第35卷 第11期 计 算 机 工 程 2009年6月
Vol.35 No.11 Computer Engineering June 2009
·工程应用技术与实现· 文章编号：1000—3428(2009)11—0254—02 文献标识码：A 中图分类号：TP273

S7-300 中 Modbus 协议的免驱动应用

陈 群
(南京工业大学信息科学与工程学院，南京 210009)

摘 要：介绍在 SIMATIC S7-300 PLC 控制系统中，利用对串口通信模块的软件编程，实现 Modbus RTU master/slave 通信的应用。实际生产应用表明，该方案在保证有效可靠的通信质量的同时，免除购买 Siemens 公司 Modbus 协议驱动模块的格外开销，具有值得推广的经济意义。

关键词：可编程逻辑控制器；Modbus 协议；串行通信

Non-driver Application of Modbus Protocol in S7-300

CHEN Qun
(College of Information Science and Engineering, Nanjing University of Technology, Nanjing 210009)

【Abstract】This paper describes the realization of Modbus RTU master/salve protocol based on SIMATIC S7-300 PLC point-to-point communication module. In a practical packaging control system, data is transmitted reliably and effectively. The scheme is worth promoting economic significance, for avoiding the expense of Siemens driver module of Modbus protocol.

【Key words】Programmable Logic Controller(PLC); Modbus protocol; serial communication

1 概述

随着现代工业自动控制系统往智能化、网络化和开放式结构方向的发展，现场总线技术的应用越来越广泛。Modbus作为一种通用的现场总线得到越来越普遍的现场设备接口支持。这对于很多基于 SIMATIC PLC 实现智能控制系统而言，就必须购买额外的协议驱动模块来完成通信，给系统开发增加不少的经济支出。本文在阐述 Modbus 通信协议的基础上，介绍在某厂通过对 SIMATIC S7-300 PLC 中串口通信模块 CP341 的软件编程，实现 Modbus RTU master/slave 协议。生产实践表明，基于此方案实现的系统通信是有效可靠的。

2 系统通信构成

某炼油厂的罐区管理控制系统主要用于对 3 组罐区中 24 个罐体液位容量进行监视管理、数据采集和过程控制。系统控制中心 SIMATIC S7-300 PLC 与现场带 Modbus 接口的 enraf 雷达液位计以屏蔽双绞线连接，作 Modbus 总线主站通信，需要对现场设备进行数据采集；与 Honeywell TDS 型 DCS 以光缆连接，作 Modbus 总线从站通信，接收来自中控室操作指令。

3 Modbus协议介绍

Modbus 协议最初由 Modicon 公司开发出来，在 1979 年末该公司成为施耐德自动化(Schneider Automation)部门的一部分，现在 Modbus 已经是工业领域全球最流行的协议。此协议支持传统的 RS-232, RS-422, RS-485 和以太网设备。许多工业设备，包括 PLC、DCS、智能仪表等都在使用 Modbus 协议作为它们之间的通信标准。有了它，不同厂商生产的控制设备可以连成工业网络，进行集中监控。

Modbus协议包括：ASCII, RTU, TCP等。Modbus的ASCII、RTU协议规定了消息、数据的结构、命令和就答的方式，数据通信采用Maser/Slave方式，Master端发出数据请求消息，Slave端接收到正确消息后就可以发送数据到Master端以响应请求；Master端也可以直接发消息修改Slave端的数据，实现双向读写。

Modbus 协议需要对数据进行校验，串行协议中除有奇偶校验外，ASCII 模式采用 LRC 校验，RTU 模式采用 16 bit CRC 校验，但 TCP 模式没有额外规定校验，因为 TCP 协议是一个面向连接的可靠协议。另外，Modbus 采用主从方式定时收发数据，在实际使用中如果某 Slave 站点断开后(如故障或关机)，Master 端可以诊断出来，而当故障修复后，网络又可自动接通。因此，Modbus 协议的可靠性较好[1]。

