EBN工业通信联盟
方案，培训，工程服务

EBN工业通信联盟简介

我们致力于工控领域的网络化与信息化，体验中心配置了各大主流品牌的专业的实验设备，定期开展产品和通信技术培训，同时我们也热忱的欢迎您前来开展学习和测试活动，和我们一起分享您成功的解决方案和行业经验。

主要仪器与设备

产品技术培训

ControlLogix 架构和编程

FactoryTalk View SE 架构和编程

GPRS/3G 无线传输专题方案

Siemens S7-300 架构和编程

Siemens S7-200 架构和编程

基于 Siemens S7-200 的通讯方案

联系我们

体验中心：（ 地址待定 ）
QQ 群号：200467216
EMAIL：2415340977@QQ.com
资料下载： http://iask.sina.com.cn/u/1401350072

SIEMENS

基于 S7-300,400 以太网通讯模块 CP Modbus TCP 通讯快速入门

Modbus TCP Communication Base On S7-300/400 Ethernet CP Module Getting Started

Getting-Started	**Edition (2009 年 11 月)**

摘　要 本文主要介绍了通过 S7-300/400 以太网通讯模块 CP343/443-1 进行 Modbus TCP 的通讯原理,并以 Modscan32 和 Modbus slave 软件为例模拟第三方设备详细介绍如何配置与 CP343-1 进行 Modus TCP 通讯,希望通过本文档,能够给读者 CP343/443-1 Modbus TCP 通讯入门指导

关键词 CP343-1,CP443-1,Modbus TCP,保持寄存器,输入寄存器,读写,服务器,客户端,Modscan32,Modbus Slave

Key Words CP343-1,CP443-1,Modbus TCP,Holding Register,Input Register Read/Write,Server,Clent,Modscan32,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 Modbus TCP 通讯概述

2.1 概述

建立 SIMATIC S7 和第三方设备的 MODBUS/TCP 通信时有三种可能情况：

1) 外部 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
产品"OPEN MODBUS / TCP" (2XV9450-1MB00) ,支持功能代码 3、4 和 16。

2) 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"OPEN MODBUS / TCP PN-CPU" (2XV9450-1MB02),已发布的版本 2 支持功能代码 1、2、3、4、5、6、15 和 16, 这对 S7-300 和 S7-400 集成 PN 接口的 CPU 都适用。

3) H 系统中的冗余通信通过 CP343-1 和 CP443-1 通讯：

通过 CP443-1 在 H 系统中的冗余通讯在 S7-400H 站和第三方设备间建立 Modbus/TCP 连接时需要产品"OPEN MODBUS / TCP Redundant" (2XV9450-1MB01) 。该产品支持单边与双边冗余,支持的功能代码有 3、4 和 16。

2.2 CP343-1 或 CP443-1 做 Modbus TCP 通讯的使用限制

1) 所支持的模块(如下表)

类别	型号
CP343-1	6GK7 343-1CX00-0XE0 及后续版本 6GK7 343-1EX11-0XE0 及后续版本 6GK7 343-1GX11-0XE0 及后续版本
CP443-1	6GK7 443-1EX11-0XE0 及后续版本 6GK7 443-1GX11-0XE0及后续版本

2) 软件版本要求

使用 CP343-1 或 CP443-1 进行 Modbus TCP 通讯需要带有 NCM S7 选项的 Step7 V5.1 或更高版本

3) 存储空间需求

功能块	内存需求
FB100(FB MODBUS)	需要用 CPU 8800 byte 的工作存储区 和 9886 byte 的装载 存储区
FB101(FB MODB4)	需要用 CPU 9822 byte 的工作存储区 和11074 byte的装载 存储区

3 配置 CP343-1 作为 Server 进行 Modbus TCP 通讯

下面以 CP343-1(6GK7343-1CX00-0XE0)及 Modscan32 软件(软件的使用及安装程序见附件 1)为例,详细介绍如何将 CP343-1 配置为 Server,Modscan32 为 Client 进行 Modbus

TCP 通讯,由于在 S7 控制器通过外部 CP343-1 或 CP443-1 和第三方设备间建立 Modbus/TCP 连接时需要产品"OPEN MODBUS / TCP" (2XV9450-1MB00),首先介绍一下产品 2XV9450-1MB00 中所包含的两个功能块 FB100 及 FB101 完成的主要功能:

Product	Identification number	From version
OPEN MODBUS / TCP	2XV9 450-1MB00	3.1
FB 100 “MODBUS”		2.3
FB 101 “MODB4”		1.1

FB100: 完成 Modbus 类别 0 功能码 FC3(读多个保持寄存器)及 FC16(写多个保持寄存器),
FB101: 完成 Modbus 类别 0 功能码 FC3(读多个保持寄存器)及 FC16(写多个保持寄存器)及类别 1 功能码 FC4(读输入寄存器),

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：

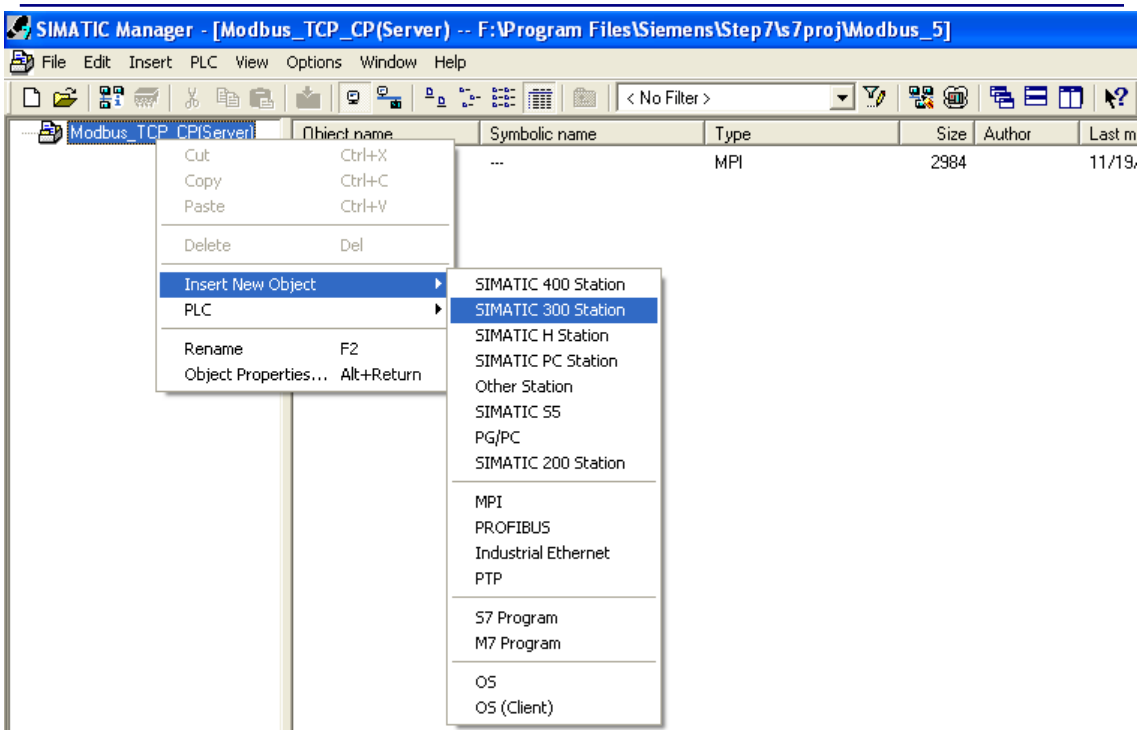
名称	数量	订货号
S7-300 电源模块 PS 307 5A	1	6ES7307-1EA00-0AA0
S7-300 CPU319-3PN/DP	1	6ES7319-3EL00-0AB0(V2.8)
S7-300 CP343 Lean	1	6GK7343-1CX00-0XE0
S7-300 机架	1	6ES7390-1AF30-0AA0
网线及 Profibus 电缆	若干	
笔记本电脑	1	

