SIEMENS

基于 S7-1200CPU 集成 PN 接口 Modbus TCP 通讯快速入门

Modbus TCP Communication Base On S7-1200 CPU Intgrated PN Interface Getting Started

Getting-Started	Edition (2010 年 10 月)

摘　要　2010 年 4 月西门子全球技术资源库发布了用于 S7-1200 CPU 的集成 PN 接口通过 Modbus/TCP 与 PAC3200(CE-X22)进行数据交换的功能块库，本文主要介绍了 Modbus TCP 的通讯原理,并详细描述以 Modbus slave 软件为例模拟第三方设备如何使用该功能块库与 S7-1200 的集成 PN 接口进行 Modus TCP 通讯,希望通过本文档,能够给读者 S7-1200 CPU 集成 PN 口的 Modbus TCP 通讯入门指导

关键词　S7-1200,PAC3200,带集成 PN 口的 CPU,开放式以太网通讯，Modbus TCP,保持寄存器,输入寄存器,读写,服务器,客户端,地址映射,Modbus Slave

Key Words S7-1200,PAC3200,CPU With Intgrated PN Interface,Open IE Communication, Modbus TCP,Holding Register,Read/Write,Server,Clent, Adress Mapping,Modbus Slave

目　录

1 Modbus TCP 通讯概述

MODBUS/TCP 是简单的、中立厂商的用于管理和控制自动化设备的 MODBUS 系列通讯协议的派生产品,显而易见,它覆盖了使用 TCP/IP 协议的"Intranet"和"Internet"环境中 MODBUS 报文的用途。协议的最通用用途是为诸如 PLC's，I/O 模块，以及连接其它简单域总线或 I/O 模块的网关服务的.

1.1 通讯所使用的以太网参考模型

Modbus TCP 传输过程中使用了 TCP/IP 以太网参考模型的 5 层：

第一层：物理层，提供设备物理接口，与市售介质/网络适配器相兼容

第二层：数据链路层，格式化信号到源/目硬件址数据帧

第三层：网络层，实现带有 32 位 IP 址 IP 报文包

第四层：传输层，实现可靠性连接、传输、查错、重发、端口服务、传输调度

第五层：应用层，Modbus 协议报文.

1.2 Modbus TCP 数据帧

Modbus 数据在 TCP/IP 以太网上传输，支持 Ethernet II 和 802.3 两种帧格式,Modbus TCP 数据帧包含报文头、功能代码和数据 3 部分,MBAP 报文头(MBAP、Modbus Application Protocol、Modbus 应用协议)分 4 个域，共 7 个字节.

1.3 Modbus TCP 使用的通讯资源端口号

在 Moodbus 服务器中按缺省协议使用 Port 502 通信端口,在 Modus 客户器程序中设置任意通信端口，为避免与其他通讯协议的冲突一般建议 2000 开始可以使用.

1.4 Modbus TCP 使用的功能代码

按照使用的通途区分,共有 3 种类型分别为：

1) 公共功能代码：已定义好功能码，保证其唯一性，由 Modbus.org 认可；
2) 用户自定义功能代码有两组，分别为 65～72 和 100～110，无需认可，但不保证代码使用唯一性,如变为公共代码，需交 RFC 认可；
3) 保留功能代码，由某些公司使用某些传统设备代码，不可作为公共用途。

按照应用深浅，可分为 3 个类别

1) 类别 0,客户机/服务器最小可用子集：读多个保持寄存器(fc.3)；写多个保持寄存器(fc.16)。

2) 类别 1，可实现基本互易操作常用代码：读线圈(fc.1)；读开关量输入(fc.2)；读输入寄存器(fc.4)；写线圈(fc.5)；写单一寄存器(fc.6)。

3) 类别 2，用于人机界面、监控系统例行操作和数据传送功能：强制多个线圈(fc.15)；读通用寄存器(fc.20)；写通用寄存器(fc.21)；屏蔽写寄存器(fc.22)；读写寄存器(fc.23)

1.5 Modbus TCP 通讯应用举例

在读寄存器的过程中,以 Modbus TCP 请求报文为例,具体的数据传输过程如下:

1) Modbus TCP 客户端实况，用 Connect()命令建立目标设备 TCP 502 端口连接数据通信过程

2) 准备 Modbus 报文，包括 7 个字节 MBAP 内请求；

3) 使用 send()命令发送；

4) 同一连接等待应答；

5) 同 recv()读报文，完成一次数据交换过程

6) 当通信任务结束时，关闭 TCP 连接，使服务器可以为其他服务

2 SIMATIC S7-1200 Modbus TCP 通讯概述

2.1 概述

由于 S7-1200 是西门子推出时间不是很长的系列产品，因此用于其进行 Modbus/TCP 的功能块库在一定时间上并没有同步发布，在 S7-1200 系列中只有 CPU 上带有集成的 PN 口，因此只能通过该 PN 口进行 Modbus/TCP 通讯，在功能块库发布之前如果用户熟悉 Modbus/TCP 的协议规范和工作原理的话可以使用 S7-1200 的开放式通信指令库“TSEND_C”和“TRCV_C”编制简单通讯程序，本文在此不作详述，本文主要阐述如何使用通过基于官方发布的功能块库进行通讯