本系统采用较高数据传送密度的 RTU 通信模式，协议定义其消息帧结构如图 1 所示。

起始位	设备地址	功能码	数 据	CRC	结束符
T1-T2-T3-T4	8 bit	8 bit	*N*个8 bit	16 bit	T1-T2-T3-T4

图 1 RTU 消息帧

Modbus 协议定义了 3 种功能码：公共功能码，用户定义功能码，保留功能码。本系统中支持公共功能码 01, 02, 03, 04, 05, 06, 15, 16，其中，Modbus slave 程序中支持功能码 01, 02 的实现方式相同，03, 04 的实现方式相同[2]。

4 系统通信实现

4.1 CP341 模块

CP341 是西门子 S7-300 系列点到点的串口通信模块，可以在 SIMATIC S7-300 中使用，其硬件接口可采用 RS232, TTY, RS422/485(X27)方式；软件协议有 Modbus Master, 3694 (R), RK512 和 ASCII。本系统选用 RS485 接口的 CP341 模块，使用集成在CP341内的ASCII Driver通信协议来实现Modbus master/slave RTU 协议。

作者简介：陈 群(1984－)，男，硕士研究生，主研方向：计算机控制

收稿日期：2008-11-15 **E-mail：**nodoor2004@163.com

CP341 用功能块 FB7"P_RCV_RK"接收数据，用 FB8"P_SND_RK"发送数据，在用户程序中，FB7/FB8 分别有一个背景数据块，FB7/FB8 是无条件调用的，数据的发送或接收可以是循环的，也可以是时间驱动的[3]。

在 STEP7 参数化工具中进行参数设置：字符延迟时间 4 ms 作为接收帧结束方式；波特率 9 600 Kb/s，8 bit 数据位，1 bit 结束位，1 bit 偶校验位；RS485 接口方式；其余为默认设置。

4.2 CRC校验实现

不论是做主机还是从机，消息帧的 CRC 校验至关重要。CRC 校验程序是通信程序成功运行的前提，只有 CRC 校验结果正确，RTU 从机才能正确响应主机的请求，RTU 主机才能正确接收从站的数据。

CRC域是 2 个字节，包含 16 bit的二进制值。CRC是先调入值是全“1”的 16 bit寄存器，然后调用一过程将消息中连续的 8 bit 字节各当前寄存器中的值进行处理。仅每个字符中的 8 bit数据对CRC有效，起始位和停止位以及奇偶校验位均无效。

CRC 产生过程中，每个 8 bit 字符都单独和寄存器内容相或(OR)，结果向最低有效位方向移动，最高有效位以 0 填充。LSB 被提取出来检测，如果 LSB 为 1，寄存器单独和预置的值或一下，如果 LSB 为 0，则不进行。整个过程要重复 8 次。在最后一位(第 8 bit)完成后，下一个 8 bit 字节又单独和寄存器的当前值相或。最终寄存器中的值，是消息中所有的字节都执行之后的 CRC 值[4-5]。

4.3 Modbus RTU master协议实现设计

在 S7 300PLC 上实现 Modbus RTU master 协议，是为了建立与 24 个罐体液位计的数据通信。采用同一个源数据块 DB42 存放 PLC 向所有从机发送的命令，定义数据块 DB43 存放从机的应答消息。针对不同地址号的液位计，只要修改数据块中相应的设备地址、功能码、数据起始地址、数据数量和 CRC 校验码即可。发送功能块 FC21 调用 FB8 发送数据，并将请求消息保存在 DB40 中，接收功能块 FC23 调用 FB7 接收数据，并将应答消息保存在 DB41 中。程序中循环中断组织块 OB35 依次执行命令号从 1~24 的递增，来完成 PLC 的轮询。其程序实现流程如图 2 所示。