所用到软件如下表：

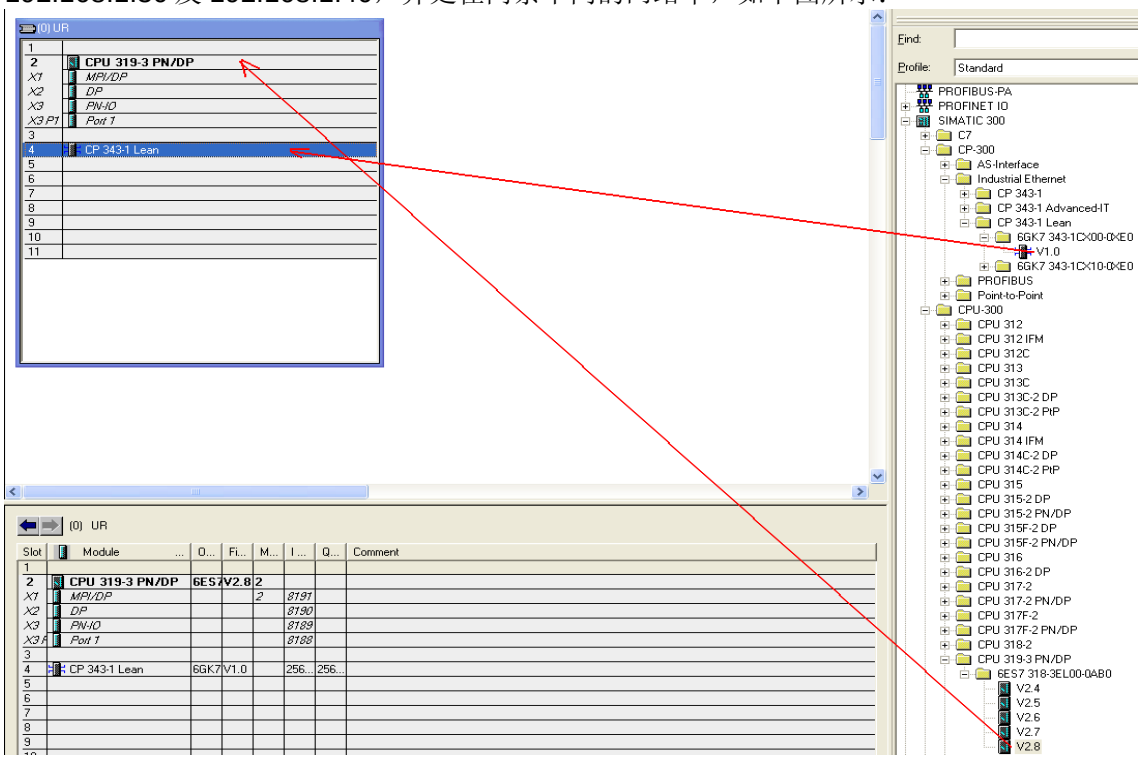
名称	订货号
STEP7 V5.4 组态编程软件 英文版	
Modscan32 V7.0	

3.2 通过 Step7/HW 及 Modscan32 软件组态

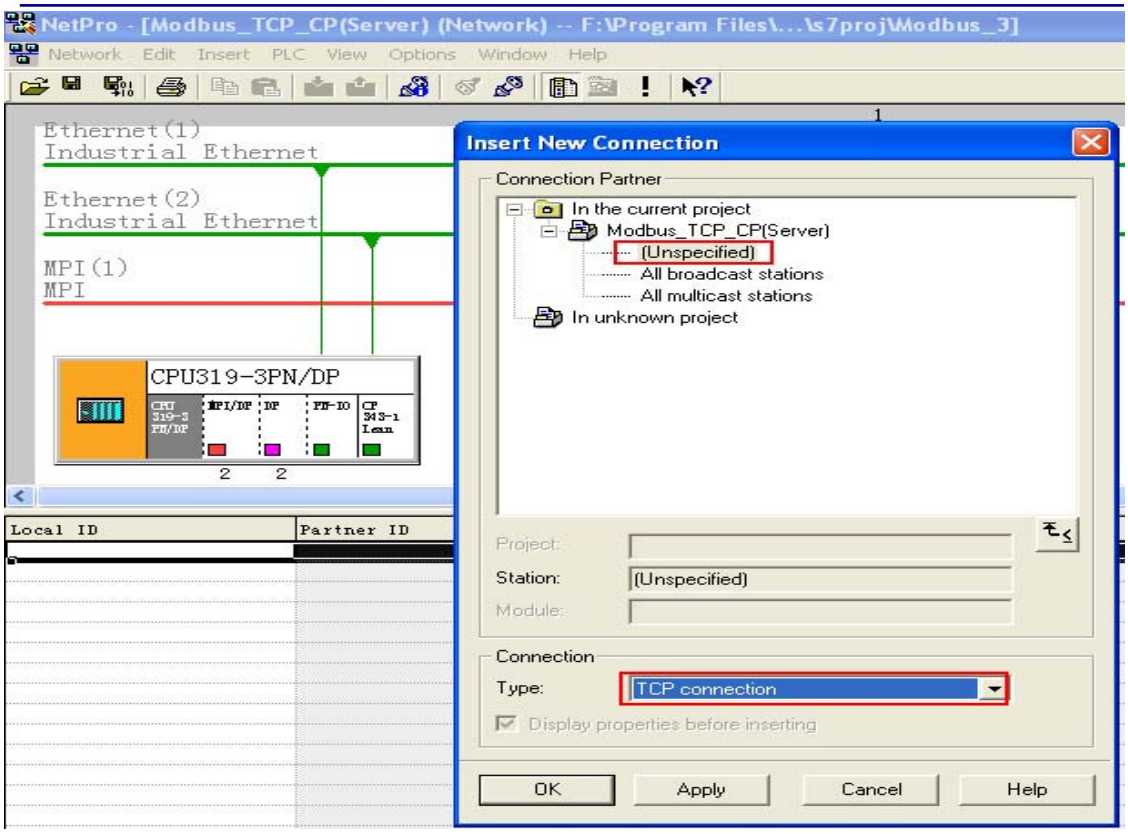
打开 Step7 软件，新建一个工程项目文件，命名为“Modbus_TCP_CP(Server)”, 在项目下插入一个 S7-300 站，如下图：