2010 年 4 月西门子官方发布了通过 Modbus TCP 与 S7-1200(CE-X22)的 PN 口进行数据通讯的功能块库(如下图 1)，随后 2010 年 7 月又对该功能块库进行一次修正(最初版本为 V1.0，之后库升级为 V1.2)，通过该功能块库可以将 SENTRON PAC3200 的相关数据(如电流，电压，IP 地址等)传送到 S7-1200 的 CPU 中,该功能块库可以从网上免费下载，无需单独购买,可以参见官方网上的 FAQ 连接：

http://support.automation.siemens.com/CN/view/zh/40614428

Program blocks

Table 1-1

Library	Element	Content
PAC_ModbusTCP_Client	PAC_FB [v1.0]	Function block FB500
	PAC_Tags	PLC tags
	PAC_TxRx_Buffer	Global data block DB502 (optional send and receive block)
	PAC_Watch Tables	Monitoring tables for send / receive buffer

图 1:通讯图示

2.2 CE-X22 功能块库的硬件和软件要求使用说明

2.2.1 所支持的 CPU 模块及通讯伙伴要求

支持的 CPU :所有的 S7-1200 系列 CPU(包括 CPU1211C、1212C、1214C)，无固件版本限制

通讯伙伴：理论上只要支持 Modbus/TCP 的设备均可以通讯，但当使用 PAC3200 时要求固件版本必须为 V2.0.6 以上

2.2.2 功能块库使用说明

1)该功能块库虽然是针对 SENTRON PAC3200 推出的，但是同样适用于任何支持 Modbus /TCP 通讯的设备，包括 PAC4200,WinCC V7,S7-300/400 及第三方设备，只不过是功能块

库中针对 PAC3200 具体定义了相关的 PLC 变量、DB 块监控表等，如下图 2 所示

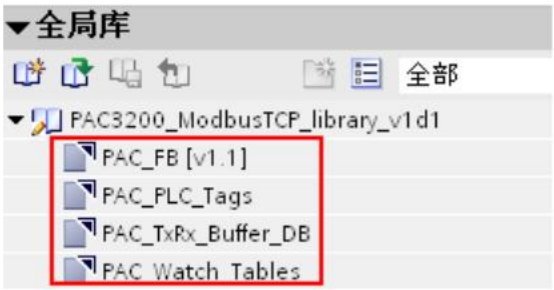

图 2:功能块库

2)当与非 PAC3200 的第三方设备通讯时只要调用 PAC_FB(FB500),填写相关参数即可

3) 该功能块库(PAC_FB FB500)只能实现 S7-1200 作为 Modbus/TCP 客户端(Client)，通讯对方作为服务器(Server),使用上还是有一定的限制，不过相信官方将会对块库改善后能够做为服务器进行通讯

4)该功能块库(PAC_FB FB500)目前只能实现功能码 FC03(读多个保持寄存器)和 FC16(写多个保持寄存器),目前功能上来说还比较简单，还不能实现离散量的读写,对于离散量的读写必须合并到一个寄存器中来完成(即将 16 个 Bit 转换成一个 Word),相信未来功能块库会进一步完善功能码

2.2.3 通讯资源端口使用限制

通常情况下对于服务器端推荐使用 Modbus/TCP 缺省的端口号 Port 502,对于客户端使用除 502 以外的端口，对于 S7-1200 来说注意不要与其别的协议通讯端口有冲突即可，在该功能块库中系统会自动使用端口，无需用户单独进行设置。

3 配置 CPU1212C 作为 Client 进行 Modbus TCP 通讯

下面以 CPU1212C(6ES7212-1BD30-0XB0)及 Modbus Slave 软件(模拟服务器端，软件的使用及安装程序见附件 2)为例,详细介绍如何将 CPU1212C 配置为 Client,Modsbus Slave 为 Server 进行 Modbus TCP 通讯.

3.1 例子中使用的硬件设备及软件

本例中所用的硬件设备如下表：

名称	数量	订货号
SIMATIC S7-1200, PM1207, 2,5A	1	6EP1332-1SH71
SIMATIC S7-1200 CPU1212C	1	6ES7211-1AD30-0XB0
网线	若干	
编程器兼软件测试机	1	

所用到软件如下表：

名称	订货号
SIMATIC STEP7 BASIC V10.5 补丁包 Service Pack SP2	U6ES7822-0AA00-0YA0
Modbus Slave V4.3	V4.3.0(免授权版)

3.2 通过 SIMATIC STEP7 BASIC V10.5 软件组态

3.2.1 硬件组态及功能块库导入

在 STEP7 Basic 中创建一个 S7-1200 的项目，本例中项目名为 Modbus_TCP_1200HA，插入一个 S7-1200 CPU，从硬件目录中插入 1212 CPU AC/DC/Rly 并对其属性组态，如下图 3 所示