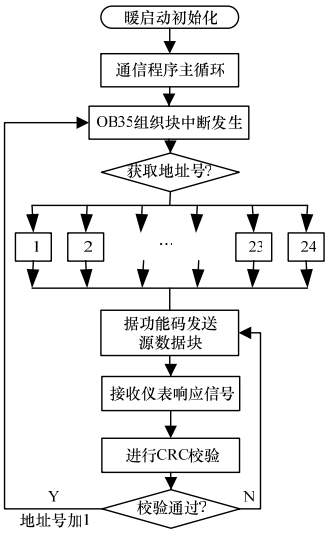

图 2 Modbus 主机协议实现流程

罐区管理控制系统中 PLC 采集每个罐体的液位信号有：Modbus 地址 10032~10056。程序运行后，PLC 作为 Modbus 主机能正确获得现场仪表采集的数据。

4.4 Modbus RTU slave协议实现设计

实现 Modbus RTU slave 协议，是为了建立和主机系统的数据连接。

PLC 装载 CP341 后，使用通信功能块 FB7 接收主机请求消息，将请求消息存放至请求数据块 DB33。利用其中由主机发送过来的占 2 B 的 CRC 校验值，进行校验计算。结果为 0 时，表示接收无误。PLC 再根据请求数据块 DB33 中功能码、数据起始地址、数据数量的要求，操作 PLC 对应内存空间的存储单元，响应数据块 DB34 中组织需要返回主机的响应消息。响应数据长度及校验值存储分 2 类，FC01, 02, 03, 04 的响应消息校验前数据长度为 byte_count+3，校验后数据长度为 byte_count+3＋2。FC05, 06, 15, 16 的响应消息校验前数据长度为 6，校验后数据长度为 8。组织好响应数据块后，调用 FB8 将响应消息发送至主机，其程序实现流程如图 3 所示。

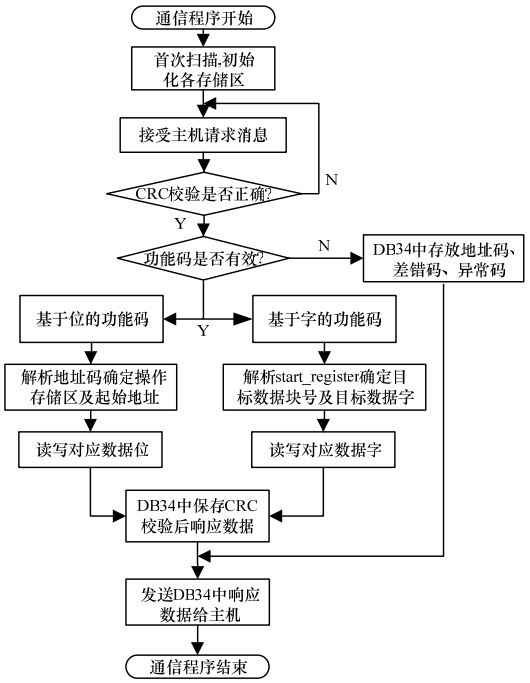

图 3 Modbus 从机协议实现流程

表 1 中列出各功能码在 Modbus 规范中功能和在 PLC SIMATIC CPU 中的数据操作区域及区域获取方式的对应关系。

表 1 SIMATIC 空间的功能码

功能码	Modbus 规范中功能	SIMATIC S7 中功能	
		获取方式	SIMATIC 数据类型
01	读线圈状态	按位读	内存位 M
		按位读	输出 Q
		按位读(16 bit 间隔)	定时器 T
		按位读(16 bit 间隔)	计数器 C
02	读输入状态	按位读	内存位 M
		按位读	输入 I
03	读保持寄存器	按位读	数据块 DB
04	读输入寄存器	按位读	数据块 DB
05	强制单个线圈	按位写	内存位 M
		按位写	输出 Q
06	预置单个寄存器	按位写	数据块 DB
15	强制多个线圈	按位写(1 bit~2 040 bit)	内存位 M
		按位写(1 bit~2 040 bit)	输出 Q
16	预置多个保持寄存器	按位写(1 个~127 个寄存器)	数据块 DB

（下转第 259 页）