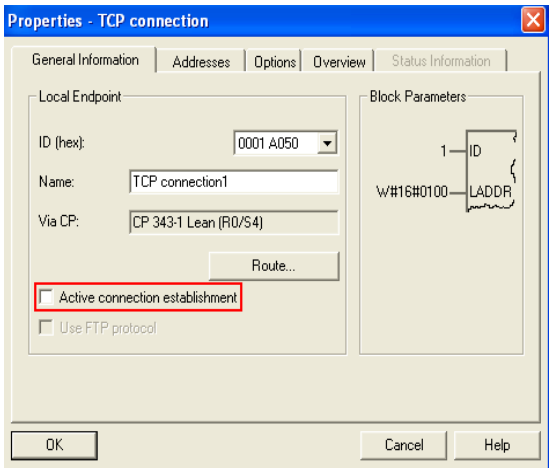
双击插入的 S7-300 站的“Hardware”，打开硬件组态，在硬件组态界面下分别插入机架，电源 PS307,CPU319-3PN/DP，CP343-1 Lean,本例中将 CPU 和 CP 的 IP 地址分别设为 192.168.1.30 及 192.168.1.40，并处在两条不同的网络中，如下图所示：

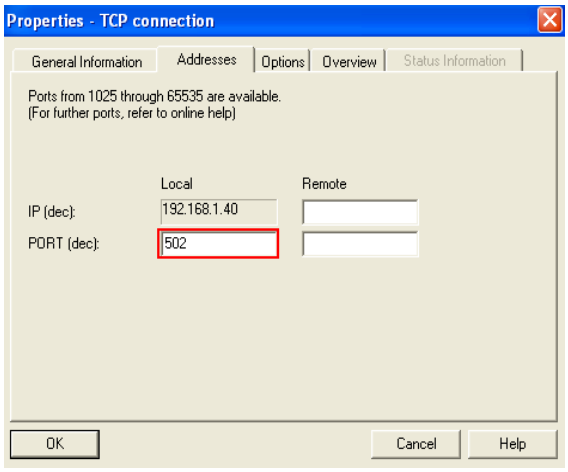


打开 Netpro 网络组态,选中 CPU319-3PN/DP,插入一个新连接，连接伙伴为 Unspecified，连接类型为 TCP Connection,如下图所示：

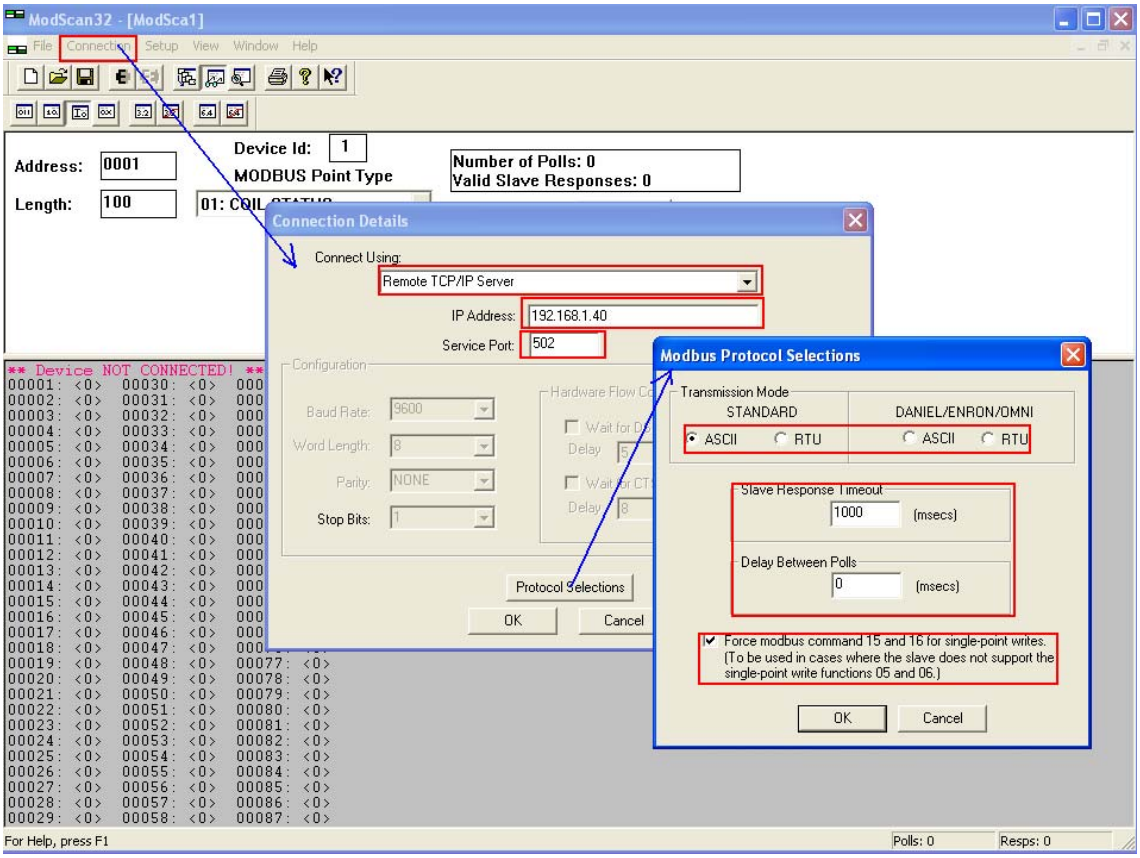


在打开的连接属性对话框中的“General Information”中由于 CP343-1 做 Server 被动连接，因此不勾选“Active connection estabishment”选项,在“Adress”栏中同样由于 CP343-1 做 Server，因此填入连接的 Port 号为 502，如下图所示：





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 填入 CP343-1 Lean 的 IP 地址 192.168.1.40，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，这里保持缺省设置即可，如下图所示：



3.3 FB100(FB MODBUS)读写保持寄存器通讯测试

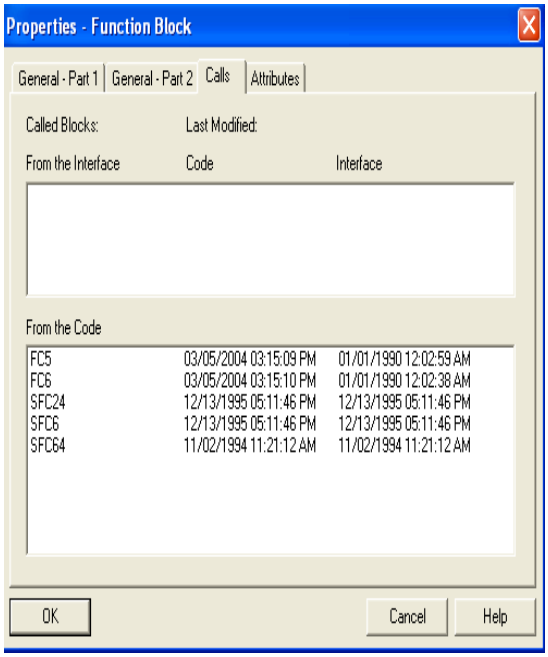
由于 FB100 的参数需要初始化，因此分别在 OB100 及 OB1 中调用 FB100，在 OB100 中调用 FB100 完成相关参数的初始化，FB100 中内部包含了相关系统功能块，完成数据读写、OB 执行监控、信息诊断等功能，如下图所示:

Network 1: cyclic call of FB MODBUS

Comment:

```
OPN   "CONTROL DAT"

CALL  "MODBUST" , "MODBUS DAT"
 ID              :=
 LADDR           :=
 TIMER_NR        :=T5              //nonattached timer
 MONITOR         :="CONTROL DAT".MONITOR
 DB_1            :=W#16#B
 START_1         :=W#16#1
 END_1           :=W#16#3E8
 DB_2            :=
 START_2         :=
 END_2           :=
 DB_3            :=
 START_3         :=
 END_3           :=
 DB_4            :=
 START_4         :=
 END_4           :=
 DB_5            :=
 START_5         :=
 END_5           :=
 WRITE_PROTECT1:=
 WRITE_PROTECT2:=
 WRITE_PROTECT3:=
 WRITE_PROTECT4:=
 WRITE_PROTECT5:=
 ENQ_ENR         :="CONTROL DAT".ENQ_ENR
 SERVER_CLIENT   :=TRUE
 DONE_NDR        :="CONTROL DAT".DONE_NDR
 ERROR           :="CONTROL DAT".ERROR
 STATUS          :="CONTROL DAT".STATUS
 START_ADDRESS   :="CONTROL DAT".START_ADDRESS
 LENGTH          :="CONTROL DAT".LENGTH
 WRITE_READ      :="CONTROL DAT".WRITE_READ
 TI              :="CONTROL DAT".TI
 UNIT            :="CONTROL DAT".UNIT
```



FC5,FC6,SFC24,SFC6,SFC64 的功能如下：

FC5:发送功能块

FC6:接收功能块

SFC6:中断组织 OB 执行确认功能块

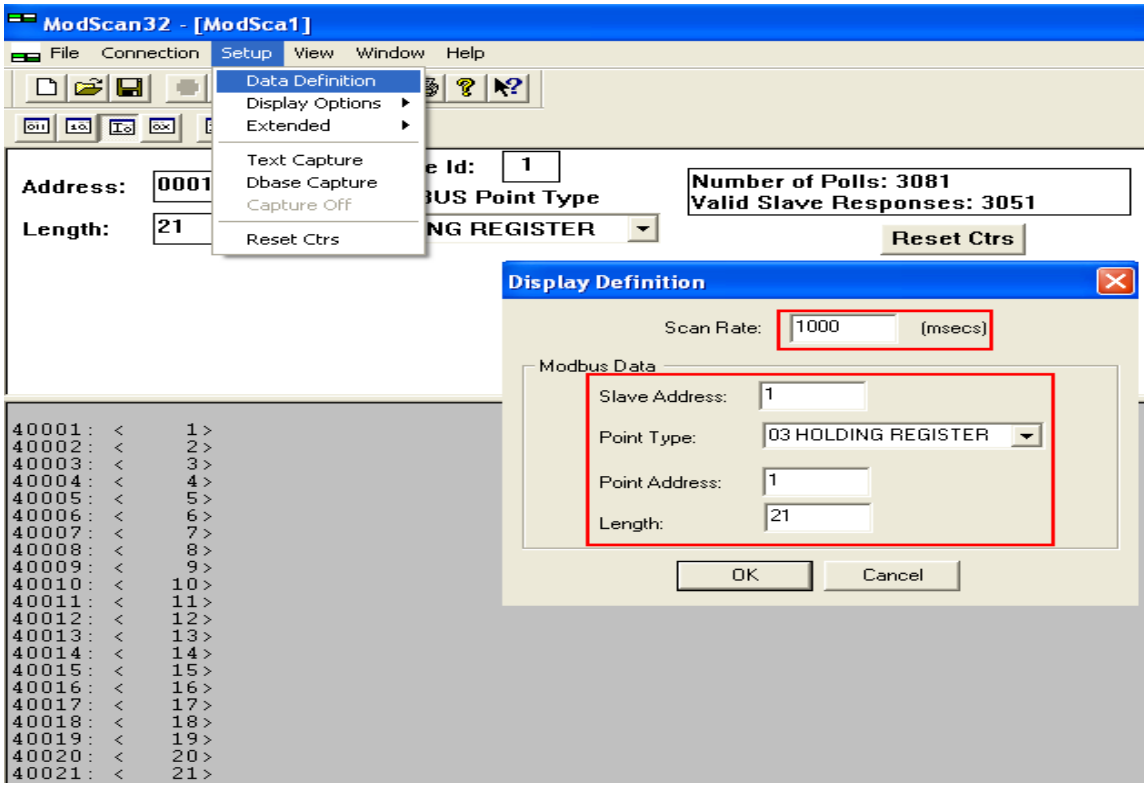
SFC24:诊断信息功能(测试定义的数据区是否可用，包括起始地址及长度等)