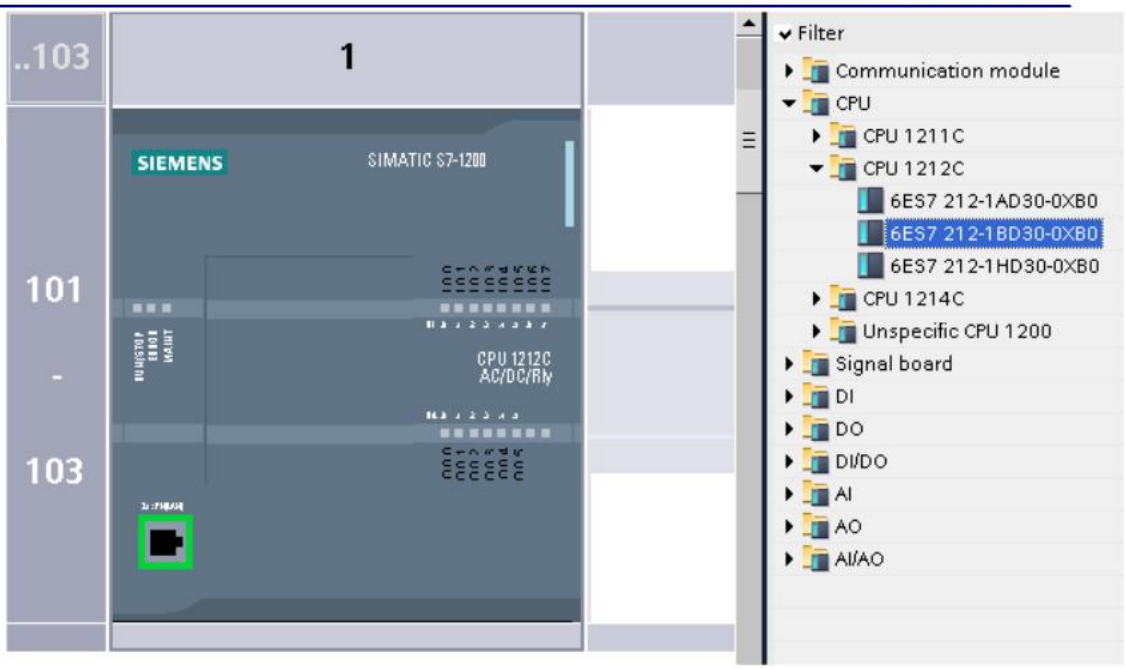

图 3:插入 CPU

设置控制器集成口以太网 IP 地址 为 192.168.1.50，由于 MDOBUS TCP 是基于 TCP 通信，因此 IP 地址是必要的，如下图 4 所示:

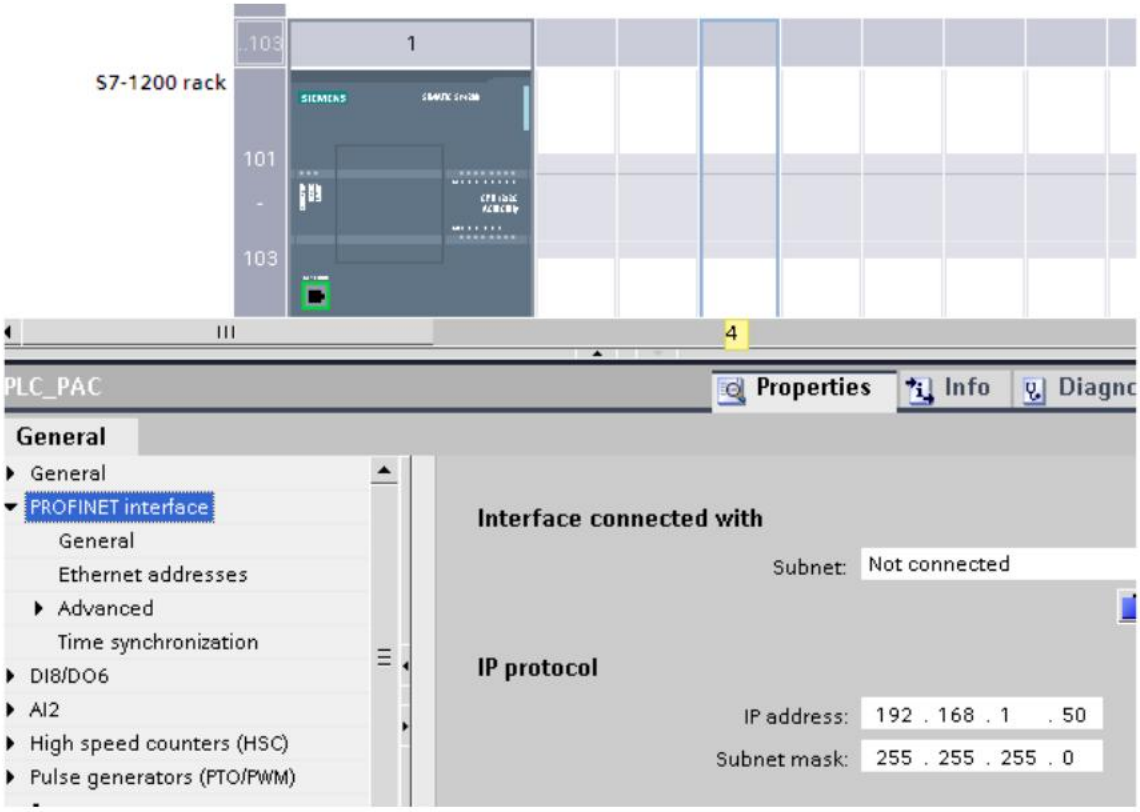

图 4: 设置 CPU IP 地址参数

将从网上下载的的库文件解压缩(或参考本文档中的附件 2)，并在 STEP7 Basic 中导入 MODBUS TCP 库，如下图 5 所示：

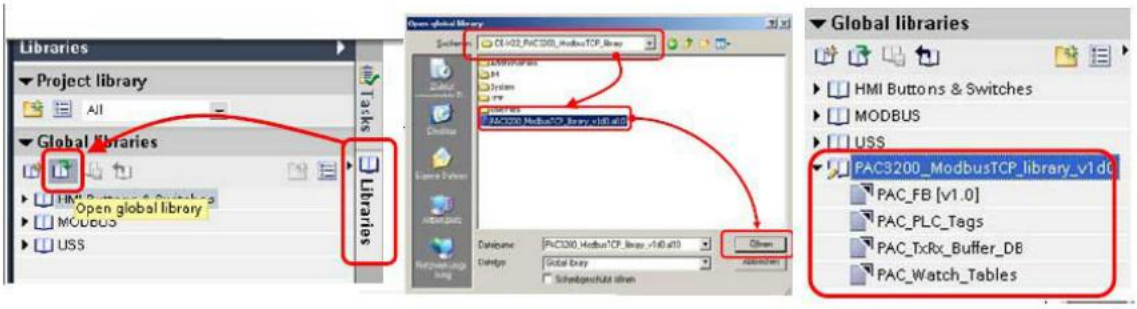

图5: 导入MODBUS TCP功能块库

3.2.2 功能块 FB500 使用说明

打开 OB1,调用通信功能块“PAC”FB500 并编写参数，如下图 6 所示:

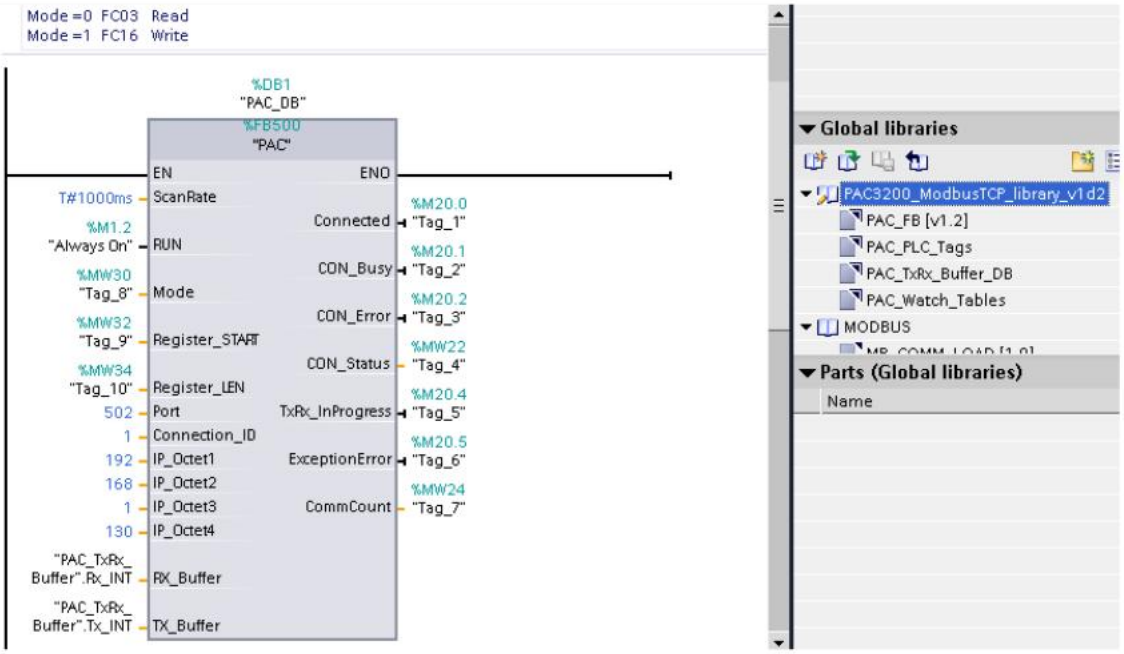

图6:在OB1中“PAC”FB500

功能块“PAC”FB500 的参数布局如下图 7 所示：

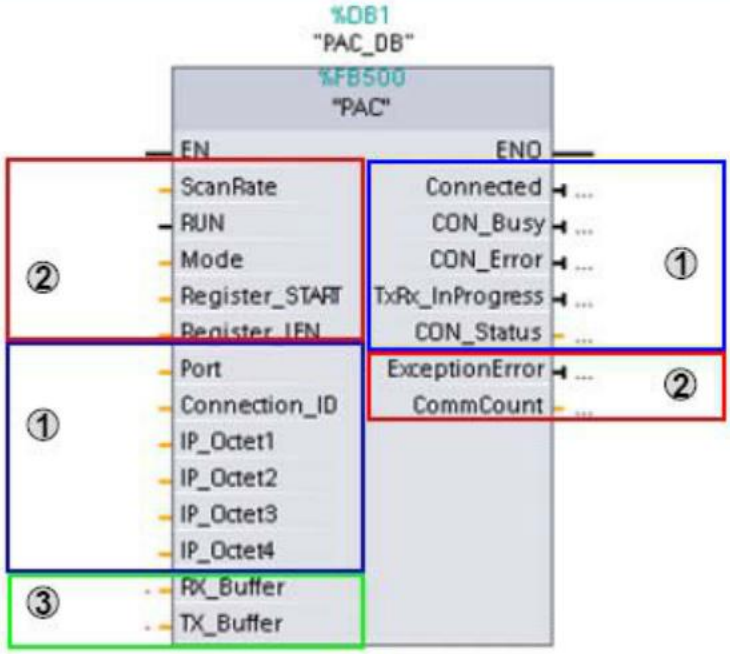

图 7:FB500 功能块参数布局

FB500 功能块共分成 3 个参数组，具体含义如下(顺序号与图 7 相对应)：

①：**连接参数和状态**

②：**Modbus 参数和状态**

③：**发送和接收缓冲区**

功能块“PAC”FB500 的各管脚参数含义如下图 8 所示：

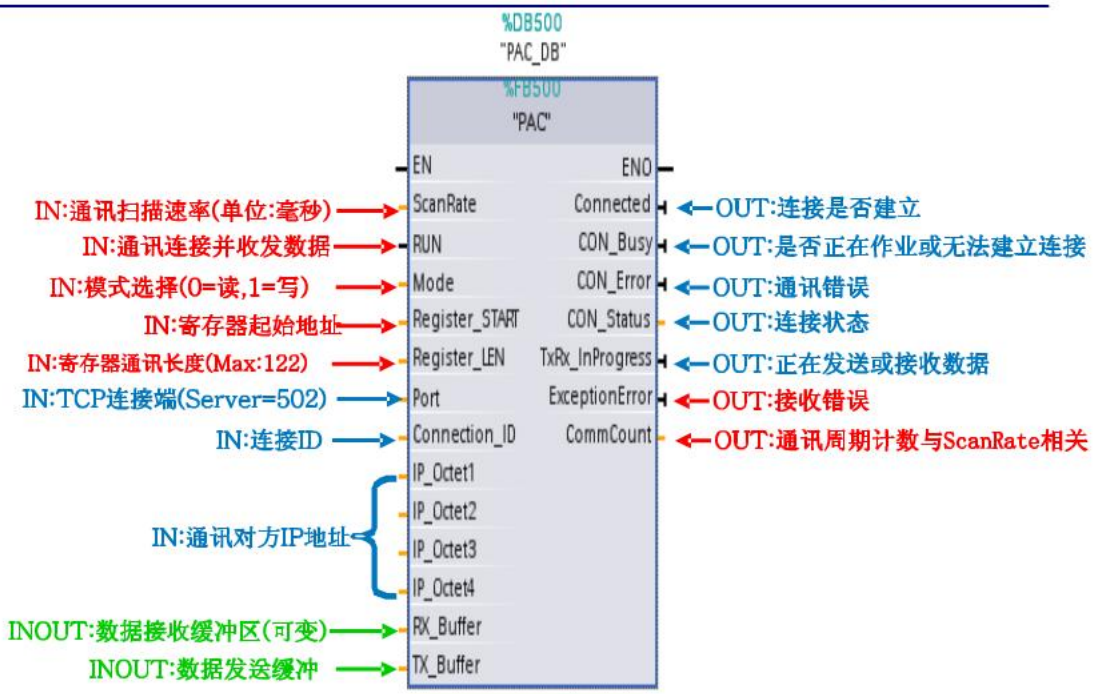

图 8：FB500 功能块参数含义

在本例中实际设置的参数如下表所示：

输入参数	输入的值	注释
ScanRate	1000	标准为 1S　ms 为单位
RUN	1	通信连接
Mode	MW30	0->FC 03 Read 1->FC 16 Write
Register_START	MW32	寄存区的起始地址
Register_LEN	MW34	寄存区的起始长度 最大 125 registers
Port	502	MODBUS TCP Server 端口
Connection_ID	1	连接 ID,每个连接 ID 唯一
IP_Octet1 to IP_Octet4	192.168.1.130	MODBUS TCP Server IP
RX buffer	DB502.RX_INT	数据通信接收区
TX buffer	DB502.TX_INT	数据通信发送区

至此 S7-1200 的组态和参数设置完毕，下载项目程序到 CPU1212C 中进行通讯测试.

