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.

MODBUS/TCP 使 MODBUS_RTU 协议运行于以太网，MODBUS TCP 使用 TCP/IP 和以太网在站点间传送 MODBUS 报文，MODBUS TCP 结合了以太网物理网络和网络标准 TCP/IP 以及以 MODBUS 作为应用协议标准的数据表示方法。MODBUS TCP 通信报文被封装于以太网 TCP/IP 数据包中。与传统的串口方式，MODBUS TCP 插入一个标准的 MODBUS 报文到 TCP 报文中，不再带有数据校验和地址

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，如图 1 所示:

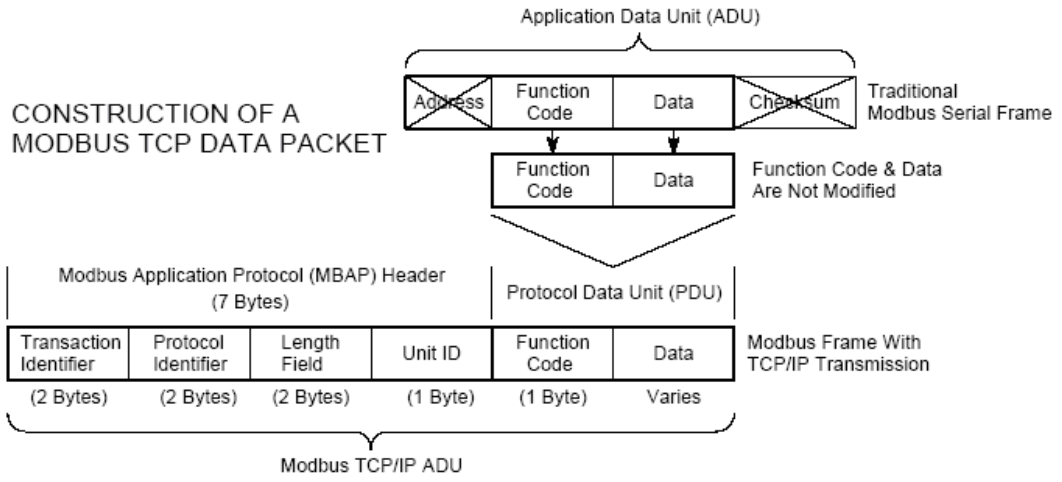

图 1：MODBUS TCP 报文

由于使用以太网 TCP/IP 数据链路层的校验机制而保证了数据的完整性，MODBUS TCP 报文中不再带有数据校验”CHECKSUM”，原有报文中的“ADDRESS”也被“UNIT ID”替代而加在 MODBUS 应用协议报文头中

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 S7-300/400 系统 Modbus/TCP 通讯概述

2.1 S7-300/400 系统 Modbus/TCP 通讯产品概述

通过 SIMATIC S7 和第三方设备的建立 MODBUS/TCP 通信时按照产品使用分单站和冗余系统，对于单站系统，又分为通过以太网通讯模块 CP 和 CPU 的集成 PN 口两种情况

1) 通过以太网通讯模块 CP343-1 或 CP443-1:

在 S7 控制器通过外部 CP343-1 或 CP443-1 和第三方设备间建立 Modbus/TCP 连接时需要软件选项包"ModbusTCP CP"， 订货号为 2XV9450-1MB00 ,单授权(仅对一个 CPU 有效)，最新的版本为 V4.1,支持功能代码 1、2、3、4、5、6、15 和 16，功能块库及订货号如下图 2 所示:

Product	Identification number	From version
OPEN MODBUS / TCP	2XV9 450-1MB00	4.1
FB 108 “MODBUSCP”		1.1 / 2.0
FB 106 “MB_CPCLI”		1.1 / 2.0
FB 107 “MB_CPSRV”		1.1 / 2.0

图 2:软件选项包”ModbusTCP CP V4.1”

2) 通过 CPU 集成的 PN 接口 :

在 S7 控制器通过 CPU 集成 PN 接口和第三方设备间建立 Modbus/TCP 连接时需要产品软件选项包"ModbusTCP PN ",订货号为 2XV9450-1MB02,最新版本 V2.4, 单授权(仅对一个 CPU 有效),支持功能代码 1、2、3、4、5、6、15 和 16, 对 S7-300 和 S7-400 集成 PN 接口的 CPU 都适用, 功能块库及订货号如下图 3 所示:

Product	Identification number	From version
OPEN MODBUS/TCP	2XV9 450-1MB02	2.4
FB 102 “MODBUSPN”		3.4
FB 103 “TCP_COMM”		3.0
FB 104 “MOD_CLI“		1.5
FB 105 “MOD_SERV“		1.3

图 3:软件选项包”ModbusTCP PN-CPU V2.4”

3) 通过 S7-400H 冗余系统的 CP443-1：

通过 S7-400H 冗余系统建立第三方设备的 MODBUS/TCP 通信包含两个版本，对应两个订货号，两个版本为升级关系，详细情况如下：

Open Modbus/TCP 冗余系统 V1 版本需要产品软件选项包” ModbusTCP Red V1”, 订货为”2XV9450-1MB01”,单授权(仅对一个冗余 CPU 对有效)，软件选项包的块库如下图 4 所示:

Product	Identification number	From version
OPEN MODBUS / TCP Redundant	2XV9 450-1MB01	1.1
FB 1733 “MODB4H		1.1
FB 1734 “MODB4”		1.3

图 4: 软件选项” ModbusTCP Red V1”

Open Modbus/TCP 冗余系统 V2 版本需要产品软件选项包” ModbusTCP Red V2”, 订货为”2XV9450-1MB11”,单授权(仅对一个冗余 CPU 对有效)，软件选项包的块库如下图 5 所示:

Product	Identification number	From version
OPEN MODBUS/TCP Redundant	2XV9 450-1MB11	2.0
FB 909 „MB_REDCL“		2.0
FB 908 „MB_CPCLI“		2.1
FB 907 „MB_REDSV“		2.0
FB 906 „MB_CPSRV“		2.0

图 5: 软件选项” ModbusTCP Red V2”

2.2 ”ModbusTCP PN-CPU V2.4”软件选项包使用概述

2.2.1 ” ModbusTCP PN-CPU V2.4”块库使用说明

1) 该功能块库可以用于 S7-300/400 单站系统或 ET200 带 CPU 的接口模块通过 CPU 的集成 PN 口进行 ModbusTCP 通讯

2) 由于需要在 SIMATIC 站与其他通讯伙伴之间建立 TCP 连接用于 Modbus 通讯，而对于 CPU 的集成 PN 口来说使通过 Open IE(开放式以太网通讯)的方式来建立 TCP 连接， 因此需要调用 SIMATIC S7 标准功能块，包括 FB63(TSEND)、FB64(TRCV)、FB65(TCON)、FB66(TDISCON)完成 TCP 的连接管理和数据通讯

需要注意的是对于用于 Modbus TCP 的功能块 FB63/64/65/66 有一定的版本要求如下：

FB63(TSEND)　　V2.1 或更高
FB64(TRCV)　　V2.2 或更高
FB65(TCON)　　V2.3 或更高
FB66(TDISCON)　V2.1 或更高

3) 通过 S7-CPU 的 PROFINET 接口 进行 Modbus TCP 通信时，需要使用通信块 FB65 "TCON"、FB66 "TDISCON"、FB63 "TSEND" 和 FB64 "TRCV"，要进行 Modbus TCP 通信，必须在数据块中为每个连接指定相应的参数，因此通过 Modbus TCP Wizard 向导软件，可以非常便捷地指定各连接的参数，通过 Modbus TCP Wizard ，只需指定各连接类型所需的相应参数，之后，该向导将包含有连接描述的所有参数的 DB 导 入到 STEP 7 项目中，向导的安装界面如下图 6 所示，另外通过软件包安装集成到 Step7 后也有参数 DB，具体可以根据实际的项目情况来进行调整，详细地内容将在下面的配置章节中详细描述

图 6: Modbus TCP Wizard 起始界面

关于 Modbus TCP Wizard 的相关信息及下载可以参考以下连接:
http://support.automation.siemens.com/CN/view/zh/31535566

2.2.2 ” ModbusTCP PN-CPU V2.4”选项包硬件和软件需求

所支持硬件和软件需求如下图 7 和图 8 所示:

ModbusTCP PN 2XV9 450-1MB02	
CPU315-2 PN/DP	
6ES7 315-2EH13-0AB0	V2.6.7
6ES7 315-2EG10-0AB0	V2.3.4
CPU317-2 PN/DP	
6ES7317-2EJ10-0AB0	V2.3.4
6ES7317-2EK13-0AB0	V2.6.7
CPU319-3 PN/DP	
6ES7319-3EL00-0AB0	V2.7.2
CPU414-3 PN/DP	
6ES7414-3EM05-0AB0	V5.2
CPU416-3 PN/DP	
6ES7416-3ER05-0AB0	V5.2
CPU417-4 PN/DP	
6ES7417-4XL04-0AB0	V4.1
IM151-8 PN/DP	
6ES7151-8AB00-0AB	V2.7.1
WinAC RTX 2008	
6ES7671-0RC06-0YA0	

图 7:” ModbusTCP PN-CPU V2.4”软件包硬件需求

Software requirements
· SIMATIC STEP 7 version 5.4 SP4 or higher for the PN PLC versions of the MODBUS blocks

图 8:” ModbusTCP PN-CPU V2.4”软件包软件需求

2.3 “ModbusTCP PN-CPU V2.4”软件选项包与 step7 集成概况

下面章节将介绍如何使用软件选项包” ModbusTCP PN-CPU V2.4 "的功能块库配置 S7-300/400 单站系统通过 CPU 的集成 PN 口与第三方模拟软件进行 Modbus/TCP 进行通讯的详细步骤，实际上当将软件选项包安装完集成到 Step7 时可以在 Step7 安装文件的相应目录中找到块库、例程、英文手册，如下图 9-11 所示，在实际的项目调试过程中由于例子程序的各项功能比较完善，因此可以直接使用例子程序根据项目的实际情况修改相应的参数即可，可以节省大量的参数设置时间，以下主要描述了使用软件选项包” ModbusTCP PN-CPU V2.4"配置 S7-300/400 站基于 CPU 集成 PN 口进行 Modbus TCP 通讯的详细配置和编程步骤.

- the library in \Program Files\Siemens\Step7\S7libs,
- the sample project in \Program Files\Siemens\Step7\Examples,
- the manual in \Program Files\Siemens\Step7\S7manual\S7Comm,
- the software registration form in \Program Files\Siemens\Step7\S7libs\Modbus_PN_CPU.