SFC64:读取系统时间

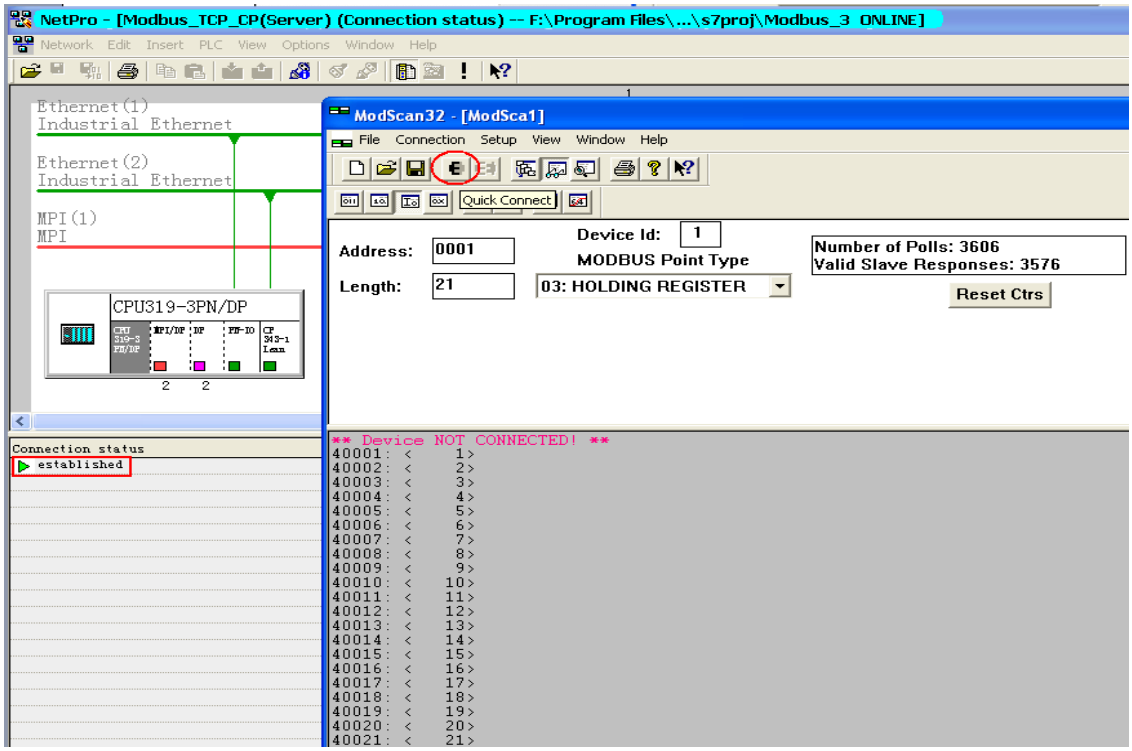
FB100(FB MODBUS)的各参数含义如下表：

类型	参数	含义	初始化
IN	ID	Netpro 中的连接 ID	是
	LADDR	CP 模块的逻辑起始地址	是
	TIMER_NR	监控定时器	否
	MONITOR	等待通信伙伴数据时间,100ms 为 1 个单位	否
	DB_x(x=1-5)	保存寄存器读取通讯数据块,可定义 5 个数据区	是
	Start_x	Modbus 保持寄存器起始地址	是
	END_x	Modbus 保持寄存器结束地址	是
	WRITE_ PROTECTx	数据区写保护使能,只对 Server 模式有效	是
	ENQ_ENR	CP 为客户端时使能请求;CP 为 Server 时接收数据准备好	否
	SERVER_CLIENT	Server 或 Clien 模式选择	否
OUT	DONE_NDR:	CP 为客户端时,激活连接无错误 CP 为服务器时,来自客户端的请求已应答	否
	ERROR	通讯错误	否
	STUTUS	通讯状态代码	否
IN/OUT	START_ADDRESS	Modbus 起始地址,CP 为 Client 时为输入参数,CP 为 Server 时为输出参数	否
	LENGTH	需要处理的寄存器字节长度, CP 为 Client 时为输入参数，CP 为 Server 时为输出参数	否
	WRITE_READ	读写使能，CP 为 Client 时为输入参数，CP 为 Server 时为输出参数	否
	TI	处理标识	否
	UNIT	单元验证码	否

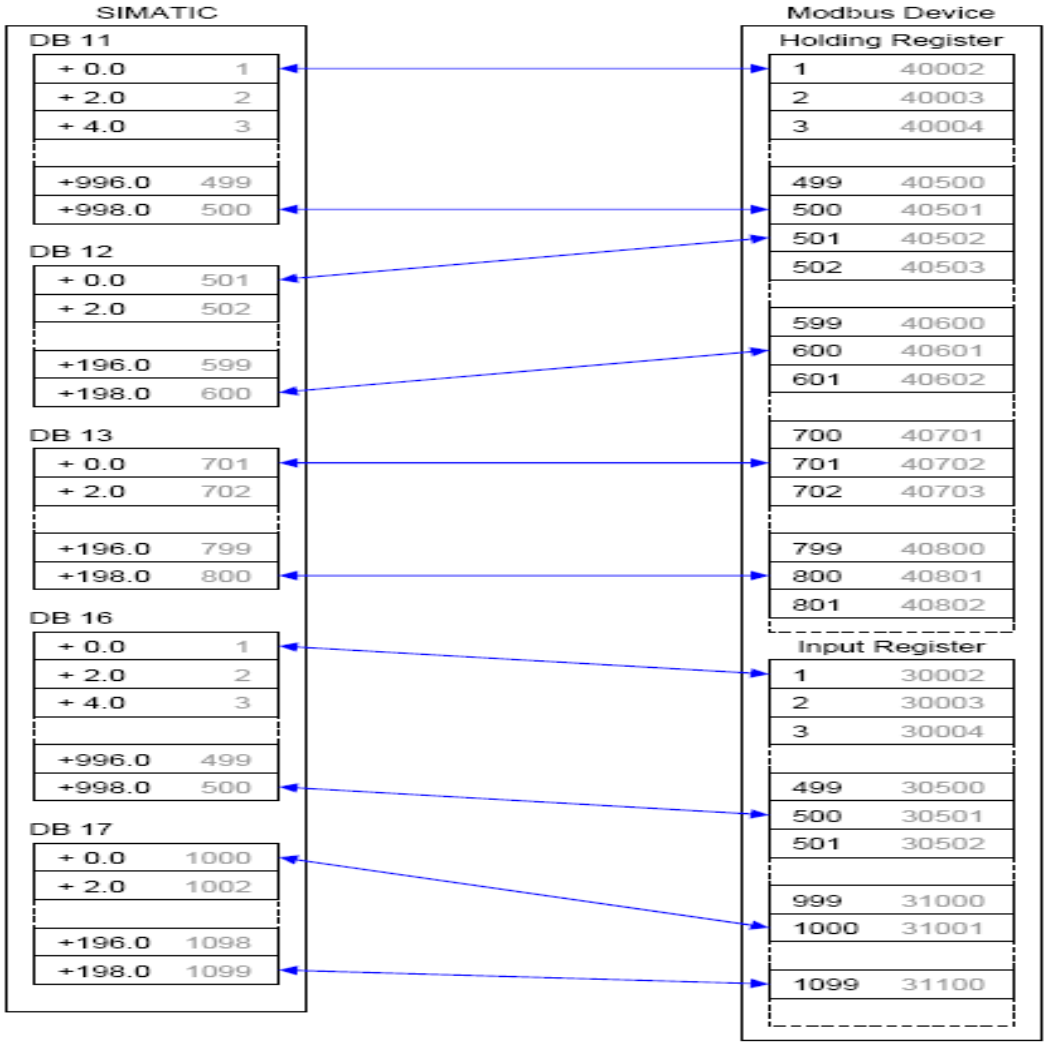
下载网络组态及程序到 CPU 中，使能参数 ENQ_ENR=1，在 Modscan32 的“Set up->Data Definition“中设置数据扫描周期、寄存器连接类型、起始地址、长度等，如下图所示：



之后在 modbus32 中就可以建立和远程 CP343-1 Server 的连接了，在 Netpro 中通过可以看到连接已经建立起来，如下图所示:



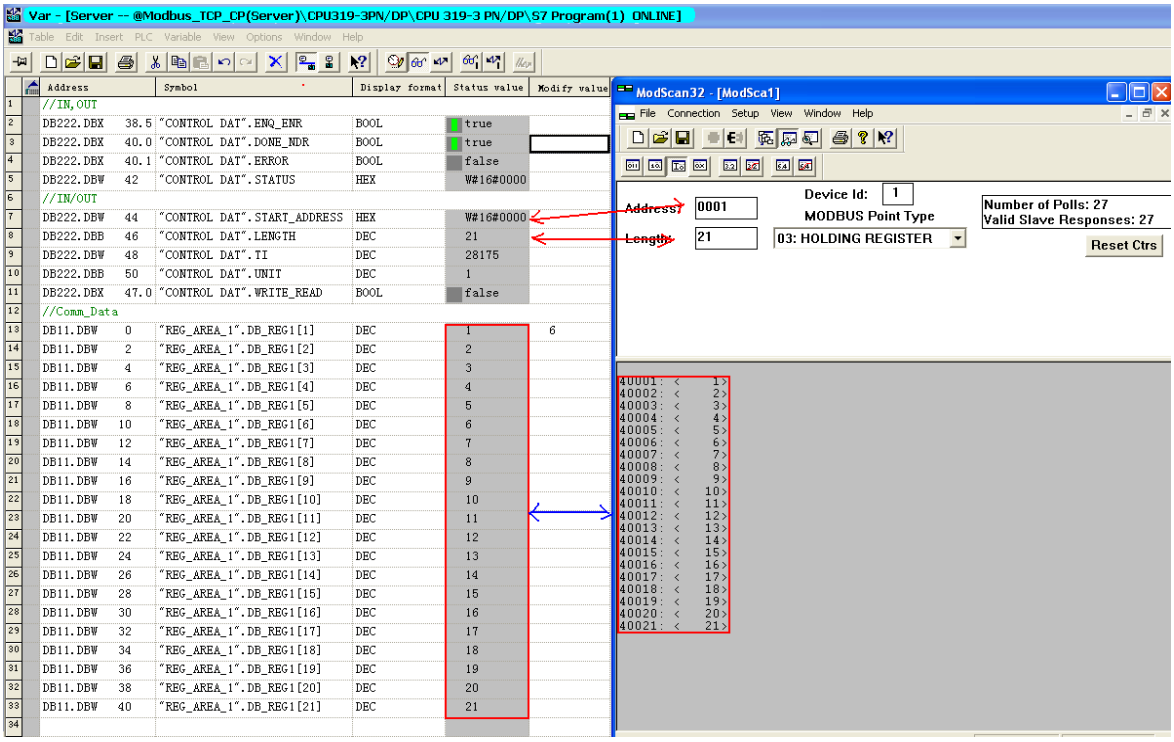
由于 Modbus 的内部地址编排时基于数据链路层和应用层有一定的映射关系，因此 Modbus 的地址与 SIMATIC 中的 DB 块的地址时按照一定的地址映射关系来相对应，这样造成了 DB 块中有一定的地址偏移量,如下图所示：



(说明:**1-**右边 **Modbus Device** 的黑色字体 **modbus** 地址基于数据链路层进行编排，灰色字体的地址是基于应用层进行编排

2-左边的 **SIMATIC** 中黑色字体为 **DB** 块中的地址偏移量，灰色字体为相对应的 **Modbus** 寄存器地址)

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 CP343-1 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，如下图所示：



3.4 FB101(FB MODB4)读写输入保持寄存器通讯测试

FB101(FB MODB4)除了能完成读写保持寄存器功能块外，还能完成读输入寄存器功能功能，由于与 FB100 (FB MODBUS)只是增加了读输入寄存器功能，因此在 OB 块中的调用、地址映射和偏移量、Modscan32 中通讯连接包括保存寄存器德读取等可以参看上述 FB100 (FB MODBUS)的相关设置,下面主要介绍它们之间参数的不同及如何进行输入寄存器的读取操作.

FB101(FB MODB4)的参数架构如下图所示:

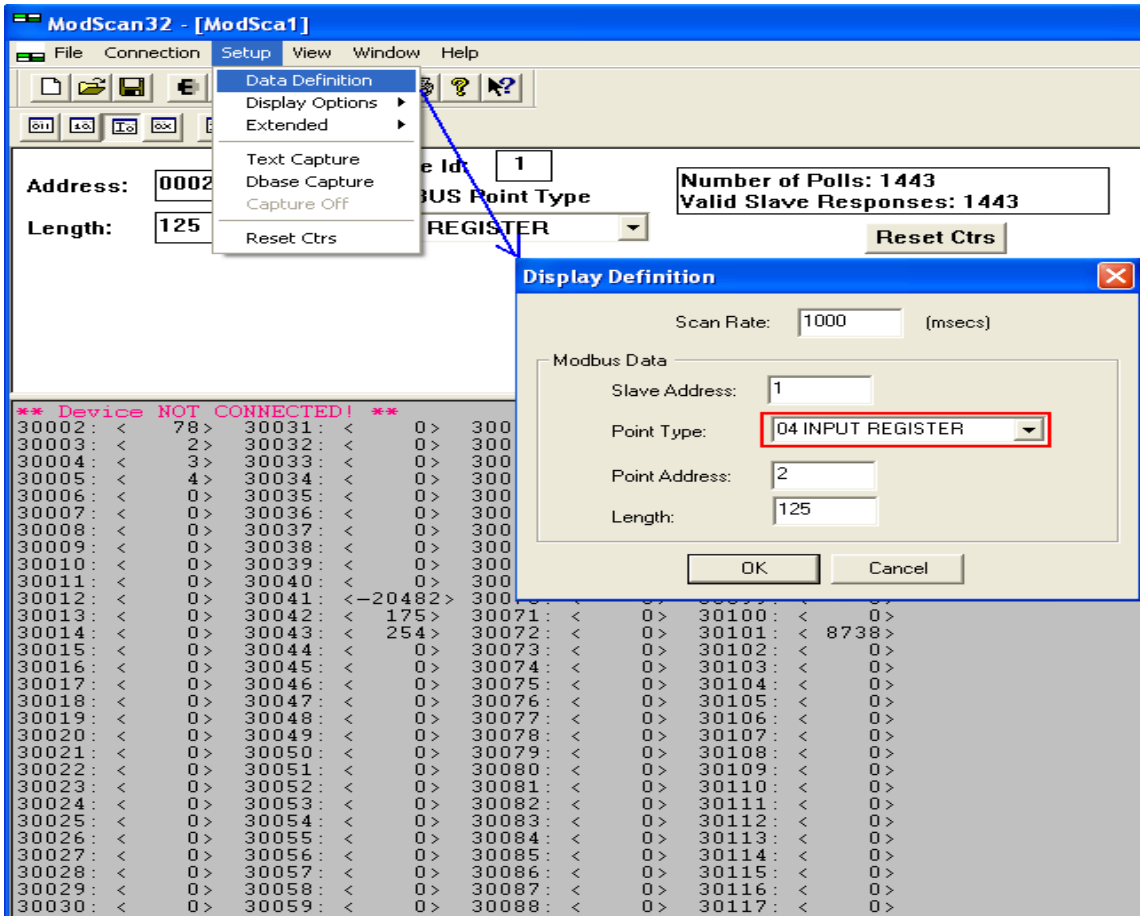
```
CALL   "MODB4" , "MODB4_DAT"
 ID              :=
 LADDR           :=
 TIMER_NR        :=
 MONITOR         :="CONTR_DAT".MONITOR
 DB_1            :=
 START_1         :=
 END_1           :=
 DB_2            :=
 START_2         :=
 END_2           :=
 DB_3            :=
 START_3         :=
 END_3           :=
 DB_4            :=
 START_4         :=
 END_4           :=
 DB_5            :=
 START_5         :=
 END_5           :=
 DB_6            :=
 START_6         :=
 END_6           :=
 DB_7            :=
 START_7         :=
 END_7           :=
 DB_8            :=
 START_8         :=
 END_8           :=
 WRITE_PROTECT1:=
 WRITE_PROTECT2:=
 WRITE_PROTECT3:=
 WRITE_PROTECT4:=
 WRITE_PROTECT5:=
 ENQ_ENR         :="CONTR_DAT".ENQ_ENR
 SERVER_CLIENT   :=
 DONE_NDR        :="CONTR_DAT".DONE_NDR
 ERROR           :="CONTR_DAT".ERROR
 STATUS          :="CONTR_DAT".STATUS
 START_ADDRESS   :="CONTR_DAT".START_ADDRESS
 LENGTH          :="CONTR_DAT".LENGTH
 WRITE_READ      :="CONTR_DAT".WRITE_READ
 INPUT_HOLDING   :="CONTR_DAT".INPUT_HOLDING
 TI              :="CONTR_DAT".TI
 UNIT            :="CONTR_DAT".UNIT
```

