S7 – 300 与第三方设备 Modbus 通讯的实现

涂智辉,高士臣

(内蒙古包钢钢联股份有限公司计量中心,内蒙古 包头 014010)

摘 要: Modbus 协议是应用于电子控制器上的一种通用语言。通过此协议,控制器相互之间、经由网络和其它设备之间可以通信。文章讲述了 S7 – 300 PLC 通过 CP341 模块与第三方设备之间的网络通讯,给出了具体的通讯协议,技术问题的解决思路,以及部分实现代码示例。

关键词: S7 – 300 PLC; Modbus; CP341

中图分类号: TP273^{+}.5 **文献标识码**: B **文章编号**: 1009 – 5438(2018)01 – 0082 – 03

DOI:10.13647/j.cnki.btgkj.2018.01.026

Realization of Modbus Communication Between S7 – 300 and Third Party Device

TU Zhi – hui, GAO Shi – chen

(*Center of Instrument of Inner Mongolia Steel Union Co. Ltd. of Baotou Steel (Group) Corp.*, *Baotou* 014010, *Nei Monggol*, *China*)

Abstract: Modbus protocol is a common language used in the electronic controller. Through this protocol, the controller can communicate with each other through the network and other devices. The paper describes the network communication between S7 – 300 PLC and third party device through the CP341 module, gives the specific communication protocol, technical solutions for the problem, and some examples of the implementation code.

Key words: S7 – 300 PLC; Modbus; CP341

污水处理的流程为通过粗格栅的原污水经过污水提升泵提升后,进入格栅或者砂滤器,之后进入沉砂池,经砂水分离的污水再进入初次沉淀池,其出水进入生物处理设备,生物处理后的出水进入二次沉淀池,沉淀后经过加氯加药等消毒后排放或者进入三级处理。二次沉淀池的污泥一部分回流至初次沉淀池或者生物处理设备,另一部分进入污泥浓缩池,之后进入污泥消化池,经过脱水和干燥设备后,污泥重复利用。

1 系统配置

(1) 该系统根据工艺由六套控制系统组成,分别为格栅间、水解酸化池、生化池、鼓风机房、加氯加药间及二沉池,每套控制系统带 2 块 CP341 模块,其中一块接仪表,用来采集仪表数据,包括流量、液位、分析仪等[1];另一块接变频器和电控器,进行采集和控制。每套系统都以西门子公司的 S7 315 – 2DP 作为主站,各种仪表及变频器为从站,实现 Modbus 网中的通讯及控制。

* **收稿日期**: 2017 – 12 – 08

作者简介: 涂智辉(1981 –),男,四川省达州市人,工程硕士,工程师,现从事自动控制系统设计与开发方面的工作。

(2) PLC 编程软件为 STEP7 V5.5,同时安装 PtP Param V5.1 + SP11 和 Modbus Master (RTU) V3.1 + SP6,安装之后,CP341 才能进行 Modbus 的主从通信组态和配置,计算机与 PLC 采用以太网通讯方式。上位机配置两台,一台做工程师站和操作员站,一台只做操作员站。

(3) 对于 CP341 模块,需要安装硬件狗才能使用,一块 CP341 模块需安装一个硬件狗,硬件狗的订货号为 6ES7 870 – 1AA01 – 0YA1。

2　通讯协议的配置

在硬件组态中选择 CP341 模块,组态好之后进行 Modbus 主站的配置[2]。具体配置如图 1 所示。

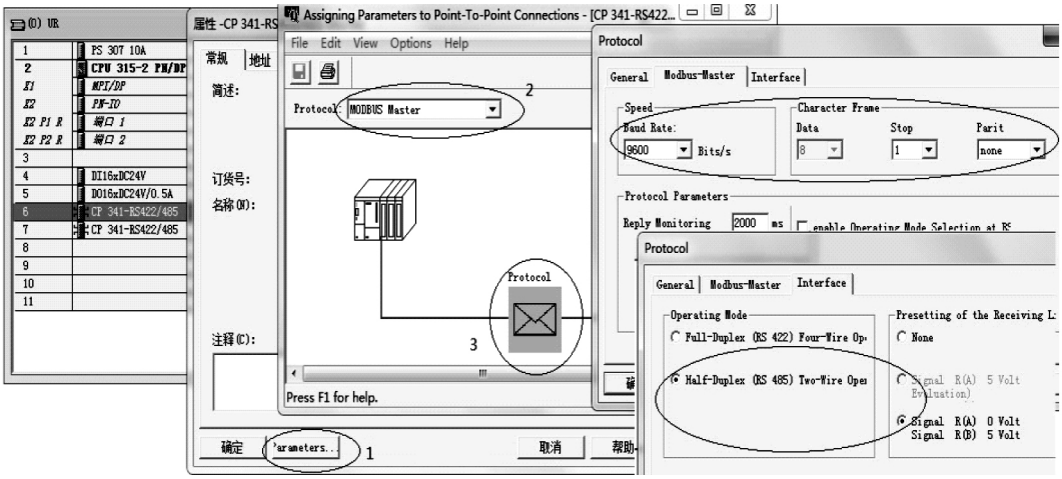


图 1　Modbus 参数配置

双击组态好的 CP341 模块,进入属性页面,点击参数“1”按钮,在 Protocol“2”中选择 Modbus Master,之后双击信封“3”,设置总线传输速率和帧字符结构,从站的设置必须和此处设置一致。此项目中传输速率为 9 600 bit/s,数据位 8 位,1 位停止位,无校验。