图 9: 块库、例程、英文手册和软件注册的文件夹位置

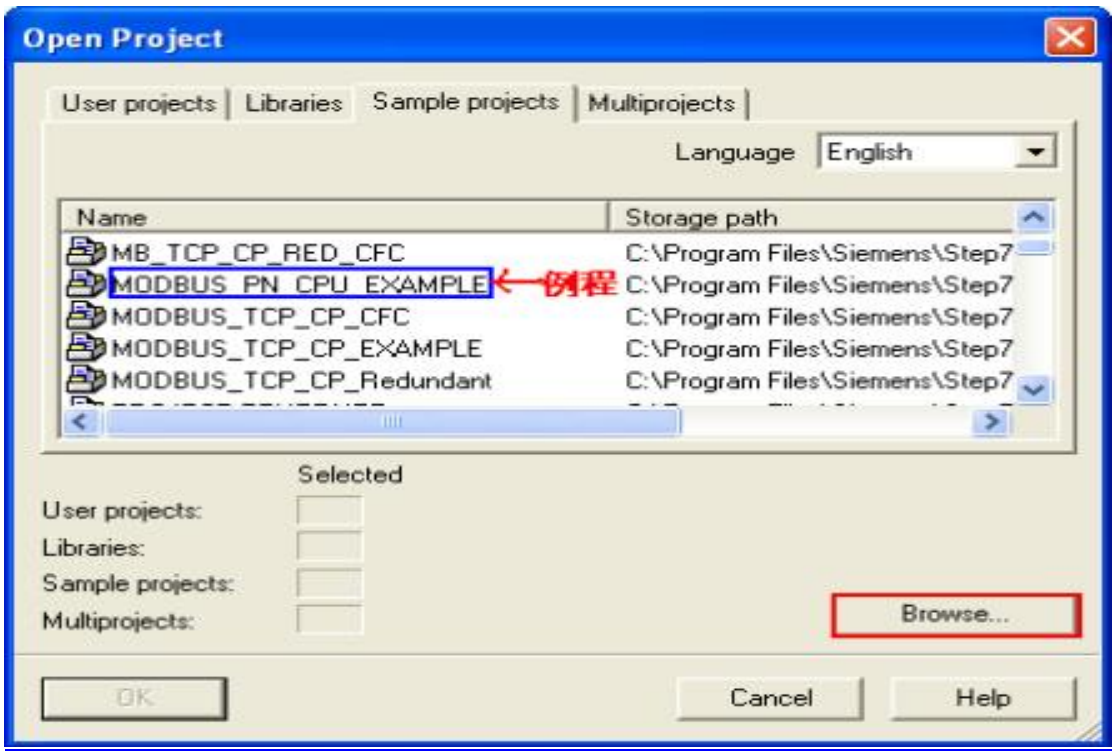

图 10:例程(注:当找不到例程时可以通过"Browse.."按钮来进行查找)

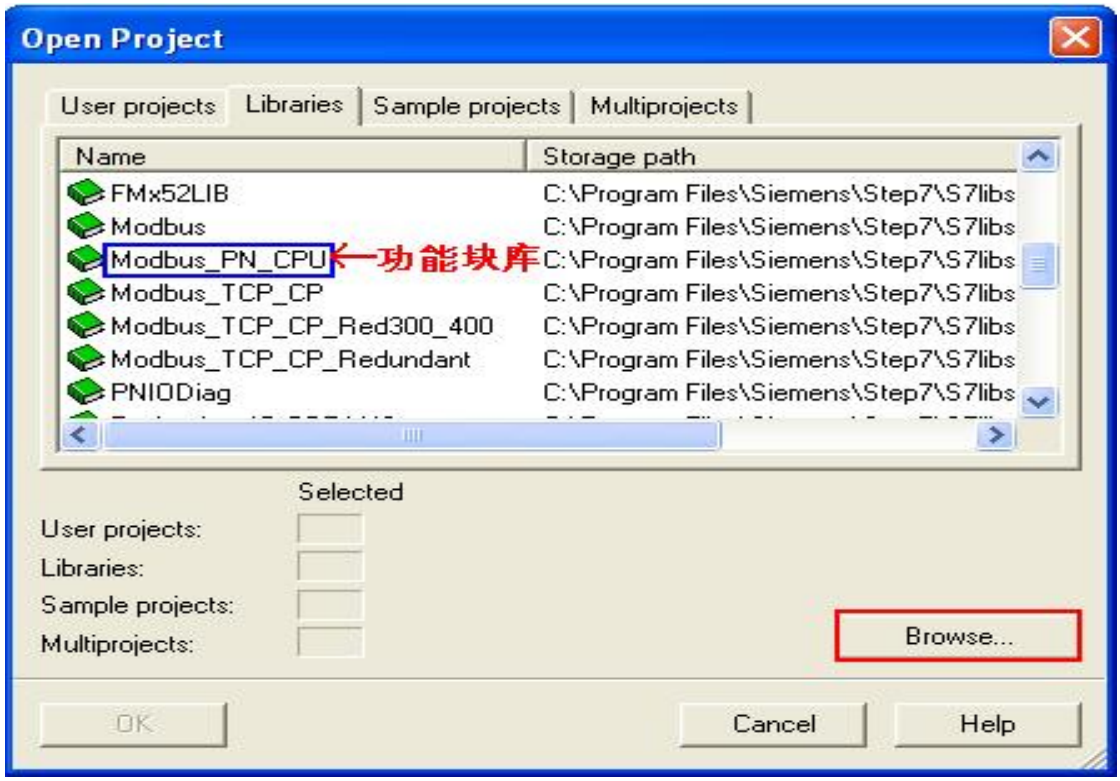

图 11:功能块库(注:当找不到块库时可以通过"Browse.."按钮来进行查找)

3 配置 S7-400 单站系统通过 CPU 集成 PN 口作为 Server 进行 Modbus TCP 通讯

下面以 S7-400 单站系统及 Modscan32 软件为例,详细介绍如何将 S7-400 单站系统通过 CPU 集成 PN 口配置为 Server,Modscan32 为 Client 进行 Modbus TCP 通讯，下图 12 为服务器功能块库的程序结构及各功能块完成的功能:

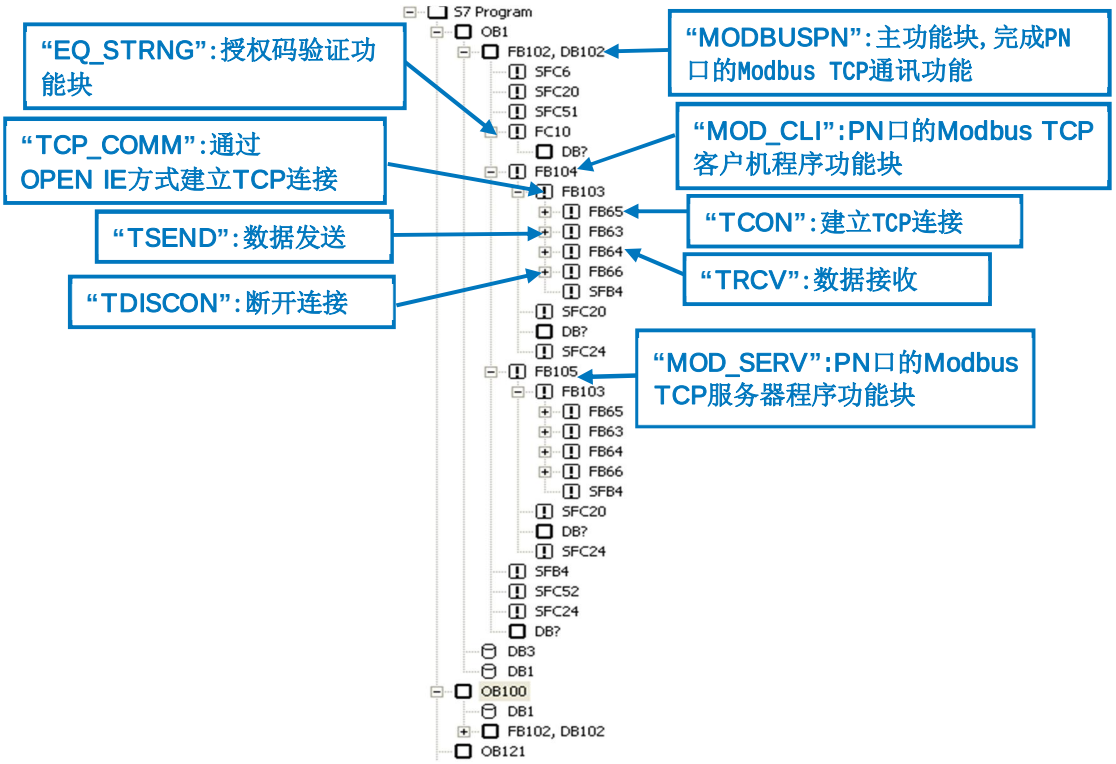

图 12:服务器功能块库程序结构

注：Modscan32 软件可以从网上免费下载得到，本例中使用的版本为 V7.0 版，由于各版本的功能不尽相同，因此需要注意版本问题

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：

表 1:服务器硬件清单

名称	数量	订货号
S7-400 电源模块 PS 407 10A	1	6ES7407-0KA01-0AA0
S7-400 CPU414-3PN/DP	1	6ES7414-3EM05-0AB0(V5.2)
S7-400 机架	1	6ES7400-1JA00-0AA0
网线	若干	
STEP 7 5.5 组态编程软件 英文版	1	6ES7810-4CC08-0YA5
“ ModbusTCP PN-CPU V2.4” 软件选项包		2XV9450-1MB02
Modscan32 V7.0		

