S7-1200PLC 基于 Modbus 通信协议的数据采集及远程传送应用

通过采集各个换热站房的实时数据，建立集中供热热网监控系统既可以实时总览热网当前运行工况又可以分析室外温度及系统供热量变化趋势，做出整体运行规划，指导运行实现自动控制。

Modbus 协议是一种已广泛应用于当今工业控制领域的通用通信协议。通过此协议，控制器相互之间、或控制器经由网络（如以太网）可以和其它设备之间进行通信。Modbus 通信物理接口可以选用串口（包括 RS232 和 RS485），也可以选择以太网口。

S7-1200 设计紧凑、组态灵活且具有功能强大的指令集，这些特点的组合使它成为控制各种应用的完美解决方案。TIA博途全集成自动化软件用于S7-1200项目管理、编程和调试，在库函数中嵌套了Modbus-RTU 和Modbus-TCP功能库，可以利用该库函数顺利完成PLC与第三方设备和上位机的通信。

1 系统概述

典型换热站所需监测的运行参数有一次侧供水压力和供水温度、一次侧回水压力和回水温度、二次侧供水压力和供水温度、二次侧回水压力和回水温度、循环变频器工作频率和故障状态、补水变频器工作频率和故障状态。各换热站现场 PLC 与智能仪表和变频器通信采集系统运行数，并通过 Internet 或企业局域网，上传至主控中心。操作员从控制中心通过该系统能够方便地得到子站运行的数据并向子站下达控制指令。数据采集以及远程传送系统连接如图 1 所示。

图 1 换热站数据采集以及远程传送系统图

2 系统设计

2.1 站内设备数据采集系统设计

目前大多数换热站内设备的运行参数都是通过智能仪表进行运算处理后显示。智能仪表兼备标准模拟量信号输出接口和 RS485 Modbus 协议通信接口。变频器工作状态输出也可以通过数字量输出接口、标准模拟量信号输出接口和 RS485 Modbus 协议通信接口输出。数字量输出和模拟量输出能够表达的状态位和数据内容非常有限，而以支持 Modbus 协议的通信方式可以读出几乎所有的工作参数值，并能够实现远程参数修改和控制。因此选择 485 总线方式连接换热站房内智能仪表、变频器与 PLC 通信模块，并通过 Modbus-RTU 协议进行设备间通信是一个优选方案。

在 Modbus-RTU 总线通信中，智能仪表及变频器作为从站，只需 选择 Modbus-RTU 通信协议并且为设备分配不重复的站地址即可。所有主从站点的通信端口设置参数必须一致。

S7-1200 PLC 作为主站必须配备 RS485 通信模块才能实现 Modbus-RTU 协议通信。S7-1200

PLC 提供了专门的 Modbus 库实现 Modbus-RTU 通信，其通信的基本原理是：首先 S7-1200 PLC 程序开始运行时，调用一次 Modbus 库中的功能块 MB_COMM_LOAD 来组态 CM11241 RS485 模块上的端口，对端口进行配置；其次调用 Modbus 库中的功能块 MB_MASTER 作为 Modbus 主站与支持 Modbus 协议的设备进行通信。

S7-1200PLC 作为主站通信是由 DATA_ADDR（从站中的起始 Modbus 地址）和 MODE（读、写、诊断模式）参数一起确定实际 Modbus 消息中使用的功能代码。DATA_PTR(数据指针)指向要写入或读取的数据的 CPU DB 地址，该 DB 必须为“非仅符号访问”DB 类型。在 TIA V12 以上平台中，将该 DB 属性中的“优化的块访问”选项取消。

S7-1200 PLC 主站发送带有站地址标识的数据来寻址不同的从站，同时不同的从站通过响应带有站地址标识的数据给主站，以完成整个通信过程。这种轮询通信，可以根据发送和接收完成的标志来完成，即发送完成后启动接收，接收完成后再启动下一次发送。也可以以固定的时间间隔进行轮询。每个 S7-1200 CPU 的 CM1241 485 通信模块理论上最多支持 247 个 Modbus 子站，但是在实际应用时需要考虑 CPU 的性能以及轮循 Modbus 子站时间。

2.2 数据远程传送系统设计

Modbus-TCP 是标准的网络通信协议,S7-1200 PLC 通过 CPU 上 PN 接口进行 TCP/IP 通信，不需要额外的通信硬件模块，Modbus-TCP 使用开放式用户通信连接作为 Modbus 通信路径。在 S7-1200 PLC 的库函数中嵌套了 Modbus-TCP 功能块库， 它包含了 Server 和 Client 的库函数, 编程时可以直接调用该库函数可实现与上位机的 Modbus-TCP 通信。

在该系统应用中 S7-1200 PLC 作为 Modbus Tcp Server（服务器），调用 “MB_SERVER”指令处理 Modbus-TCP 客户机的连接请求、接收 Modbus 功能的请求并发送响应，设置连接 ID、IP 端口等参数。

MB_HOLD_REG 是 “MB_SERVER”指令的 Modbus 保持寄存器的指针，保持寄存器可以是全局 DB 块或 M 区，如果是 DB 块则需要定义为“非仅符号访问”DB 类型。

S7-1200 PLC 作为网络的服务器端，上位机可以按需建立连接访问 PLC 的数据区，这样在上位机对多个换热站的 PLC 连接中不会占用太多的资源。

3 结束语

本设计方案在多个城市供热系统中得到应用。实际运行结果表明，该控制系统抗干扰能力强、自动化程度高，并可以大量减少现场布线，是一种很好的工程化实现方法。通过以太网的方式进行数据远传也是当前最稳定的数据传送方式。S7-1200 PLC 同时支持有关基于字符的串行协议的点对点通信，可为通信提供更大的自由度和灵活性编程。