3.3 服务器端 Modbus Slave 软件设置

打开 Modbus Slave 软件，在 Connection-connection 中打开连接属性对话框，连接接口选择“Modbus TCP/IP”，TCP/IP Server Port 为本地服务器的端口 502，并可以勾选“Ignore Unit ID”选项，如下图 9 所示：

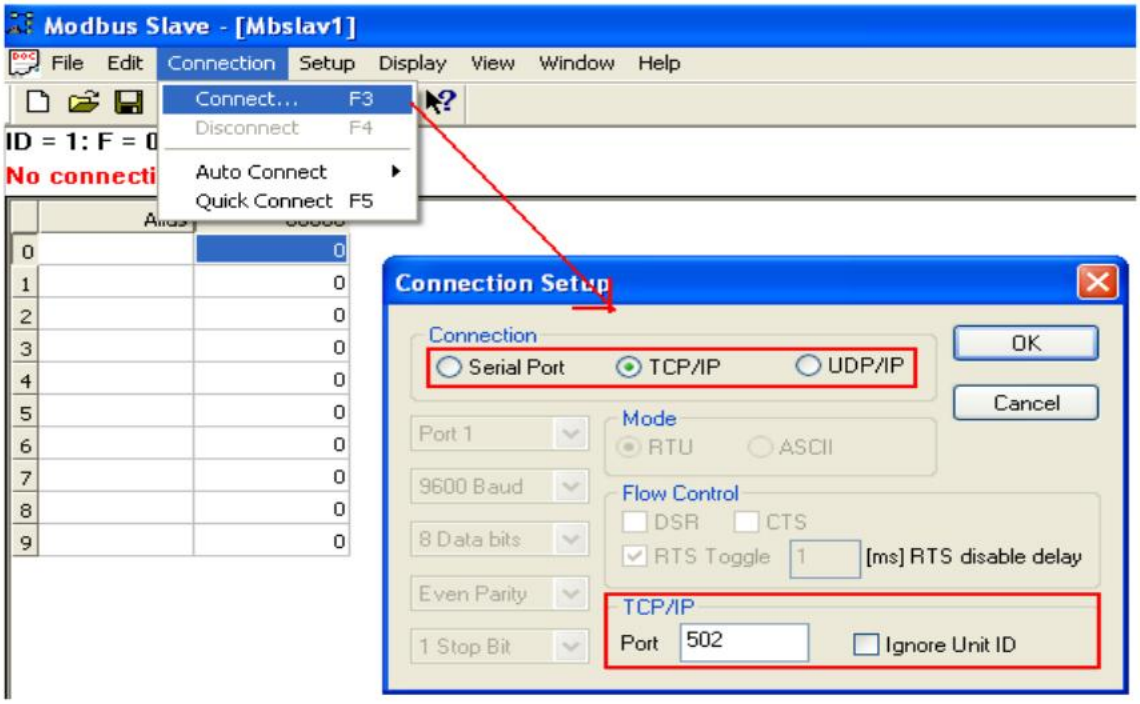

图 9:Modbus Slave 连接设置

（说明-“Ignore Unit ID”及“Any Adress”选项的含义如下：

Ignore Unit ID-在一些厂商的 PLC 的程序或网关中可能会用到 Unit ID 以指定处理类型）

在 Modbus Slave 的“Set up->Slave Definition“中可以设置功能码、起始地址、长度、显示的列数、数据显示格式及响应时间等，并可勾选“Hide Alias Columns”、“PLC Adresses(Base1)”、“Insert CRC/LRC error”、“Skip response”、“Return Exception 06,Busy”选项，如下图所示：