所用到软件如下表：

表 2:服务器软件清单

名称	订货号
笔记本电脑	

3.2 S7-

400 系统及 Modscan32 软件组态

打开 Step7 软件，新建一个工程项目文件，命名为“M_TCP_CPU_V2-4(Server)”, 在项目下插入一个 S7-400 站，如下图 13 所示：

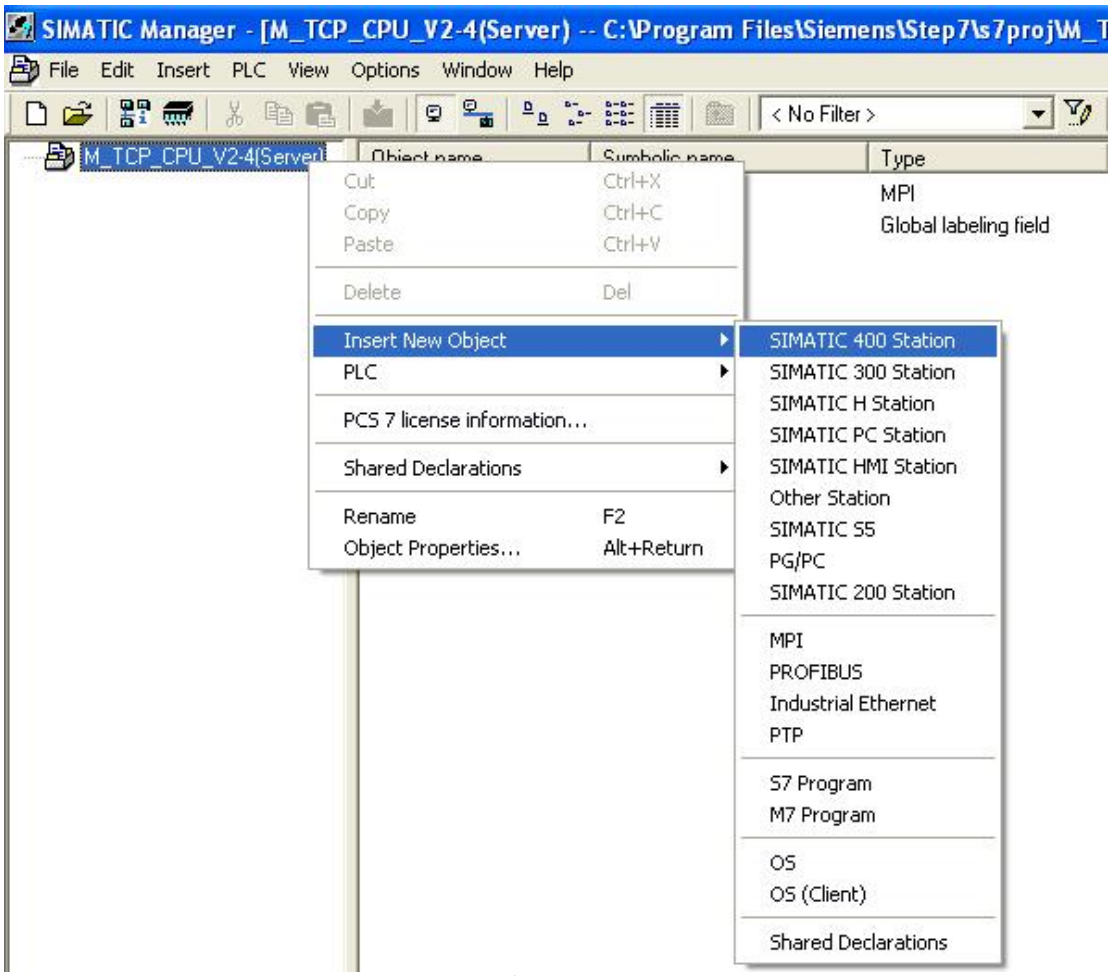

图 13:新建 S7-400 Station

双击插入的 SIMATIC 400 Station 的“Hardware”，打开硬件组态，在硬件组态界面下分别插入机架，电源 PS407、CPU414-3PN/DP,本例中将 CPU 的 PN 口 IP 地址设为 **192.70.44.10，**如下图 14 所示：

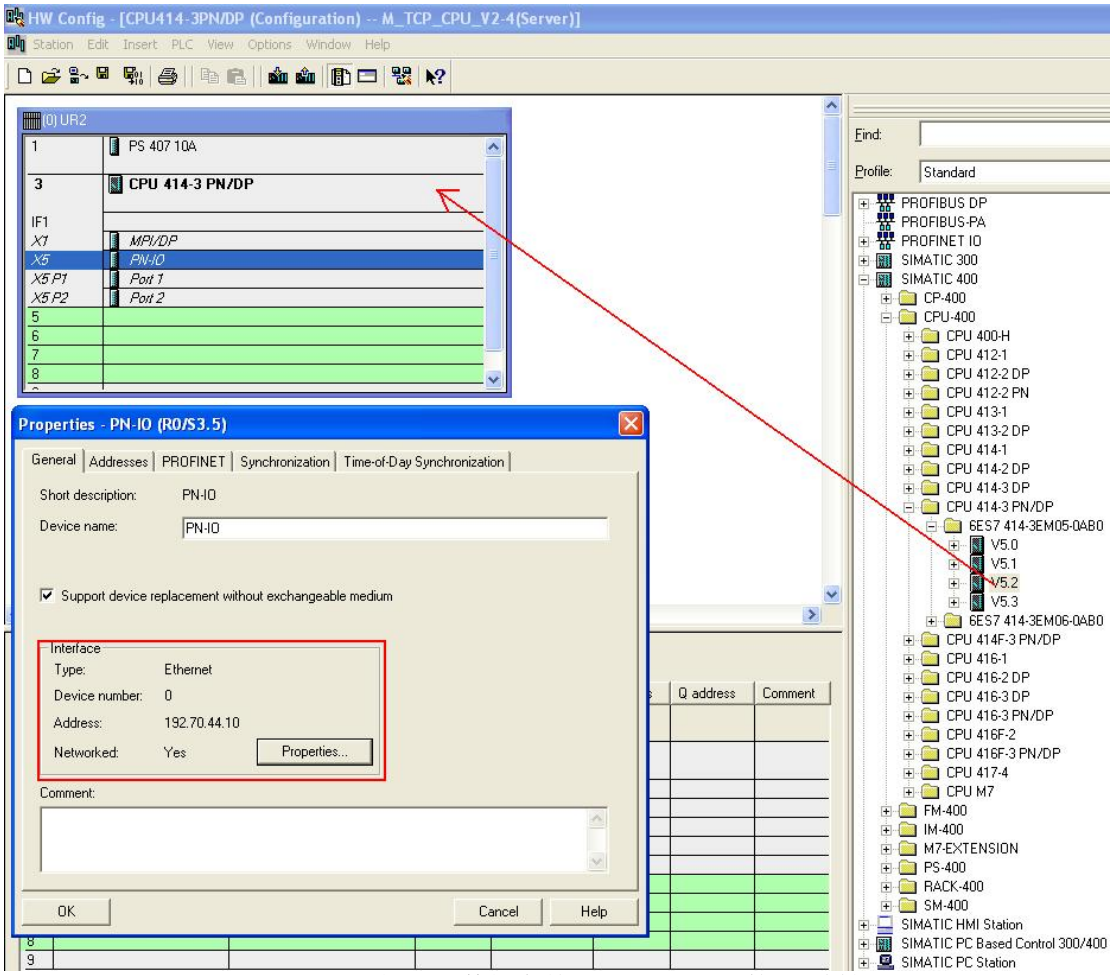

图 14:硬件组态并设置 CP443-1 的 IP 地址

由于需要在 SIMATIC 站与其他通讯伙伴之间建立 TCP 连接用于 Modbus 通讯，而对于 CPU 的集成 PN 口来说须通过 Open IE(开放式以太网通讯)的方式来建立 TCP 连接， 通过 S7-CPU 的 PROFINET 接口 进行 Modbus TCP 通信时，需要使用通信块 FB65 "TCON"、FB66 "TDISCON"、FB63 "TSEND" 和 FB64 "TRCV"，要进行 Modbus TCP 通信，必须在数据块中为每个连接指定相应的参数，相应得参数在程序中主要由 DB2“MODBUS_PARAM“来完成初始化，其中各参数的含义如下图 15、16 所示:

Addre:	Name	Type	Initial value
0.0		STRUCT	
+0.0	OUCW_1	STRUCT	
+0.0	block_length	WORD	W#16#40
+2.0	id	WORD	W#16#1
+4.0	connection_type	BYTE	B#16#11
+5.0	active_est	BOOL	TRUE
+6.0	local_device_id	BYTE	B#16#5
+7.0	local_tsap_id_len	BYTE	B#16#0
+8.0	rem_subnet_id_len	BYTE	B#16#0
+9.0	rem_staddr_len	BYTE	B#16#4
+10.0	rem_tsap_id_len	BYTE	B#16#2
+11.0	next_staddr_len	BYTE	B#16#0
+12.0	local_tsap_id	ARRAY[1..16]	B#16#0, B#16#0, B#16#0,
*1.0		BYTE	
+28.0	rem_subnet_id	ARRAY[1..6]	B#16#0, B#16#0, B#16#0,
*1.0		BYTE	
+34.0	rem_staddr	ARRAY[1..6]	B#16#A, B#16#0, B#16#0,
*1.0		BYTE	
+40.0	rem_tsap_id	ARRAY[1..16]	B#16#1, B#16#F6, B#16#0
*1.0		BYTE	
+56.0	next_staddr	ARRAY[1..6]	B#16#0, B#16#0, B#16#0,
*1.0		BYTE	
+62.0	spare	WORD	W#16#0

通过OPEN IE方式创建的TCP连接的相关参数设置

图 15:DB2“MODBUS_PARAM“的 TCP 连接参数设置部分

关于 DB2“MODBUS_PARAM“的 TCP 连接参数含义如下表 3 所示:

类型	参数	含义
OPEN IE 通讯参数	block_length	固定值W#16#40
	Id	连接ID,用于FB63/64/65/66
	connection_type	取决于CPU类型，用于FB65(TCON) TCP(兼容模式): CPU315、317<= FWV2.3 W#16#01 TCP:CPU315,317>= FW V2.4、IM151-8PN/DP、 CPU319、CPU414与CPU416 W#16#11
	active_est	主动或被动连接: S7作Client时为主动 TRUE S7作Server时为被动 FALSE
	local_device_id	取决于CPU类型: IM151-8PN/DP B#16#1 CPU315、317 B#16#2 CPU319 B#16#3 CPU414、416 B#16#5
	local_tsap_id_len	local_device_id的长度: 主动连接时 W#16#0 被动连接时 W#16#2

	rem_subnet_id_len	未使用
	rem_staddr_len	参数rem_staddr的长度： 未具体定义连接 B#16#0 有具体连接 B#16#4
	rem_tsap_id_len	rem_tsap_id的长度： 主动连接时 W#16#2 被动连接时 W#16#0
	next_staddr_len	通讯接口类型选择: 通过外部CP模块： 非0的其它值 通过CPU的集成PN 口： W#16#0
	local_tsap_id	本地连接TSAP号,与参数connection_type有关： 1)connection_type= B#16#01时 local_tsap_id[1] 本地连接端口号的低字节[16进制] local_tsap_id[2] 本地连接端口号的高字节[16进制] local_tsap_id[3-16] B#16#00 2)connection_type= B#16#11时 local_tsap_id[1] 本地连接端口号的高字节[16进制] local_tsap_id[2] 本地连接端口号的低字节[16进制] local_tsap_id[3-16] B#16#00
	rem_subnet_id	未使用
	rem_staddr	通信伙伴的IP地址，与参数connection_type有关，以192.168.0.1为例： 1)connection_type= B#16#01时 rem_staddr[1]= B#16#01(1), rem_staddr[2]= B#16#00(0) rem_staddr[3]= B#16#A8(168) rem_staddr[4]= B#16#C0(192) rem_staddr[5-6]=B#16#00(为IPV6预留) 2)connection_type= B#16#11时 rem_staddr[1]= B#16#C0(192) rem_staddr[2]= B#16#A8(168) rem_staddr[3]= B#16#00(0) rem_staddr[4]= B#16#01(1) rem_staddr[5-6]=B#16#00(为IPV6预留)
	rem_tsap_id	远程连接TSAP号,与参数connection_type有关： 1)connection_type= B#16#01时 local_tsap_id[1] 本地连接端口号的低字节[16进制] local_tsap_id[2] 本地连接端口号的高字节[16进制] local_tsap_id[3-16] B#16#00 2)connection_type= B#16#11时 local_tsap_id[1] 本地连接端口号的高字节[16进制] local_tsap_id[2] 本地连接端口号的低字节[16进制] local_tsap_id[3-16] B#16#00
	next_staddr	CP的机架号和槽号，当使用CPU的PN口时为 B#16#00

