

AB PLC 与 MODBUS 网络的通信

The communication between AB PLC and MODBUS network

(西村水厂) 曾永基

Ceng, Yongji

摘要: 介绍了应用 3100/3150-MCM 模块实现 AB PLC 与 MODBUS 网络通讯的方法,该方法使用 MODBUS 协议,通过开发 AB PLC 的应用程序,从而实现主从结构网络通信

关键词: 3100/3150-MCM 模块;AB PLC;MODBUS;主从通信

中图分类号:TP393.12 文献标识码:A

文章编号:1008-0570(2004)06-0012-03

Abstract: This paper introduces the application of 3100/3150-MCM in the communication between AB PLC and MODBUS network. By using MODBUS protocol and developing program of PLC, a master-slave structure network can be setup.

Keywords: 3100/3150-MCM;AB PLC; MODBUS; master-slave communication

1 引言

目前的工业控制现场大量使用了 PLC 和各种智能仪表用于生产过程控制。随着控制规模的扩大和控制功能的复杂化,常需要多台 PLC 及一定数量的外设仪表组成一个控制系统。

MODBUS 是美国 MODICON 公司制订的一种串行传输协议,可实现主从命令响应型通信。作为一种工业通信和分布式控制系统协议,已经得到多家公司的 PLC 和智能仪表支持。

A-B 公司(Allen-Bradley)是美国生产可编程控制器的主要厂家之一,具有先进的通信和数据处理功能。在水处理行业中,使用大量的可编程控制器用于生产过程控制,其中 A-B 公司的 PLC 占了相当的比重。

由于不同硬件厂商支持不同的工业通信和分布式控制系统协议,要实现 AB PLC 与 MODBUS 仪表组成控制网络,实现设备的连网,就存在着互相通信协议转换问题。

3100/3150-MCM 模块是 PROSOFT TECHNOLOGY 公司推出的在 AB PLC 通用框架上安装的 MODBUS 通信接口模块。该模块可以实现 AB PLC 与 MODBUS 现场设备之间的通信,从而使 AB PLC 通信能力得到增强,灵活实现 AB PLC 与 MODBUS 网络的互连,完成复杂的控制要求。

本文基于自来水厂泵站集散控制系统的设计,着重介绍 AB 公司的 SLC 系列的 PLC 通过 3150-MCM 模块和 MODBUS 网络连接的实现方法。

2 系统联网方案

自来水厂泵站集散控制系统,不仅实现一般的逻辑控制,还具备了包括模拟量在内的数值处理和网络通信等功能。在现场的实际应用中,系统使用的电机保护装置 Sepam2000 采用了 MODBUS 通信协议,出于系统控制功能的需要,要求在 AB PLC 中实现对 MODBUS 协议的支持。我们利用 3150-MCM 模块建立起 MODBUS 设备网。

系统的网络结构遵循 MODBUS 协议的规范,采用标准简单的主从总线结构,以 PLC 作为主机发起通信,多台电机保护装置 Sepam2000 作为从机,各从机在进行传输之前必需要等待来自主机的允许信号。主机可以发送和接收来自通信链上从机的信息,而从机则始终处于被动状态,随时准备响应来自主机的通信请求。设备层部分网络结构如图 1。