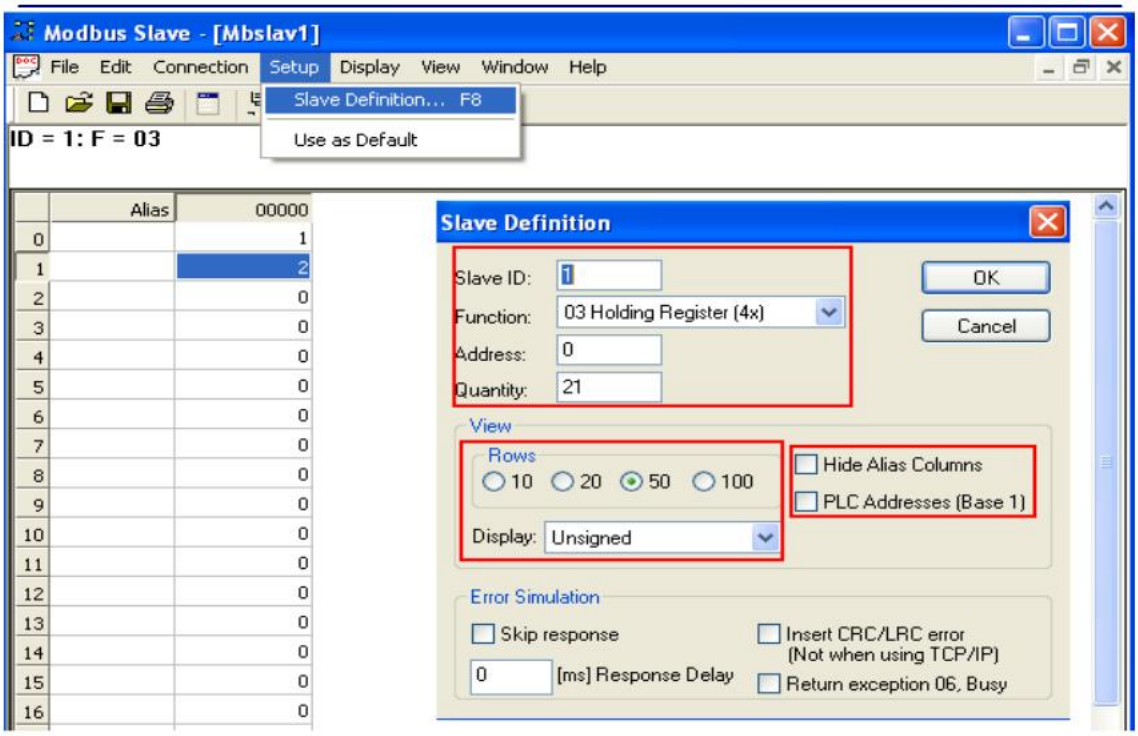

图 10:Modbus Slave 数据定义

(说明-各勾选选项的含义如下：

Hide Alias Columns –隐藏注释选项

PLC Addresses(Base1) **-** 选择寄存器地址是基于 PLC 地址编排(1..65535)还是基于协议编排(0-65535)

Insert CRC/LRC error - 选择是否进行 CRC/LRC 错误校验

Skip response – 选择是否忽略报文丢失响应

Return Exception 06,Busy – 选择是否返回 Slave 忙信号)

Modsbus Slave 支持读写线圈(fc.1/5)、读开关量输入(fc.2)、读输入寄存器(fc.4)、读写多个保持寄存器(fc.3/16)等多个功能码，下面将对 FC03/16(读写保持寄存器)功能码进行测试

3.4 通讯测试

3.4.1 FC03 功能码(读取服务器端保存寄存器)测试

设置客户机和服务器端在功能码，起始地址和长度等参数想对应，将 FB500 的参数“mode”MW30 设置为 0(读模式)，在 S7-1200 端中使能“Run”参数后，可以看见通讯已经建

立，Modbus Slave 服务器端的寄存区 40001-40005 被客户端 S7-1200 读到地址区 RX_INT，如下图 9 所示：

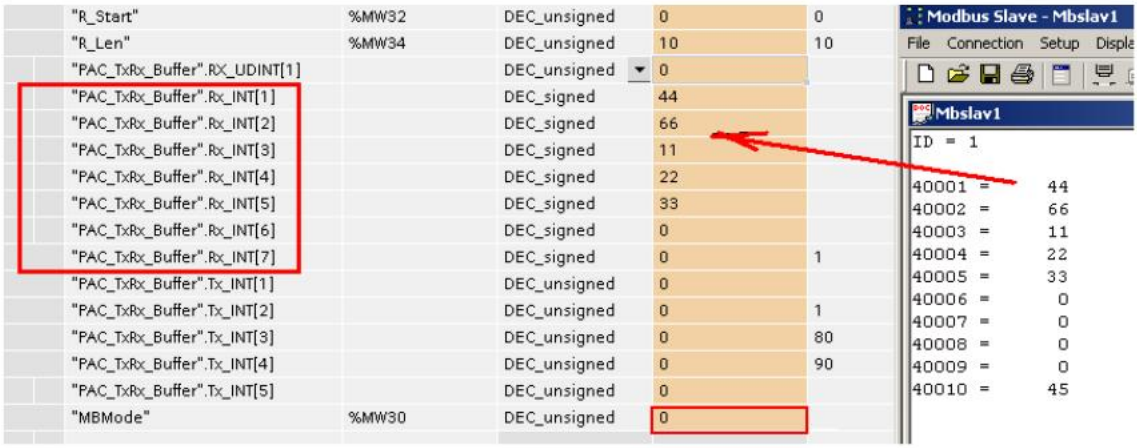

图11:FC03功能码客户端读取服务器端数据

3.4.2 FC16 功能码(向服务器端写保存寄存器)测试

同样设置客户机和服务器端在功能码，起始地址和长度等参数想对应，将FB500的参数“mode”MW30设置为1(写模式)，在S7-1200端中使能“Run”参数后，可以看见通讯已经建立，S7-1200写数据区TX_INT 到MODBUS 从站的寄存区40001-40005，如下图12所示：