表 3: DB2“MODBUS_PARAM“的 TCP 连接参数含义

+64.0	server_client	BOOL	FALSE
+64.1	single_write	BOOL	FALSE
+64.2	connect_at_startup	BOOL	FALSE
+65.0	reserved	BYTE	B#16#0
+66.0	data_type_1	BYTE	B#16#3
+68.0	db_1	WORD	W#16#B
+70.0	start_1	WORD	W#16#1
+72.0	end_1	WORD	W#16#1F4
+74.0	data_type_2	BYTE	B#16#3
+76.0	db_2	WORD	W#16#C
+78.0	start_2	WORD	W#16#2D0
+80.0	end_2	WORD	W#16#384
+82.0	data_type_3	BYTE	B#16#4
+84.0	db_3	WORD	W#16#D
+86.0	start_3	WORD	W#16#2D0
+88.0	end_3	WORD	W#16#3E8
+90.0	data_type_4	BYTE	B#16#1
+92.0	db_4	WORD	W#16#E
+94.0	start_4	WORD	W#16#280
+96.0	end_4	WORD	W#16#4E2
+98.0	data_type_5	BYTE	B#16#2
+100.0	db_5	WORD	W#16#F
+102.0	start_5	WORD	W#16#6A4
+104.0	end_5	WORD	W#16#8FC
+106.0	data_type_6	BYTE	B#16#1
+108.0	db_6	WORD	W#16#10
+110.0	start_6	WORD	W#16#6A4
+112.0	end_6	WORD	W#16#8FC
+114.0	data_type_7	BYTE	B#16#0
+116.0	db_7	WORD	W#16#7
+118.0	start_7	WORD	W#16#0
+120.0	end_7	WORD	W#16#64
+122.0	data_type_8	BYTE	B#16#0
+124.0	db_8	WORD	W#16#8
+126.0	start_8	WORD	W#16#0
+128.0	end_8	WORD	W#16#64
+130.0	internal_send_buffe	ARRAY[1..260	B#16#0
*1.0		BYTE	
+390.0	internal_recv_buffe	ARRAY[1..260	B#16#0

Identifier	Data type	Size
0	Area not used	
1	Coils	Bit
2	Inputs	Bit
3	Holding Register	Word
4	Input Register	Word

图 16:DB2“MODBUS_PARAM“的 Modbus 参数设置部分

打开 Modscan32 软件，在“Connection-connection”中打开连接属性对话框，连接接口选择“Remote TCP/IP Server”，IP Adress 分别填入 CPU 的 IP 地址 192.70.44.10,Server Port 为远程服务器的端口 502，在协议的选择对话框中可以定义传输模式、通讯超时响应时间，报文发送间隔及允许写多个保持寄存器等，这里分别保持缺省设置即可，如下图 17 所示：

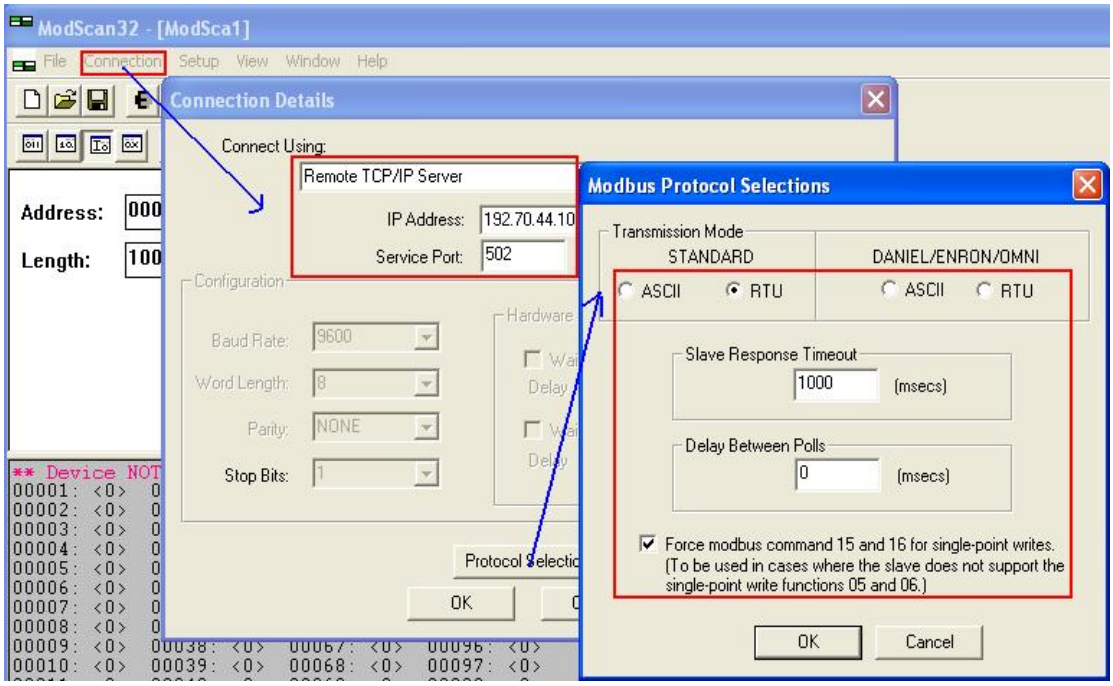

图 17:对应 TCP 通讯的 Modscan32 连接窗口

3.3 通讯测试

由于“ ModbusTCP PN-CPU V2.4”选项包支持功能码 FC1，2，3，4，5，6，15，16，不同的功能码测试过程中类似，因此下面以 FC03(读写保持寄存器)为例来说明通讯测试的整个过程，对于其他功能码的测试将不再重复描述，对于 Modbus 的数据类型可以参考下表 4:

基本表	对象类型	访问类型	注释
离散量输入	单个位	只读	I/O系统可提供这种类型数据
线圈	单个位	读写	通过应用程序可改变这种类型数据
输入寄存器	16位字	只读	I/O系统可提供这种类型数据
保持寄存器	16位字	读写	通过应用程序可改变这种类型数据

表 4:Modbus 数据类型

由于服务器主功能块 FB102“MODBUSPN”的参数需要初始化，因此分别在 OB100 及 OB1 中调用 FB102，在 OB100 中调用 FB102 完成相关参数的初始化，FB102 的管脚分布如下图 18 所示:

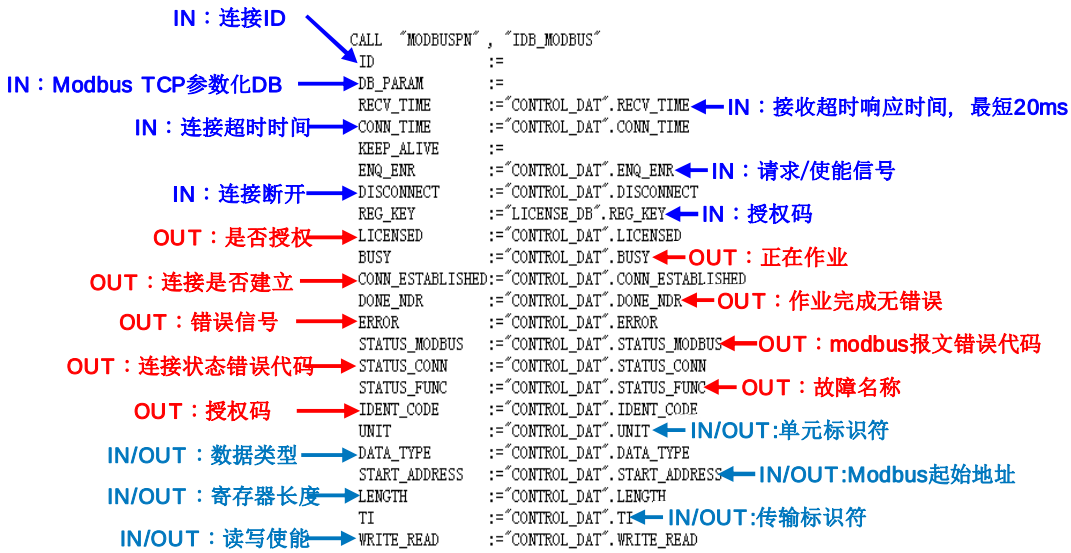

图 18: FB102“MODBUSPN”的管脚参数定义

注意:在图 18 中已经填写的参数不需要初始化,在 OB1 调用赋值；而未填写的参数需要初始化在 OB100 中调用完成

下载硬件组态及程序到 CPU 中，将 DB2“MODBUS_PARAM“的参数“server_client“使能为 1，在 Modscan32 的“Set up->Data Definition“中设置数据扫描周期、寄存器连接类型、起始地址、长度等，如下图 19 所示：

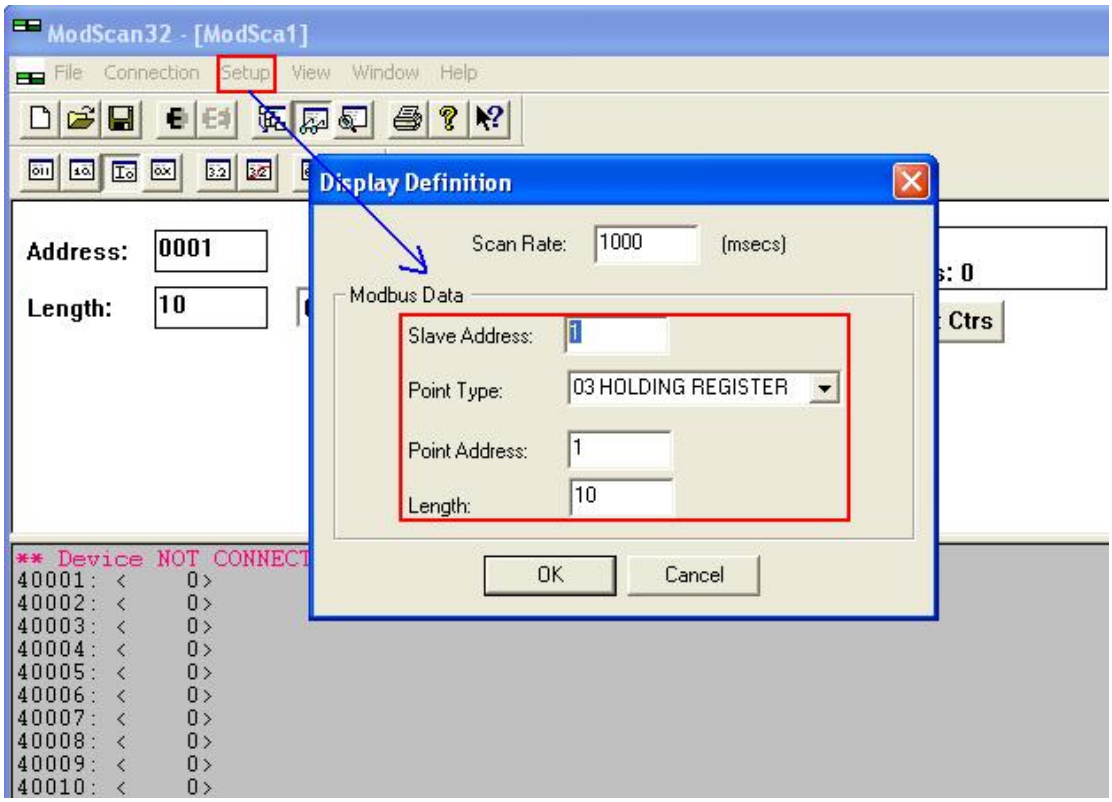

图 19:Modscan32 中 Modbus 数据参数定义

由于 Modbus 的内部地址编排时基于数据链路层和应用层有一定的映射关系，因此 Modbus 的地址与 SIMATIC 中的 DB 块的地址时按照一定的地址映射关系来相对应，这样造成了 DB 块中有一定的地址偏移量,在本例中假设数据区的定义如下图 20 所示，其 DB 偏移量、Modbus 物理编址、应用层编址如下图 21 所示：