由于一些参数和 FB100 (FB MODBUS)的参数相同，因此下表只列出了 FB101(FB MODB4)的额外一些参数:

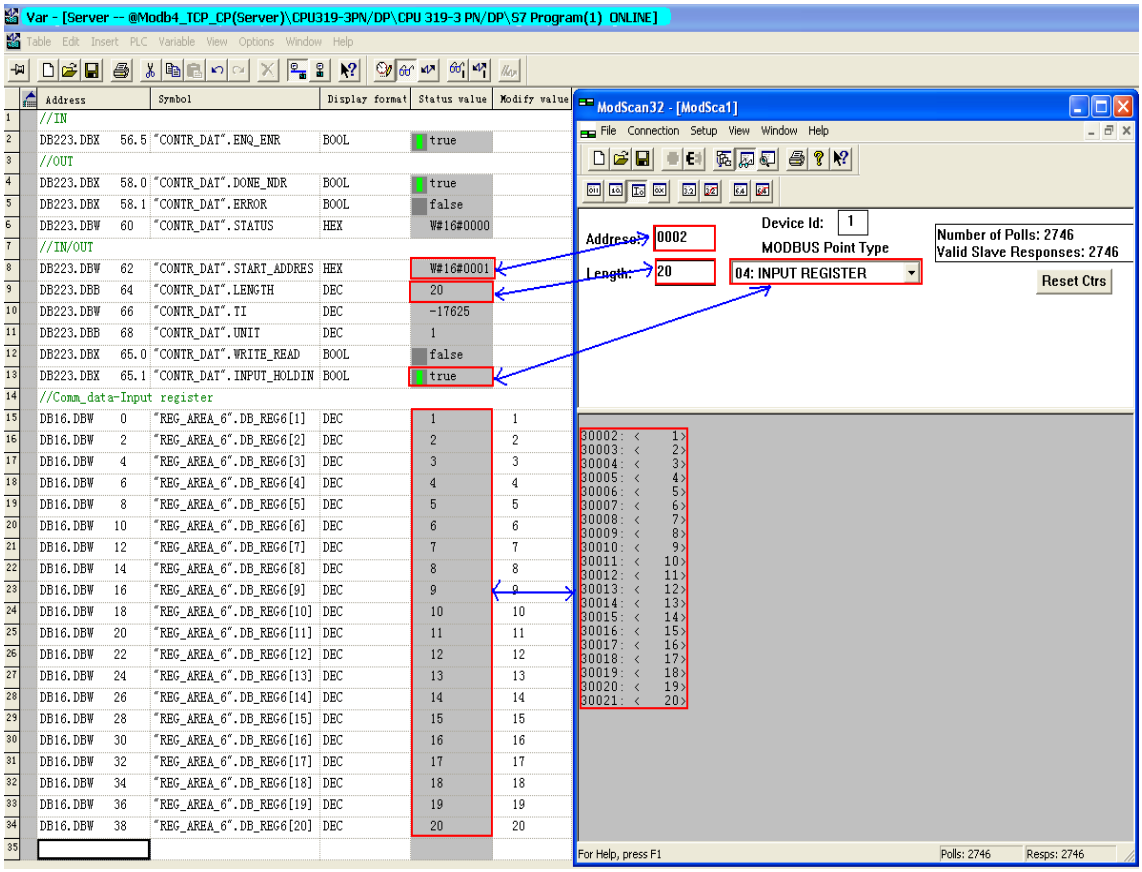
类型	参数	含义	初始化
IN	DB_x(x=6-8)	输入寄存器读取通讯数据块,可定义 3 个数据区	是
	Start_x	Modbus 输入寄存器起始地址	是
	END_x	Modbus 输入寄存器结束地址,不能小于 Start_x	是
IN/OUT	INPUT_HOLDING	寄存器读取类型选择，FALSE 时为读取保持寄存器，TRUE 时为读输入寄存器；CP 为 Client 时为输入参数,CP 为 Server 时为输出参数	否

（注意：**FB101 可以建立 8 个 DB 区与对方通讯，其中 DB1-5 为 MODBUS 保持寄存器通讯区，DB6-8 为输入寄存器通讯区，两个区的 DB 不能相互交错及出现叠加情况**）

在 Modscan32 中的“Set up->Data Definition“设置数据扫描周期、寄存器连接类型、起始地址、长度等，此时寄存器连接类型应该选择输入寄存器，如下图所示：



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 CP343-1 的数据通讯已经建立起来了，双方可以进行正常的输入寄存器数据读取操作，如下图所示：



4 配置 CP343-1 作为 Client 进行 Modbus TCP 通讯

下面以 CP343-1(6GK7343-1CX00-0XE0)及 Modbus Slave 软件(软件的使用及安装程序见附件 2)为例,详细介绍如何将 CP343-1 配置为 Client,Modsbus Slave 为 Server 进行 Modbus TCP 通讯.

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:

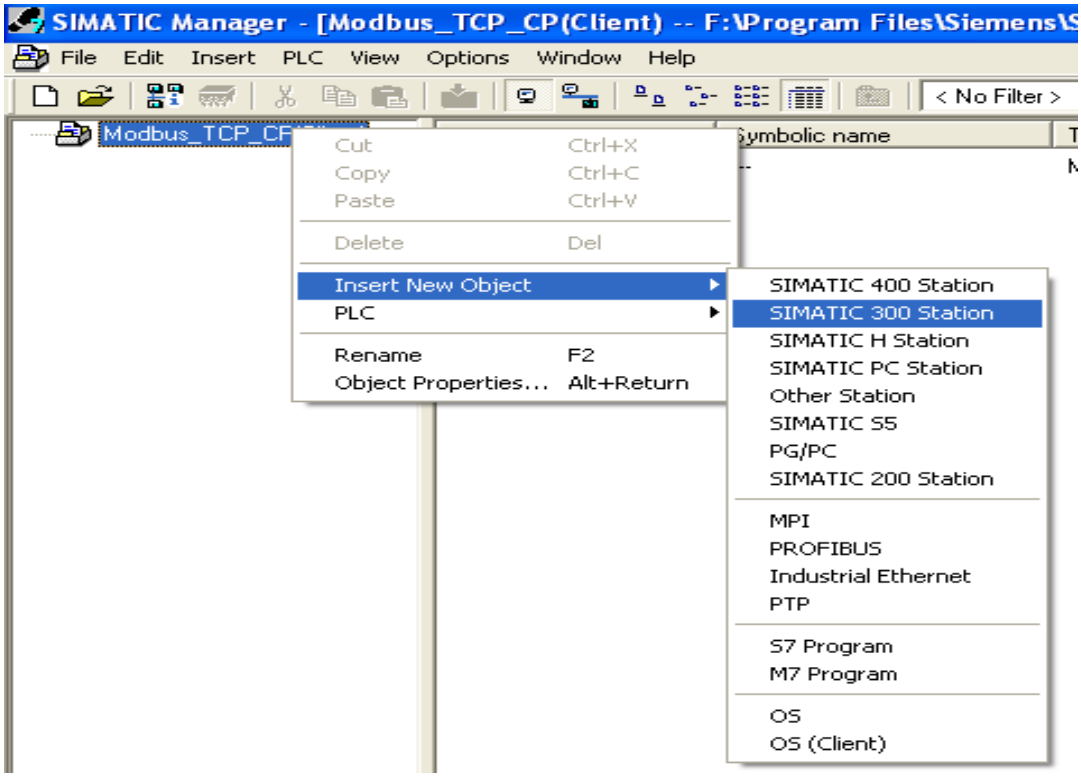
名称	数量	订货号
S7-300 电源模块 PS 307 5A	1	6ES7307-1EA00-0AA0
S7-300 CPU319-3PN/DP	1	6ES7319-3EL00-0AB0(V2.8)
S7-300 CP343 Lean	1	6GK7343-1CX00-0XE0
S7-300 机架	1	6ES7390-1AF30-0AA0
网线及 Profibus 电缆	若干	
笔记本电脑	1	