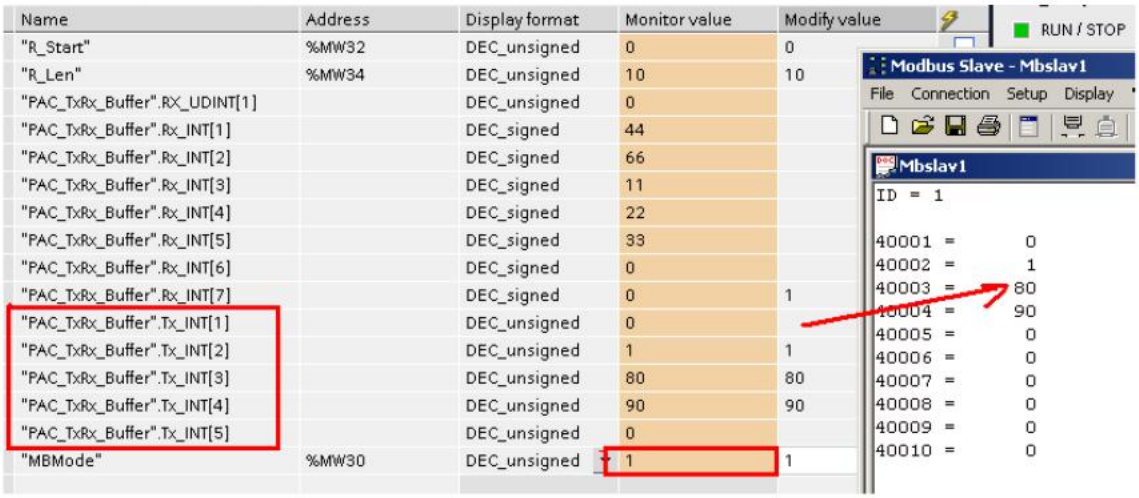

图12:FC16功能码客户端向服务器写数据

4 通讯注意事项

由于是通过 PC 测试软件模拟第三方设备与 CPU1212C 进行 Modbus TCP 通讯，因此在实际的第三方设备与 S7-1200 进行通讯时需要注意以下几点：

1) 关于通讯长度，根据 Modbus/TCP 本身的协议规范限制，寄存器最多不超过 125 个，而该功能块库也做了一定限制，对于读模式最多不超过 125 个寄存器。对于写模式不超过 123 个寄存器，另外通讯伙伴端可能也会对长度做一定的限制，比如 PAC3200 读写模式下均不超过 122 个寄存器，因此要综合双方来决定最终的长度.

2) 对于功能块 FB500 的发送区参数“Tx-Buffer“中 DB 区的格式已固定，只能为“Array [1 .. x] of uint“,而接收区参数“Rx-Buffer“相对比较灵活，可以定义为“Array [1 .. x] of uint“、 “Array [1 .. x] of word“, “Array [1 .. x] of real“等格式

3) 如果连接多个MODBUS Server从站，需要建立多个连接，Connection_ID号要不同且不能超出S7-1200 通信能力 8 个连接.

更多关于 Modbus TCP 的相关信息请参考 FAQ :

“如何从SIMATIC建立OPEN MODBUS /TCP 通信，以及在哪可以找到更多信息? ”

http://support.automation.siemens.com//CN/view/zh/22660304

如果您对该文档有任何建议，请将您的宝贵建议提交至下载中心留言板。

该文档的文档编号：A0500

附录一推荐网址

通信/网络
西门子（中国）有限公司
工业自动化与驱动技术集团 客户服务与支持中心
网站首页：www.4008104288.com.cn
通信/网络 **下载中心**：
http://www.ad.siemens.com.cn/download/DocList.aspx?TypeId=0&CatFirst=12
通信/网络 **全球技术资源**：
http://support.automation.siemens.com/CN/view/zh/10805868/140000
“找答案”Net版区：
http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1041

自动化与驱动集团技术支持与服务热线

电话：+86 400-810-4288
传真：+86 10 64719991
邮箱：4008104288.cn@siemens.com
网址：www.4008104288.com.c

注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系，并不完全相关。应用示例不表示客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使用这些应用示例时，应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责任。我们保留随时修改这些应用示例的权利，恕不另行通知。如果这些应用示例与其它西门子出版物(例如，目录)给出的建议不同，则以其它文档的内容为准。

声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免，我们不能保证完全一致。我们会经常对手册中的数据进行检查，并在后续的版本中进行必要的更正。欢迎您提出宝贵意见。