data_type_1 *db_1* *start_1* *end_1*	B#16#3 W#16#B W#16#1 W#16#1F4	Holding Register DB 11 Start address: 1 End address: 500
data_type_2 *db _2* *start _2* *end _2*	B#16#3 W#16#C W#16#2D0 W#16#384	Holding Register DB 12 Start address: 720 End address: 900
data_type_3 *db _3* *start _3* *end _3*	B#16#4 W#16#D W#16#2D0 W#16#3E8	Input Register DB 13 Start address: 720 End address: 900
data_type_4 *db _4* *start _4* *end _4*	B#16#0 0 0 0	Not used 0 0 0
data_type_5 *db _5* *start _5* *end _5*	B#16#1 W#16#E W#16#280 W#16#4E2	Coils DB 14 Start address: 640 End address: 1250
data_type_6 *db _6* *start _6* *end _6*	B#16#2 W#16#F W#16#6A4 W#16#8FC	Inputs DB 15 Start address:1700 End address: 2300
data_type_7 *db _7* *start _7* *end _7*	B#16#1 W#16#10 W#16#6A4 W#16#8FC	Coils DB 16 Start address: 1700 End address: 2300
data_type_8 *db _8* *start _8* *end _8*	B#16#0 0 0 0	Not used 0 0 0

图 20:本例中的数据区定义

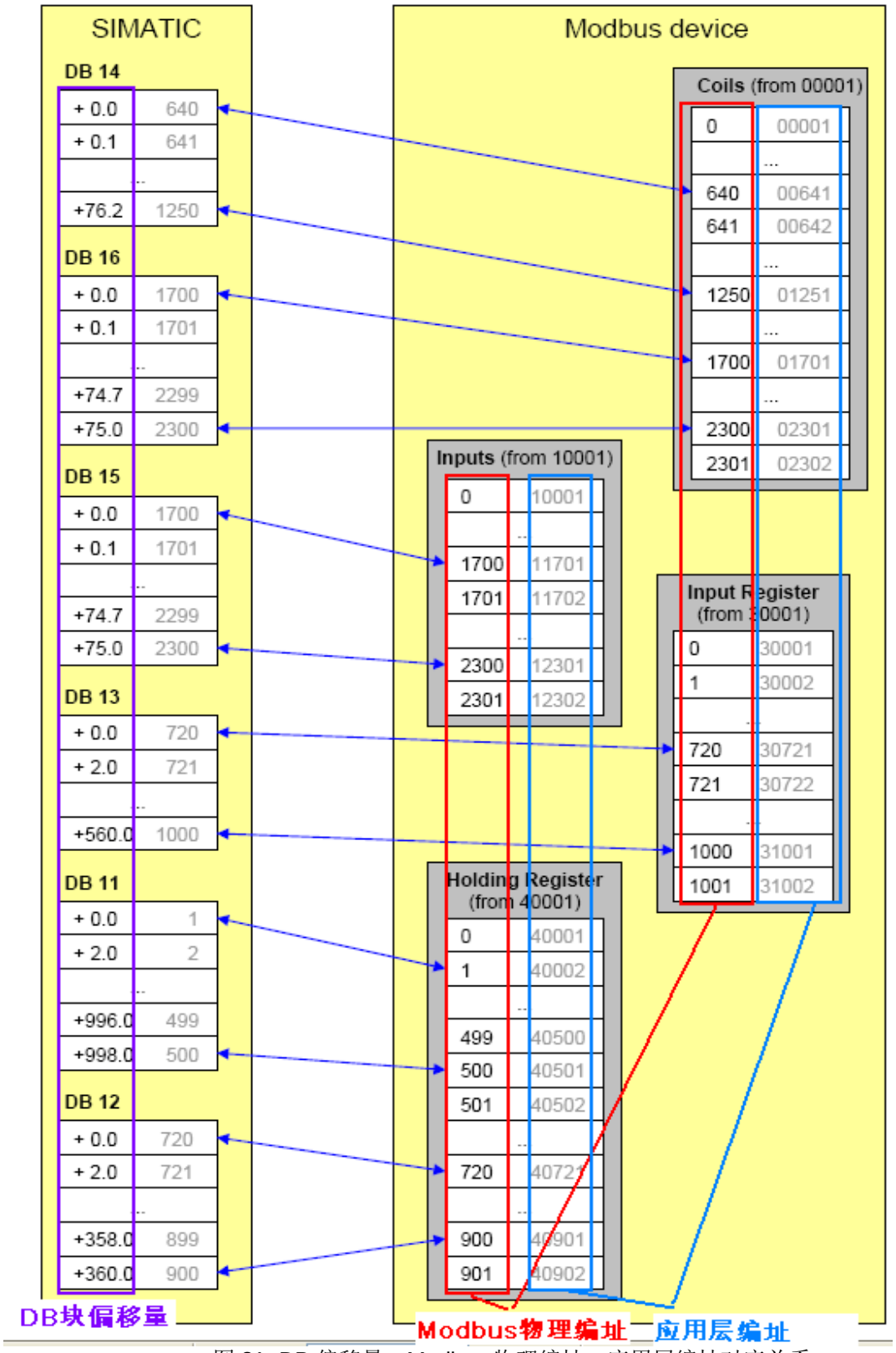

图 21: DB 偏移量、Modbus 物理编址、应用层编址对应关系

在 Step7 的项目程序中新建一个变量监控表，插入需要监控的参数和数据区变量，可以看到 Modscan32 软件与 CPU414-3PN/DP 的数据通讯已经建立起来了，双方可以进行正常的保持寄存器数据读写操作，如下图 22 所示：

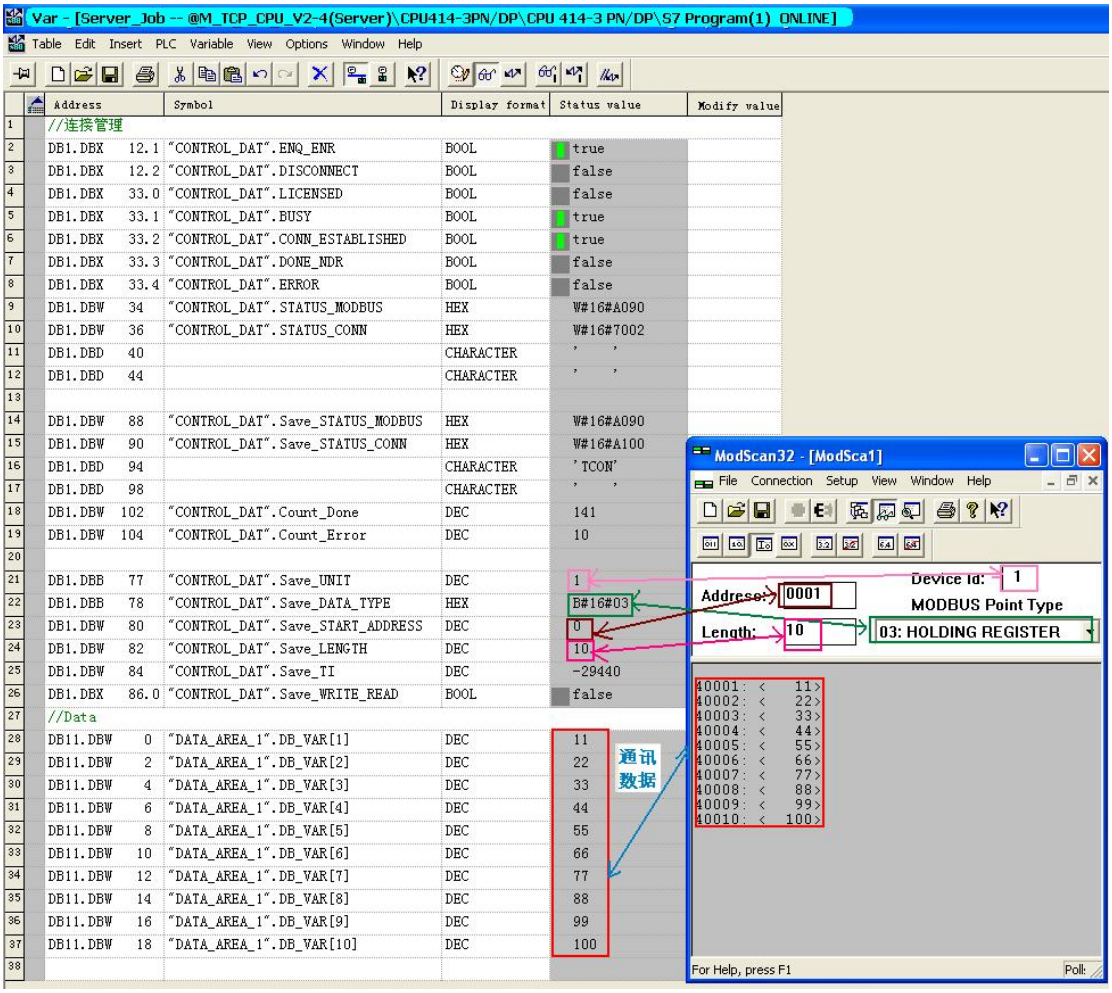

图 22:通讯连接建立

4 配置 S7-400 单站系统通过 CPU 集成 PN 口作为 Client 进行 Modbus TCP 通讯

下面以 S7-400 单站系统及 Modbus Slave 软件为例,详细介绍如何将 S7-400 单站系统 CPU 的集成 PN 口配置为 Client,Modbus Slave 为 Server 进行 Modbus TCP 通讯，由于客户端和服务器模式均使用相同的功能块，因此客户端功能块库的程序结构及各功能块完成的功能可以参考图 12

4.1 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
S7-400 电源模块 PS 407 10A	1	6ES7407-0KA01-0AA0
S7-400 CPU414-3PN/DP	1	6ES7414-3EM05-0AB0(V5.2)

S7-400 机架	1	6ES7400-1JA00-0AA0
网线	若干	
笔记本电脑	1	

表 5:客户端硬件清单

所用到软件如下表：

名称	订货号
STEP7 V5.5 组态编程软件 英文版	
“ ModbusTCP PN-CPU V2.4” 软件选项包	2XV9450-1MB02
Modslave V4.3.0 免授权版本	**可从网上免费获取**