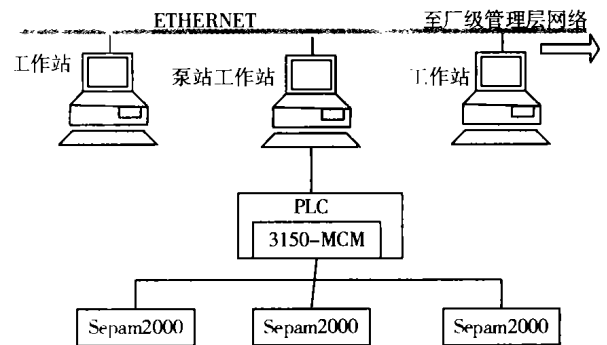


图1 设备层拓扑结构示意图

3 Sepam2000 及 MODBUS 协议的介绍

Sepam2000 作为电机保护装置,提供了所有保护、测量、控制、通信等功能。Sepam2000 与远程监控系统之间的通信是采用 MODBUS 协议的通信方式。

MODBUS 的通信采用的是一种主/从式数据传输,在主从结构的通信方式中,有一台主机,多台从机,主机可与各个从机作双向通信,而各从机之间不能通信。主机与各个从机通信的报文形式为请求/响应帧方式。每次通信均由主机发起,不需握手。主机发出请求帧后,等待从机返回响应帧直至响应时间超时。从机只能通过提供数据响应主机的请求,或根据请求做出相应的动作。

MODBUS 协议定义了主机请求的格式,包括:请求的编址,要求动作的功能编码,传输数据和错误校验等。请求中的编址(即地址码)提供接收主机报文的从机地址,从机根据地址判别是否接受该请求,用户必须设置每台从机的地址。功能编码告诉指定编址的从机完成什么样的动作。数据字段中包含了从机执行任务时所需的附加信息。例如,功能编码 03 表示读取从机的保持寄存器并返回其中的内容,数据区中的信息就必须告诉从机从哪个寄存器开始读,需要读的寄存器数。错误校验字段为从机提供了信息完整性校验的方法。同样,响应的格式也是采用 MODBUS 协议结构,从机响应的功能编码与接受的请求的功能编码相对应,数据字段包含根据请求返回的数据,错误校验字段允许主机确认信息内容是否有效。

MODBUS 协议共有 24 种功能编码,但是并不都适用于 Sepam2000,实际应用中 Sepam2000 只是支持下面有限的几种:

- 01 读取输出状态
- 02 读取输入状态
- 03 读取内部寄存器内容
- 04 读取输入寄存器内容

- 05 强制单个输出状态
- 06 刷新单个寄存器内容
- 07 读取异常事件状态
- 08 诊断测试
- 11 读取计数器和状态字
- 15 强制多个输出状态
- 16 刷新多个寄存器内容

如果主机希望读取 2 号 Sepam2000 从机中寄存器 0805h-080Ah 的内容,则需要调用功能 03。主机请求和从机响应的帧格式如下:

请求帧:

地址	功能号	数据起始寄存器编号	寄存器数目	错误校验字段
2	03	0C05	06	CRC16

响应帧:

地址	功能号	字节计数	数据寄存器 (0805)	数据寄存器 (080A)	错误校验字段
2	03	0C	Data1	Data6	CRC16

而如果主机希望刷新 2 号 Sepam2000 从机中寄存器 0810h 的内容并把寄存器内容设置为 1000,则需要调用功能 06。主机请求和从机响应的帧格式如下:

请求帧:

地址	功能号	寄存器编号	设置值	错误校验字段
2	06	0C0E	1000	CRC16

响应帧: (返回收到的请求帧)

地址	功能号	寄存器编号	设置值	错误校验字段
2	06	0C0E	1000	CRC16

Sepam2000 的帧格式以及所执行的功能都有明确的定义,不能随意更改。在通信过程中,要确保主机和各从机的对应关系正确。此外,用户可以根据实际需要配置合适的传输波特率、字符奇偶校验、停止位的个数等通信参数设置。

4 AB PLC 中 MODBUS 协议的实现

1.MCM 模块的通信控制

PROSOFT TECHNOLOGY 公司的 3100/3150-MCM 通信模块,相当于网络接口,PLC 通过 MCM 模块与 MODBUS 总线相连。MCM 模块能快速、可靠地在 AB PLC 中实现 MODBUS 协议。

