧格式如图8所示,说明 MCU 已实现系统对 PLC 的操作^[10]。(下转第 75 页)



图5 客户端用户操作界面

(352 × 288) 格式图像的的稳定传输,延时小,相对其他视频传输系统有了长足的进步。随着 3G 网建成,数据通信速率可达到:静止 2 Mbps,慢速移动 384 Kbps,高速移动 144 Kbps。因此,相应的视频传输帧率在高速移动下能达到近 19 fps,完全可实现流畅监控。

6 结束语

本研究设计了嵌入式无线监控系统,主要针对固定监控客户端,进一步的扩展阶段可考虑开发移动设备监控客户端。与其他远程视频监控系统相比,本系统有如下优点:

(1) 传输效率高,低传输带宽要求,系统可在低至约 30 ~ 40 Kbps 码率下保持稳定进行 4 ~ 5 fps 播放速

率。采用 UDP 协议传输,自行设计数据丢失及重传等处理机制,有效地提高传输效率。

(2) 安装方便快捷,使用方便,扩展性好。基于嵌入式系统开发,系统硬件体积小,易于安装。在网络中的每一台计算机,只要安装客户端,就可以实现远程监控。

(3) 覆盖范围广,几乎不受区域限制。采用无线传输网络,不受有线布线范围限制,只要在无线通讯覆盖范围内都可安装使用。

参考文献 (References):

- [1] 陈文祥,孟利民. 新型嵌入式视频监控系统的设计[J]. 电子器件应用,2008,10(2):56-58,62.
- [2] 阮越广,赵伟胜. 基于无线网络的家用安全视频监控系统[J]. 机电工程,2008,25(8):58-61.
- [3] 罗小科,朱善安. 无线视频监控系统视频传输模块的软件设计[J]. 机电工程,2007,24(1):42-45.
- [4] 刘源,朱善安,叶旭东. 基于 DM642 的嵌入式视频监控系统硬件设计[J]. 电子器件,2006,29(3):905-908.
- [5] CHIASSERINI C F, MAGLI E. Energy efficient coding and error control for wireless video surveillance networks[J]. **Telecommunication Systems**,2004,26(2-4):369-387.
- [6] LEE Y C, ALTUNBASAK Y, MERSEREAU R M. Multi-frame error concealment for MPEG-coded video delivery over error-prone networks[J]. **IEEE Transactions on Image Processing**,2002,11(11):1314-1331.
- [7] 陆其明. Directshow 开发指南[M]. 北京:清华大学出版社,2003.

[编辑:李辉]

(上接第 54 页)

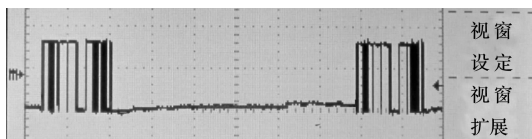


图7 MCU 对 PLC Q 0.0 置位的 Modbus 数据波形

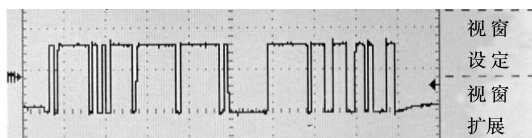


图8 MCU 对 Q 0.0 置位的响应帧格式

6 结束语

本研究通过对 Modbus 通信协议的介绍与研究,设计了基于 Modbus 协议的 MCU 与 PLC 通信系统。该系统实现了 MCU 与 S7-200 系列 PLC 的 Modbus-RTU 通信,使 PLC 设备可通过系统的人机交互程序进行控制,解决了其交互性能差的缺点;也为 Modbus 协议在工控领域的应用提供了参考和解决方案,并可方便地移植到工业设备中。该系统具有成本低、适用性强等特点,将具有良好的推广应用前景。

参考文献 (References):

- [1] 卢文俊,冷杉,杨建军. 基于 Modbus 协议的控制器远程监控系统[J]. 电力自动化设备,2003,23(6):54-56.
- [2] 潘洪跃. 基于 MODBUS 协议通信的设计与实现[J]. 计量技术,2002(4):35-36.
- [3] 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[J]. 超重运输机械,2008(7):39-42.
- [4] 叶露林,洪雷峰. 新型智能通风系统[J]. 机电工程技术,2008,37(11):45-47.
- [5] 廖常初. PLC 编程及应用[M]. 2 版. 北京:机械工业出版社,2005:155-163.
- [6] CHEN L. Research on Voltage Acquisition System Based on Modbus Industrial Bus and Single Chip[C]//2009 International Conference on Signal Processing Systems,2009:585-588.
- [7] 胡金华. 基于 PLC 自由通信的 CRC 校验算法实现[J]. 机电工程,2007,24(10):19-21.
- [8] 赵晓明,徐立,邵威,等. 基于 VC++ 的上位机与西门子系列 PLC 通信的研究[J]. 机电工程,2007,24(7):42-44.
- [9] 潘悦,佟为明,赵志衡. 基于 C8051F02x 单片机的 Modbus 实验系统[J]. 仪器仪表学报,2007,28(4):305-306.
- [10] 李晓波,高倩. 基于触摸屏和 PLC 的交通灯监控系统设计[J]. 机电技术,2008(4):63-65.

[编辑:张翔]