表 6:客户端软件清单

4.2 S7-400 单站系统与 Modbus Slave 软件组态

打开 Step7 软件，新建一个工程项目文件，命名为“M_TCP_CPU_V2-4(Client)”, 在项目下插入一个 S7-400 站，如下图 23 所示：

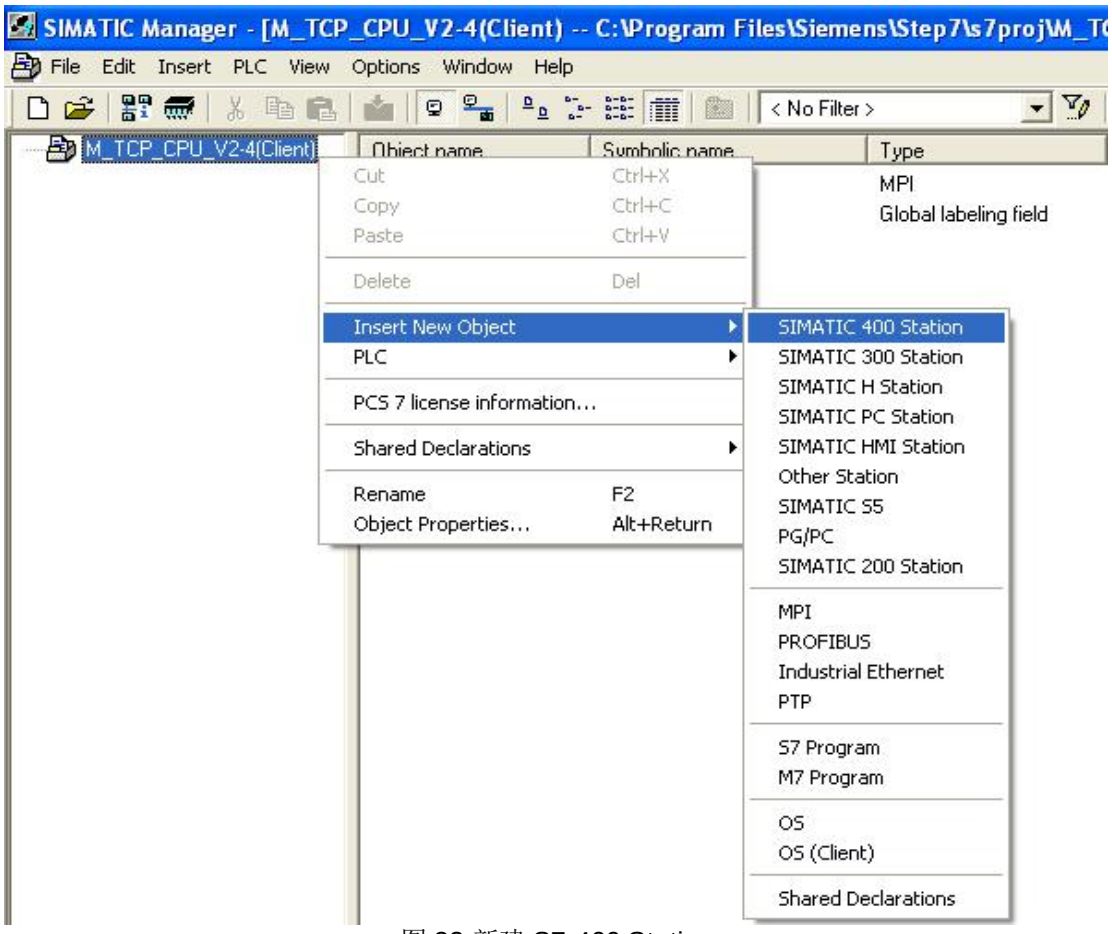

图 23:新建 S7-400 Station

双击插入的 SIMATIC 400 Station 的“Hardware”，打开硬件组态，在硬件组态界面下分别插入机架，电源 PS407、CPU414-3PN/DP,本例中将 CPU 的 PN 口 IP 地址设为**192.70.44.10，**如下图 24 所示：

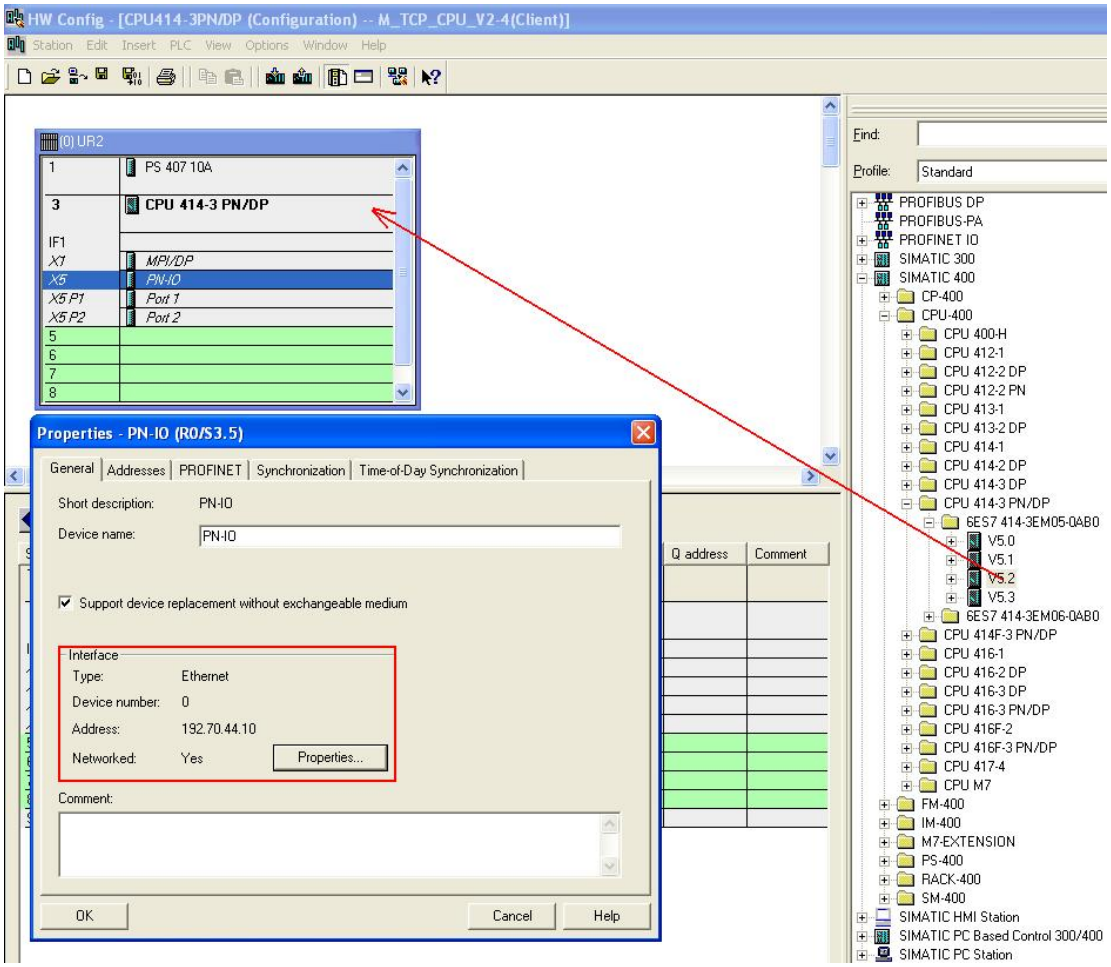

图 26: 硬件组态并设置 CPU 的 IP 地址

由于需要在 SIMATIC 站与其他通讯伙伴之间建立 TCP 连接用于 Modbus 通讯，而对于 CPU 的集成 PN 口来说须通过 Open IE(开放式以太网通讯)的方式来建立 TCP 连接， 通过 S7-CPU 的 PROFINET 接口 进行 Modbus TCP 通信时，需要使用通信块 FB65 "TCON"、FB66 "TDISCON"、FB63 "TSEND" 和 FB64 "TRCV"，要进行 Modbus TCP 通信，必须在数据块中为每个连接指定相应的参数，相应得参数在程序中主要由 DB2“MODBUS_PARAM“来完成初始化，关于 DB2“MODBUS_PARAM“各参数的含义请参见 V3.2 章节中的图 15、16 说明

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 为为本地服务器的端口 502，并可以勾选“Ignore Unit ID”选项，如下图 27 所示：

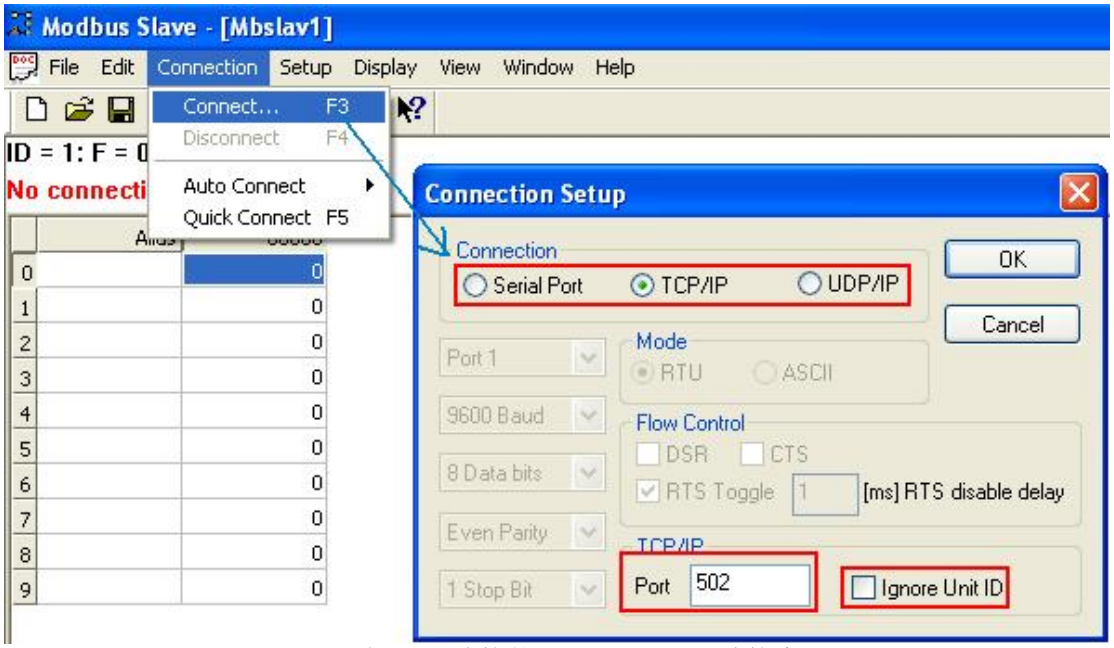

图 27:对应 TCP 连接的 Modbus Slave 连接窗口

（说明-“**Ignore Unit ID**”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）

4.3 通讯测试

由于“ModbusTCP CP V4.1”选项包支持功能码 FC1，2，3，4，5，6，15，16，不同的功能码测试过程中类似，因此下面同样以 FC03(读写保持寄存器)为例来说明通讯测试的整个过程，对于其他功能码的测试将不再重复描述