3100/3150-MCM 通信模块可供用户选择使用主机模式或者从机模式。当 MCM 模块设定为主机,它对连接到总线上的从机进行控制,支持 MODBUS 协议中(01、02、03、04、05、06、15、16)8 种功能编码,可以发送多达一百条定制的请求指令,并支持以“广播”方式发出请求。当 MCM 模块指定为从机,它响应主机的请求,此时能够支持 MODBUS 协议中(01、02、03、04、05、06、08、15、16)9 种功能编码。同时,无论是主机模式或者是从机模式,3100/3150-MCM 通信模块都支持 ASCII 和 RTU 两种传输模式。

当 AB PLC 配置了 3100/3150-MCM 通信模块作为主机模式时,PLC 采用周期扫描方式,按请求指令的顺序与从机交换数据。每次扫描期间,处理器使用逻辑写指令将主机内存中要输出到各从机的数据传送到 3100/3150-MCM 通信模块中的发送缓冲区,模块根据存储的功能指令,发送到指定的从机;而各从机响应后返回的数据,3100/3150-MCM 通信模块将其先存放在接收缓冲区,然后 PLC 使用逻辑读指令把数据移入相应的输入数据存储器。周而复始,使主机与从机中的数据得到周期性的刷

新。整个数据流程如图 2 所示:

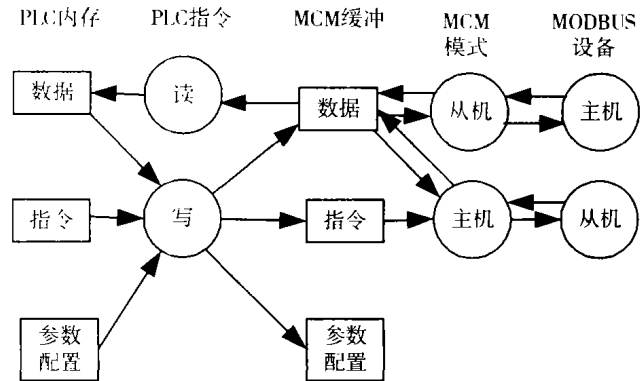


图2 MCM模块数据流程示意图

2.MCM 模块与 MODBUS 的硬件连接

MCM 模块使用的是与 RS232C 兼容的标准通讯接口,但在实际应用中由于要实现多点通信,所以采用 RS485 方式。图 3 是 3150-MCM 模块 9 芯串行口与 MODBUS 的连接图。

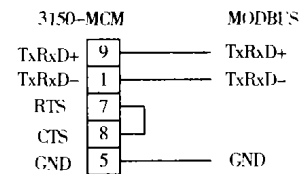


图3 3150-MCM端口与MODBUS连接示意图

3.MCM 模块的缓冲区管理

PLC 与 MCM 模块之间是通过模块输入、输出映像文件进行数据传送。PLC 写数据时,将数据写入输出映像文件,然后 3100/3150-MCM 通信模块把数据映射到相应的缓冲区位置上;PLC 读数据时,根据映射地址,从输入映像文件中读取模块缓冲区中对应地址的数据。映像文件的数据传送单位为一个 50 字节的数据块,PLC 必须循环地一次传送一个数据块。

MCM 把缓冲区按数据传送的单位大小,分为若干个块,并一一标号,用块号对应起来,并且划分为三个区,分别用于数据、指令、参数设置。数据存储区从 0 块号开始,结束于 79 块号,中间有 4000 个字节的空间,用于存储接收的数据和发送的数据,是主机、从机交换数据的场所;指令存储区从第 80 块至第 99 块,共 1000 个字节,用于存储主机模式下,模块的功能指令表,每次扫描,顺序按功能指令列表向从机发出请求帧;第 255 块前 40 个字节则专门定义为模块设置参数存储区,用于初始化模块。

在通信过程中,首先要对主机进行初始化,即对第 255 块号对应的缓冲区内容进行参数配置,主要是定义通信端口的设置,模块缓冲区的详细划分。设置的有以下参数:

- (1) 定义 MCM 通信模块两个独立的通讯接口设置,包括:选择主机模式或者从机模式、定义字符奇偶校验、停止位的个数,传输的波特率,响应延时等参数。
- (2) 定义模块的缓冲区中存储接收数据的数据存储区。包括:接收数据存储区的起始块号,存储区的连续块数。
- (3) 定义模块的缓冲区中存储发送数据的数据存储区。包括:发送数据存储区的起始块号,存储区的连续块数。
- (4) 定义模块的缓冲区中指令存储区。由于指令存储区固定从 80 号数据块开始,所以只需指定存储区的块数。

4.MCM 模块的功能指令设置

MCM 模块处于主机模式下时,功能指令列表存放在模块缓冲区中的指令存储区。主机向从机发出请求时,模块从指令存储区逐条读出功能指令,并按照 MODBUS 请求帧格式发送数据。

指令存储区中每条功能指令的具体内容如下:

1	模块通信端口选择
2	从机的站地址。从机在接收数据时将本站编址的值与收到的站地址比较,以此判定信息是否是发给本站的。而主机在接收时则将收到的站地址与发送的站地址比较,以判断是否是正确的从机响应
3	指令的功能编码
4	源地址。即主机要发送或接收的数据在缓冲区中的起始数据地址
5	数据长度。即主机要发送或接收的数据的字节数
6	目的地址。即从机要接收或响应的数据的寄存器地址
7	数据的类型。用于标示读、写的的数据是双字节的浮点数还是单字节的整数
8	轮询时间

如果主机希望在1号通讯接口读取2号Sepam2000从机中寄存器0805h-080Ah的内容并存放放到模块缓冲区第50个字节开始的连续6个字节中,功能指令内容如下:

端口号	从机地址	功能编码	源地址	数据长度	目的地址	类型	时间
1	2	3	50	6	0805	0	0

5. AB PLC 通讯程序的开发

程序执行时,在第一个扫描周期,都必须设置MCM的状态,即初始化MCM模块。

通信程序中,PLC在输入、输出映像文件中为MCM缓冲区设置当前以及后续读写指针,分别指向当前MCM缓冲区数据块号,后续缓冲区数据块号。若MCM处于数据传送允许状态,即I1:I/0=1, O0:I/0=0时,PLC判别当前读写指针,调用相应读写逻辑指令。如果指针指向接收数据的数据存储区,则PLC从MCM模块中接收数据;如果指针指向发送数据的数据存储区,则PLC向MCM模块发送数据;如果指针指向指令存储区,则PLC向MCM模块传送功能指令。每次执行一个数据块的传送,并在传送后,把后续读写指针覆盖当前读写指针,从而在下一个扫描周期进行下一个数据块的传送。PLC自动周期性扫描,按照编定的功能指令向从机的输入/输出数据进行发送/接收,以满足数据传输的要求。