Modbus 参数配置完以后,进行电气接口设置,点击接口(Interface) 页,选中半双工 RS – 485,从站的接口电气标准应和主站一致。

3　通讯程序的设计

在硬件配置中,根据从站控制要求和数量,每个主站都安装了 2 块 CP341 模块,一块用于读取仪表数据,另一块用于控制现场设备。每块 CP341 模块上都连接多台第三方设备,为了编写程序的简洁,采用轮询的编程方式对第三方设备进行读写[3]。

对从站设备的通讯参数和站地址进行设置,连接好线缆,注意 A/B 的接线端子。读 Modbus 从站时,功能码为十六进制 03; 控制 Modbus 从站时,功能码为十六进制 10。本文以两个从站设备为例,建好发送和接收数据块 DB,发送数据块存放通讯参数用,而接收数据块则存放读取回来的数据。将读功能放在一个子程序如 FC1 中,定义一个数,每扫描一次加 1,若两个站则作两次比较,依此循环,数值为 1 时表示第一个站,此时将站址、功能码、起始地址和寄存器个数给到发送数据块中,并更改此站对应接收数据块(改 FB7 引脚的 DB_NO 与 DBB_NO); 当数值为 2 时表示第二个站,此时同样将站址、功能码、起始地址和寄存器个数给到发送数据块中,并更改此站对应接收数据块。此方法中调用 1 套 FB7 与 FB8 块,发送数据块 1 个,接收数据块 2 个。将写功能放在另一个子程序如 FC2 中,编程思想与读从站相同。但区别在于不仅要更改 FB7 的前引脚,同时要更改 FB8 前的引脚,即改变各从站对应的发送数据块。所以此 FC2 中调用 1 套 FB7 与 FB8 块,发送数据块 2 个,接收数据块 2 个。对于 FB7 与 FB8 块需要更改的引脚,使用中间变量代替,多台设备按照此方法类推即可。

新建功能 FC1,编写通讯程序,同时调用数据发送和接收功能块 FB8 和功能块 FB7。如图 2、图 3 所示。图 2 中,a 表示从站的地址,b 表示读功能码,c 表示读取从站 Modbus 的起始地址(0 对应 40001,

不同仪表起始地址不一样。)，d 表示读取从站数据的长度(整型)。在 FC2 中，a 表示从站的地址，b 表示写功能码，c 表示写入从站 Modbus 的起始地址(0 对应 40001，不同仪表起始地址不一样)，d 表示向从站写入数据的长度。

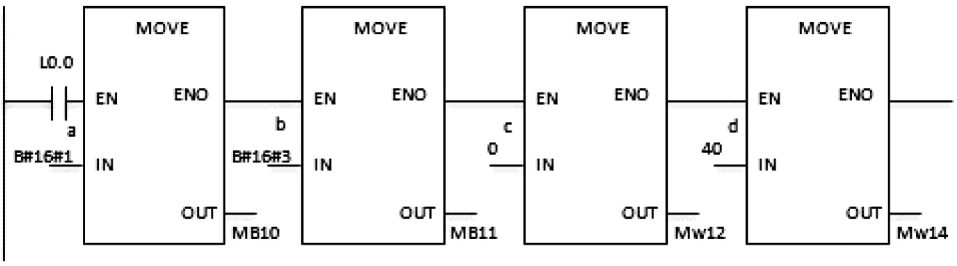


图 2 编写通讯参数

调用 FB8 时，建立相应的背景数据块，管脚参数设置为: SF，'S'为发送，此处必须为大写的'S'; LADDR，硬件组态中的起始逻辑地址; REQ，发送数据触发位，上升沿触发; DB_NO，发送参数数据块号; DBB_NO，发送数据的起始地址 0; LEN，发送数据的长度; R_TYP，'X'为扩展的数据块，此处必须为大写的'X'。

调用 FB7 时，建立相应的背景数据块，管脚参数设置为: LADDR，硬件组态中的起始逻辑地址; DB_NO，接收数据块号; DBB_NO，接收数据的起始地址。

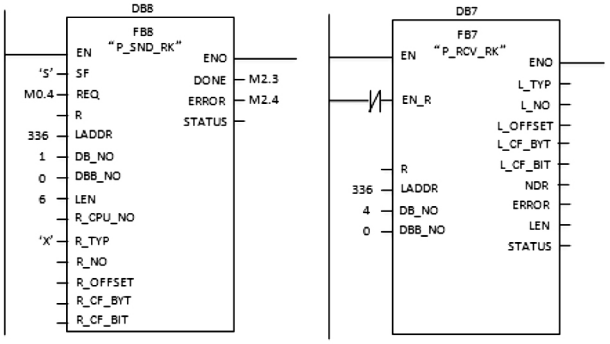


图 3 发送和接收功能块

4 结论

(1) 运用 Modbus 协议，可以方便地对多台第三方设备进行数据的读取和控制，减少线路的铺设，节约了成本。

(2) 因为连接设备的数量和距离，更新速率较慢，需要适当的调整波特率才能保证数据通讯的正常。

(3) 不同设备其 AB 管脚定义不同，要查看设备的说明书; 在联网调试设备之前，最好先用 Modbus 模拟软件对该设备进行单独通讯调试。

(4) FB8 中 REQ 触发时间根据连接设备多少而不同。

参 考 文 献

[1] 张华，赵文柱. 热工测量仪表(第 1 版) [M]. 北京: 化学工业出版社，2006.

[2] 廖常初. S7 - 300/400PLC 应用技术(第 2 版) [M]. 北京: 机械工业出版社，2011.

[3] 林德杰. 过程控制仪表及控制系统(第 2 版) [M]. 北京: 机械工业出版社，2004.