需要说明的是由于客户端功能块需要定义具体的功能码，而主功能块 FB102“MODBUSPN”并没有直接的管脚来定义功能码，而是由其中的两个参数“DATA_TYPE”和 DB2“MODBUS_PARAM“中的参数“single-write”共同决定，详细情况如下图 28 所示:

Data type	DATA_ TYPE	Function	Length	single_ write	Function code
Coils	1	read	any	irrelevant	1
Coils	1	write	1	TRUE	5
Coils	1	write	1	FALSE	15
Coils	1	write	>1	irrelevant	15
Inputs	2	read	any	irrelevant	2
Holding Register	3	read	any	irrelevant	3
Holding Register	3	write	1	TRUE	6
Holding Register	3	write	1	FALSE	16
Holding Register	3	write	>1	irrelevant	16
Input Register	4	read	any	irrelevant	4

图 28:S7-400 单站系统做客户端时不同的功能码的参数定义

由于客户端和服务器均使用相同的功能块 FB102“MODBUSPN”的参数需要初始化，因此分别在 OB100 及 OB1 中调用 FB108，在 OB100 中调用 FB909 完成相关参数的初始化，FB108 的管脚分布参见 V3.3 章节中的图 18 说明

下载硬件组态及程序到 CPU 中，将 DB2“MODBUS_PARAM“的参数“server_client“使能为 0，给参数 ENQ_ENR 发送脉冲信号，在打开的两个 Modbus Slave 软件窗口的“Set up->Slave Definition“中设置、寄存器连接类型、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”，如下图 29 所示：

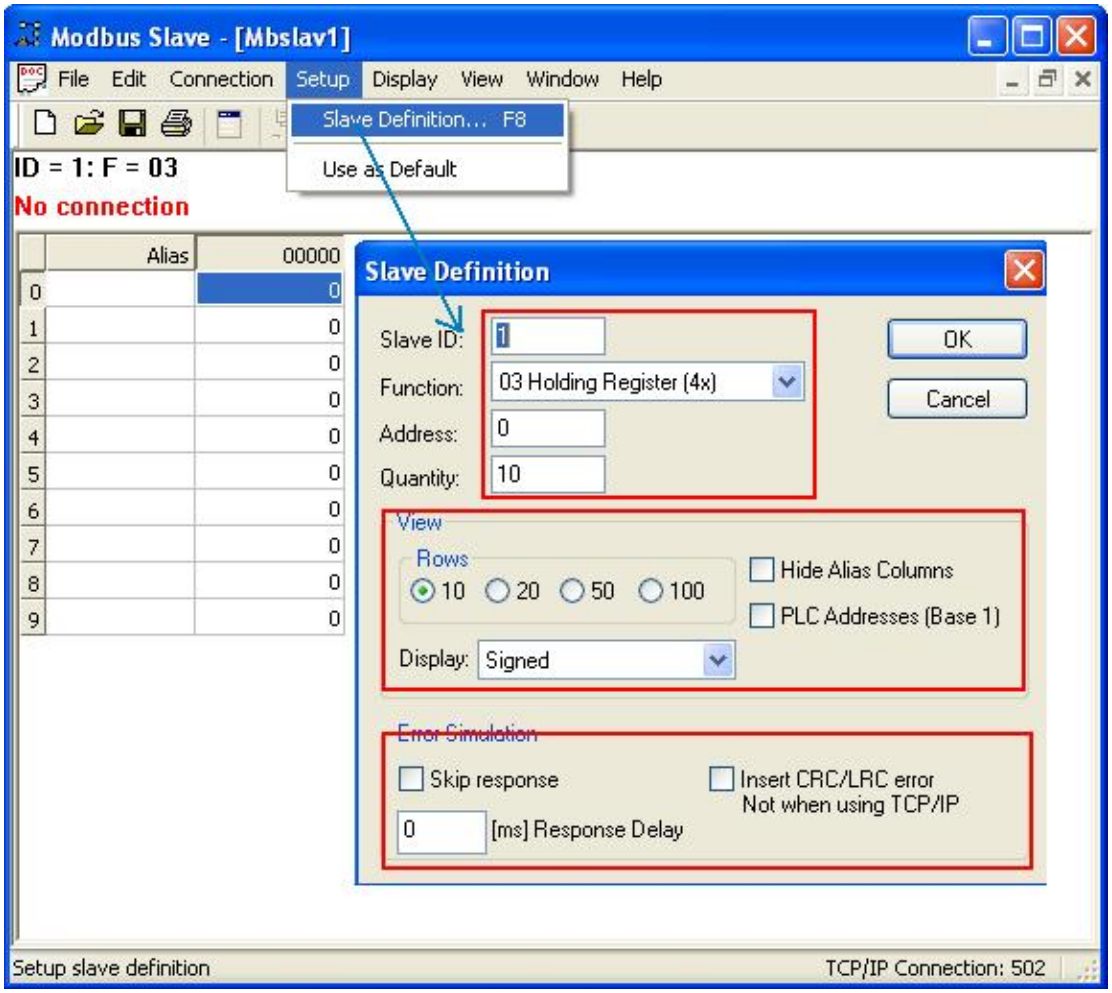

图 29: Modbus Slave 中 Modbus 数据参数定义

(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)

关于 SIMATIC 中 DB 偏移量、Modbus 物理编址、应用层编址对应关系请参考本文中 V3.3 章节图 21 说明

在 Step7 的项目程序中新建一个变量监控表，插入需要监控的参数和数据区变量，可以看到 Modsbus Slave 软件与 CPU414-3PN/DP 的数据通讯已经建立起来了，双方可以进行正常的保持寄存器数据读写操作(读写权限由参数"WRITE_ READ"决定)，如下图 30 所示：

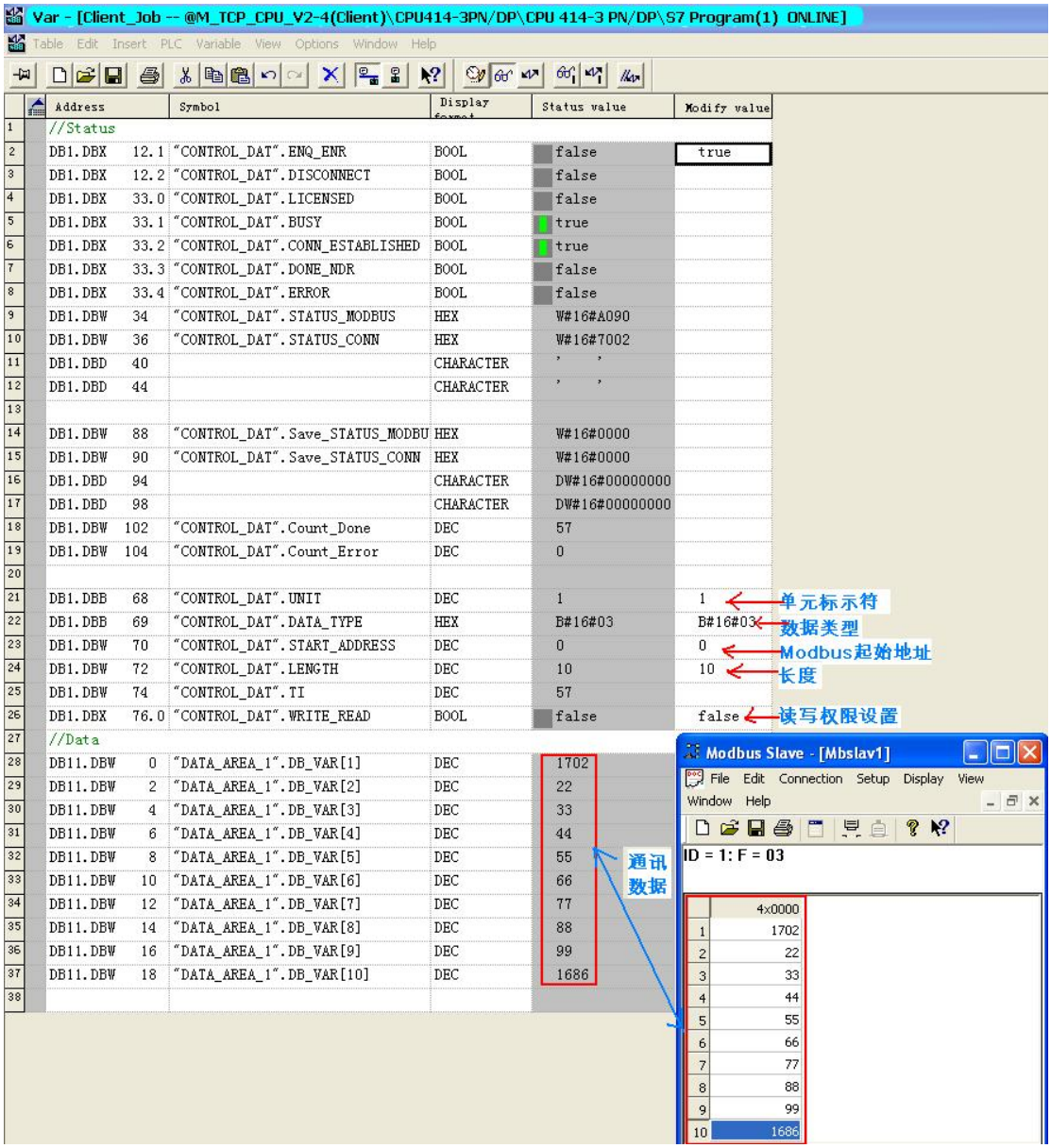

图 30:S7-400 单站系统 作为客户端与 Modbus Slave 软件通讯

5 “ModbusTCP PN-CPU V2.4” 选项包通讯使用总结及相关注意事项

由于是通过 PC 测试软件模拟第三方设备与 SIMATIC CPU 的集成 PN 口进行 Modbus TCP 通讯，因此在实际的第三方设备与 CPU 的集成 PN 口进行通讯时需要注意以下几点：

1) 由于订货号 2XV9450-1MB02 程序中会占用 CPU 较大的装载和工作存储区，因此对于性能比较低特别是 S7-300 的低端 CPU 进行通讯时必须考虑一定的富余量。

2) 对于 SIMATIC S7 这边，参数 **DB_x** 的数据区必须使用不同的 DB 块，使用同一个 DB 的不同地址区会造成地址编排混乱，另外参数 **Start_x** 与 **END_x** 参数不能出现地址叠加情况

3) 第三方设备的数据区与 SIMATIC S7 的数据 DB 块的地址对应关系可以先按照第三方的数据区域 Modbus 地址的偏移关系之后计算相应的偏移量

4)建议使用项目中的样例程序，只须修改连接 ID，定义通讯双方的 IP 地址、端口号及相应的

数据存储区等，能减少编程量，只须把样例程序放到一个单独的 FC 块中即可，样例程序中定义了足够的数据区，连接成功及错误次数指示等

5) Modbus TCP 每一包的数据最多只能发送 125 个寄存器或 2000 个比特位，超过该范围必须进行分包处理

6) S7-300/400 作为 Client 能与多少个 Server 建立通讯或者作为 Server 时能与多少个 Client 通讯取决于产品所支持的 TCP 连接数，Modbus/TCP 协议并没有对此进行约束和限制