根据PLC的逻辑指令及MCM的通信原理,画出了图4所示的主机通信程序结构框图。

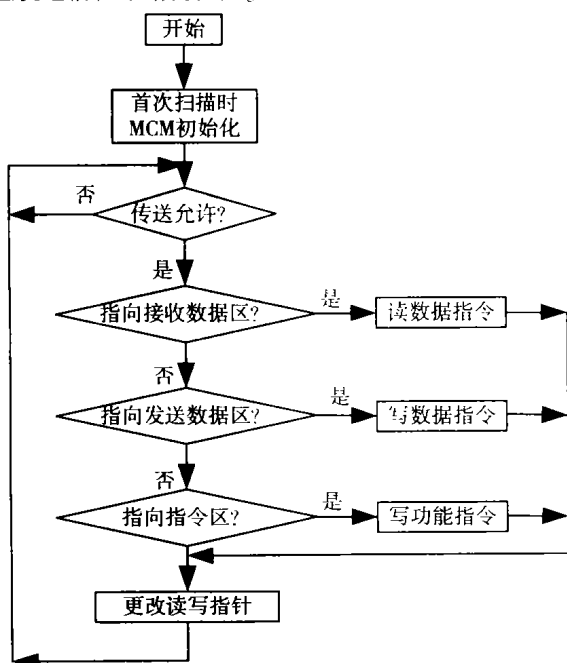


图4 PLC程序框图

5 结束语

经过现场调试,实现了1台AB PLC与13台SEPAM2000组成的MODBUS网络连接。实际应用证明,这种方式组成的系统结构简单,应用方便,能满足复杂的控制需要。

参考文献

- [1]3100/3150 MCM USER Manual, ProSoft Technology, 1997.
- [2]AB PLC Programming Reference Manual, AB, 1997.
- [3]Sepam2000 Communication protocol, Schneider, 1999.

作者简介:曾永基:(1975.3~),男,广东省台山市人。1998年毕业于华南理工大学自动控制专业,现在广州市自来水公司工作,主要从事水处理行业自动控制系统的设计开发工作。E-mail: ira2000@21cn.com, 电话:13189028145

(510160 广东省广州市环市西路水厂路3号西村水厂)曾永基

(收稿日期:2003.12.11)

(接第94页)更高的要求。在这种形式下,要提高开发的效率,必须采用IP复用技术来进行大规模FPGA的开发设计。

IP即知识产权(Intellectual Property),是预先设计好的电路功能模块。IP核可以分为软核,硬核和固核。软核是用RTL级或门级HDL描述的功能模块,软核不涉及具体的硬件实现。硬核是结合特定的工艺参数经过电路布局布线后的设计。而固核则是介于硬核和软核之间的IP,是完成了综合的功能块,它允许用户重新设定关键性能参数。大多数的FPGA厂商都有自己的IP库,这些库往往是谁它们的开发工具一起提供的。随着IP产业的发展,一大批IP的专业开发公司不断开发出新的高性能的IP模块,因此,IP资源应该是相当丰富的。当我们采用自顶向下的方式进行大规模FPGA开发的时候,为了提高开发的效率,应该优先考虑将各个功能模块用现成的IP模块来实现,因为这些IP模块的功能是经过验证的,从而可以大大的节省开发时间,同时提高系统的性能。如果采用传统的设计方法,是很难在较短的时间内设计出高性能的大规模FPGA应用系统的。

参考文献:

- [1]王国平,周端.高性能低功耗微控制器IP软核设计综述.计算机应用与研究第二期.2003
- [2]夏宇闻.复杂数字电路与系统的Verilog HDL设计技术.北京:北京航空航天大学出版社.1998.

作者简介:袁本荣(1980.3.12~),男,汉族,湖北石首人,北京理工大学计算机科学与工程系计算机软件应用专业硕士研究生,主要研究方向:模式识别、图像处理;E-mail: ybr312.student@sina.com;手机:13810364226;刘万春(1949~),男,河北栾县人,教授,主要研究方向:图像分析与理解、数据挖掘。贾云得(1962~),男,山西大同人,教授,博士生导师,主要研究方向:人工智能、计算机视觉、人机交互技术;朱玉文(1950~),女,四川邛崃人,副教授,主要研究方向:图像分析与理解;

Author brief introduction: Yuan, Benrong, Mar. 12, 1980, the Han nationality, native place of Shishou city. Hubei province, Dept. of Computer Science and Engineer, school of Beijing Institute of Technology, major of Computer Application, Master Degree, research field of Pattern Recognition and image process.

(100081 北京理工大学计算机科学与工程系2001级硕士1班)袁本荣 刘万春 贾云得 朱玉文

(Department of Computer Science and Engineering, Beijing Institute of Technology, Beijing 100081, China) Yuan, Benrong Liu, Wanchun Jia, Yunde Zhu, Yuwen

(收稿日期:2003.12.2)