7)如果使用 SIMATIC 作为 Modbus 服务器，那么一些 CPU 的可用端口号会受到限制，以下端口号可用于本地端口，如下图 31 所示:

CPU	MLFB(订货号)	软件版本	被释放的通信端口
IM151-8	6ES7 151-8AB00-0AB0	一直到 V2.6 版本	2000 到5000
IM151-8	6ES7 151-8AB00-0AB0	从 V2.7 版本开始	所有
CPU 315-2PN/DP	6ES7 315-2EG10-0AB0 and 6ES7 315-2EH13-0AB0	一直到 V2.3.4版本	2000 到5000
CPU 315-2PN/DP	6ES7 315-2EH14-0AB0	从 V3.1 版本开始	所有
CPU 317-2PN/DP	6ES7 317-2EK13-0AB0	直到 V2.3 版本	2000 到5000
CPU 317-2PN/DP	6ES7 317-2EK14-0AB0	从 V3.1 版本开始	所有
CPU 319-3PN/DP	6ES7 318-2EL00-0AB0	一直到 V2.6 版本	2000 到5000
CPU 319-3PN/DP	6ES7 318-2EL00-0AB0	从 V2.7 版本开始	所有
CPU 414-3PN/DP	6ES7414-3EM05-0AB0	V5.0从 V5.0 版本开始	所有
CPU 416-3PN/DP	6ES7416-3ER05-0AB0	V5.0从 V5.0 版本开始	所有

图 31: SIMATIC 作为 Modbus 服务器的端口号使用限制

详细情况可参考以下 FAQ 连接:
http://support.automation.siemens.com/CN/view/zh/34010717

更多关于 S7 Open Modbus/TCP 通讯的详细信息请参考西门子 Industrial IT 部门的以下连接：
http://www.industrysolutions.siemens.com/industrial-services/it/en/PRODUCTS/SIMATIC_ADD_ONS/S7_OPEN_MODBUS_TCP.HTM

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

附表一 CPU 集成 PN 口进行 Modbus TCP 通讯 FB 输出常见故障代码及处理

STATUS(Hex)	故障原因	处理措施
参数STATUS_MODBUS代码含义		
A001	数据块 DB(MODBUS_PARAM)长度过短	修改 DB 长度
A002	参数 END_x 小于 Start_x	修改参数 END_x 大于 Start_x
A003	Modbus 地址映射的 DB 块的数据区长度太短，最低长度: -寄存器: (START_ADDRESS – start_x +	扩展 DB 区域 当 CPU 为 Client 时： 修改参数 START-ADRESS 或者 LENGTH

	LENGTH) * 2 -位 (START_ADDRESS – start_x + LENGTH) / 8 其他可能的原因: ·参数初始化错误(CPU 为 Client 时) ·客户端请求报文时错误的地址区域(CPU 为 Server 时)	当 CPU 为 Server 时： 修改客户端的请求
A004	仅在 CP 为 Client 时才有此故障： 参数DATA_TYPE及WRITE_READ 设置不匹配，不可能对输入寄存器或离散输入进行写操作	修改此两个参数
A005	CP 为 Client 时： 参数 LENGTH 设置无效 CP 为 Server 时： Client 请求的寄存器号无效,合法的数据类型范围如下: 读线圈/离散输入: 1 to 2000 写线圈: 1 to 1968 读寄存器: 1 to 125 写保持寄存器: 1 to 123	CPU 为 Client 时： 修改参数 LENGTH CPU 为 Server 时： 修改 Client 请求的寄存器地址
A006	CP为客户端时： 数据区1-8中对应的Modbus地址范围(DATA_TYPE, START_ADDRESS和 LENGTH)不存在 CP 为服务器时： 客户端请求的报文不正确	CPU 为 Client 时： 修改参数 DATA_TYPE,START-ADRESS 或者 LENGTH CPU 为 Server 时： 修改 Client 请求或修改参数 data_type_x
A007	CPU 为 Client 时： 参数RECV_TIME或CONN_TIME时间设置无效，RECV_TIME最少20ms, CONN_ TIME为100ms	修改此两参数
A009	仅在 CPU 为 Client 时发生，标示符 TI 与发送方不一致，连接中断	修正通讯伙伴的报文
A00A	CPU 为 Client 时： 接收参数 UNIT 与发送的不一致	
A00B	CPU 为 Client 时： 接收与发送功能码不一致 CPU 为 Server 时： 无效的功能码被接收	CPU 为 Client 时： 检查通讯伙伴的数据报文格式 CPU 为 Server 时： 注意 FB MODBUSPN 仅支持功能码 FC01，02，03，04，05，06、15，16
A00C	接收到的字节长度与寄存器地址+不匹配，连接中断	检查通讯伙伴的数据报文格式
A00D	仅在 CPU 为 Client 时发生: 响应的 MODBUS 寄存器地址与请求	

	的不一致	
A00E	MODBUS 报文报头的长度与寄存器地址不匹配，FB 将忽略	
A00F	非 0 的协议标示符被接收,通讯中断	
A010	参数 DB1-DB8 中有重复使用的 DB 块	修改为单独的 DB
A011	参数 DATA_TYPE 设置无效(范围为 1-4)	修改该参数
A012	数据区参数data_type_1和data_type_2设置重叠	统一类型的寄存器地址不能有叠加情况
A013	数据区参数 data_type_1 和 data_type_3 设置重叠	
A014	数据区参数 data_type_1 和 data_type_4 设置重叠	
A015	数据区参数 data_type_1 和 data_type_5 设置重叠	
A016	数据区参数 data_type_1 和 data_type_6 设置重叠	
A017	数据区参数 data_type_1 和 data_type_7 设置重叠	
A018	数据区参数 data_type_1 和 data_type_8 设置重叠	
A019	当参数 data_type_x 设置不为 0 时，db_x 被赋值 0	DB 块号不能为 0
A01A	Modbus 报头中错误的长度(1-253 字节有效)	检查通讯伙伴的数据报文格式
A01F	FB MODBUSPN 处于无效的连接状态	联系产品支持
A023	数据区参数data_type_2和data_type_3设置重叠	统一类型的寄存器地址不能有叠加情况
A024	数据区参数data_type_2和data_type_4设置重叠	
A025	数据区参数data_type_2和data_type_5设置重叠	
A026	数据区参数data_type_2和data_type_6设置重叠	
A027	数据区参数data_type_2和data_type_7设置重叠	
A028	数据区参数data_type_2和data_type_8设置重叠	
A034	数据区参数data_type_3和data_type_4设置重叠	
A035	数据区参数data_type_3和data_type_5设置重叠	
A036	数据区参数data_type_3和data_type_6	

	设置重叠	
A037	数据区参数data_type_3和data_type_7设置重叠	
A038	数据区参数data_type_3和data_type_8设置重叠	
A045	数据区参数data_type_4和data_type_5设置重叠	
A046	数据区参数data_type_4和data_type_6设置重叠	
A047	数据区参数data_type_4和data_type_7设置重叠	
A048	数据区参数data_type_4和data_type_8设置重叠	
A056	数据区参数data_type_5和data_type_6设置重叠	
A057	数据区参数data_type_5和data_type_7设置重叠	
A058	数据区参数data_type_5和data_type_8设置重叠	
A067	数据区参数data_type_6和data_type_7设置重叠	
A068	数据区参数data_type_6和data_type_8设置重叠	
A078	数据区参数data_type_7和data_type_8设置重叠	
A079	参数 ID 在 DB(MODBUS_PARAM)中未定义	修改参数 ID
A07A	无效的参数 ID(ID 值范围为 1-4095)	
A07B	参数 ID 在 DB(MODBUS_PARAM)中存在 2 次	修改 DB 块 DB(MODBUS_PARAM)
A07C	参数 data_type_x 无效(范围 1-4)	
A07D	参数 data_type_1 未定义，data_type_1 为缺省的使用数据区，需要定义	
A07E	参数 DB_x 与 DB(MODBUS_PARAM)或 FB102 的背景 DB 号冲突	
A07F	FB102 接口参数 PARAM_DB 错误，非通讯参数 DB	指定正确的 DB 给接口参数 PARAM_DB
A080	数据块 DB(MODBUS_PARAM)更改但没有执行 CPU 重起	数据块 DB(MODBUS_PARAM)需要初始化，当更改时需要 CPU 重起
A081	CP 为 Client 且使用 FC05 功能码时:接收的线圈状态与发送不一致	通过抓包工具来分析和修正通讯伙伴的报文
A082	CP 为 Client 且使用 FC06 功能码时:接收的寄存器值与发送不一致	通过抓包工具来分析和修正通讯伙伴的报文
A083	仅在 CP 为 Client 时:在上一个请求还	等待DONE =TRUE 或 ERROR = TRUE

	没有处理完成时又发送新的请求	后再发送新请求
A084	授权码”IDENT_CODE”不能识别	联系产品支持
A085	在授权期间由于无效的写权限导致发生错误	对于授权DB，确认参数REG_KEY的结构是否正确
A090	功能块未授权，此为一状态信息，参数 ERROR 并不会置 1，功能块在未授权情况仍然可以运行而不影响通讯	针对CPU读出预授权解码，之后按照授权操作向IT4industry.部门索取授权码
A091	收到异常响应码 1(仅在 Client 模式)，连接将终止和重新建立	通讯伙伴不支持请求的报文
A092	收到异常响应码 2(仅在 Client 模式)，无效的或不存在的地址请求	确认参数LENGTH 或 START_ADDRESS 是否正确
A093	收到异常响应码 3(仅在 Client 模式)	通讯伙伴无法执行报文接收(例如请求长度不支持等)
A094	收到异常响应码 4(仅在 Client 模式)	通讯伙伴无法执行报文接收
A095	收到未知的异常响应码(仅在 Client 模式)	通过抓包工具来分析和修正通讯伙伴的报文
参数STATUS_CONN代码含义		
A100	CONN_TIME 与 RECV_TIME 时间超出，RECV_TIME 超出时连接终止	检查连接参数
A101	参数 TDISCON 的监控时间超出	联系产品供应商
SFC6/20 故障代码		
7xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager -> mark block -> key F1 –> Ethernet -> see also -> code evaluation 可以查到相关帮助信息
8xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager -> mark block -> key F1 –> Ethernet -> see also -> code evaluation 可以查到相关帮助信息
FB63,64,65,66 故障代码		
7xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager -> mark block -> key F1 –> Ethernet -> see also -> code evaluation 可以查到相关帮助信息
8xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager -> mark block -> key F1 –> Ethernet -> see also -> code evaluation 可以查到相关帮助信息
SFC24 故障代码		
80A1	DB=0 或超出了 CPU 允许的范围	选择有效的 DB
80B1	DB 块在 CPUU 中不存在	DB_x 参数中的 DB 块必须创建并下载到 CPUU 中
80B2	DB 块被创建为“Unlinked”类型	DB 块不能创建为“Unlinked”类型