所用到软件如下表:

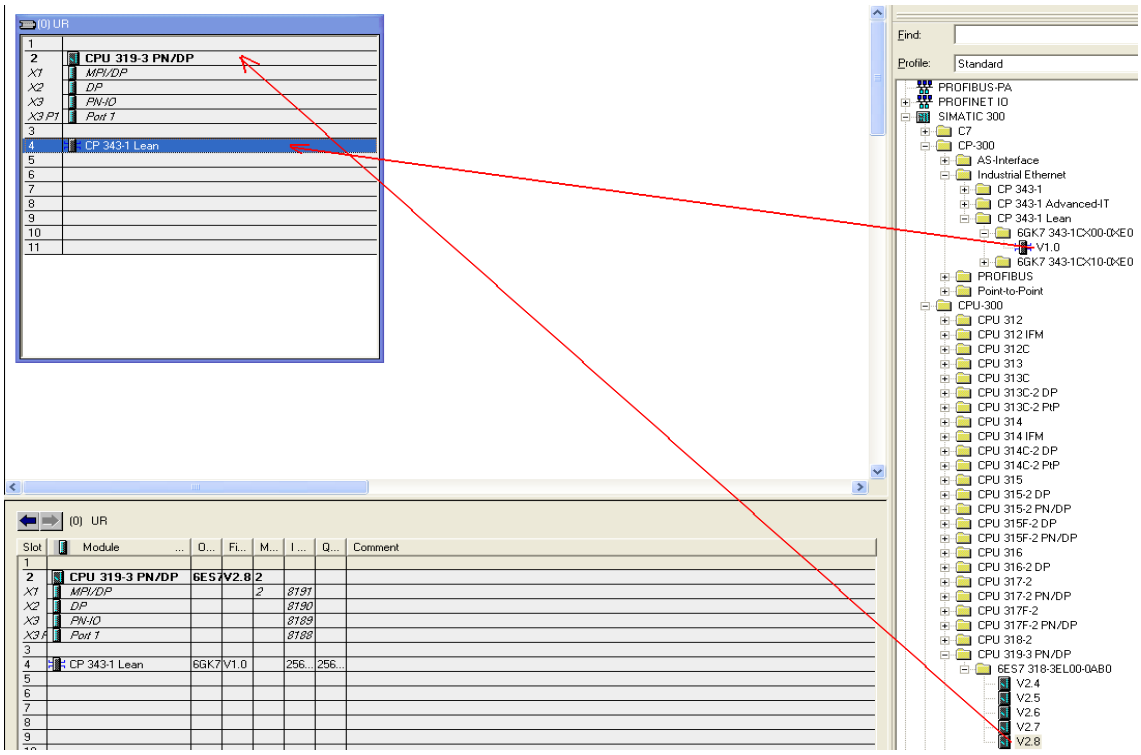
名称	订货号
STEP7 V5.4 组态编程软件 英文版	
Modbus Slave V4.4.1	

4.2 通过 Step7/HW 及 Modbus Slave 软件组态

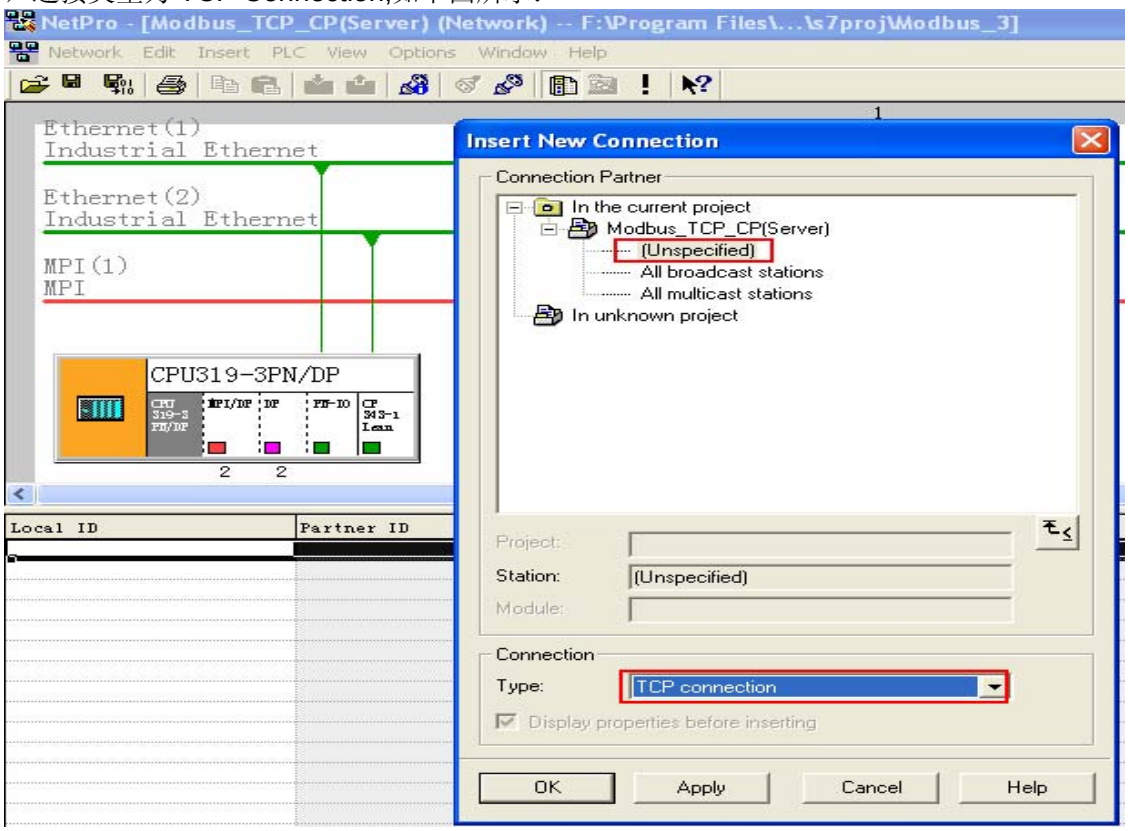
打开 Step7 软件，新建一个工程项目文件，命名为“Modbus_TCP_CP(Client)”, 在项目下插入一个 S7-300 站，如下图：



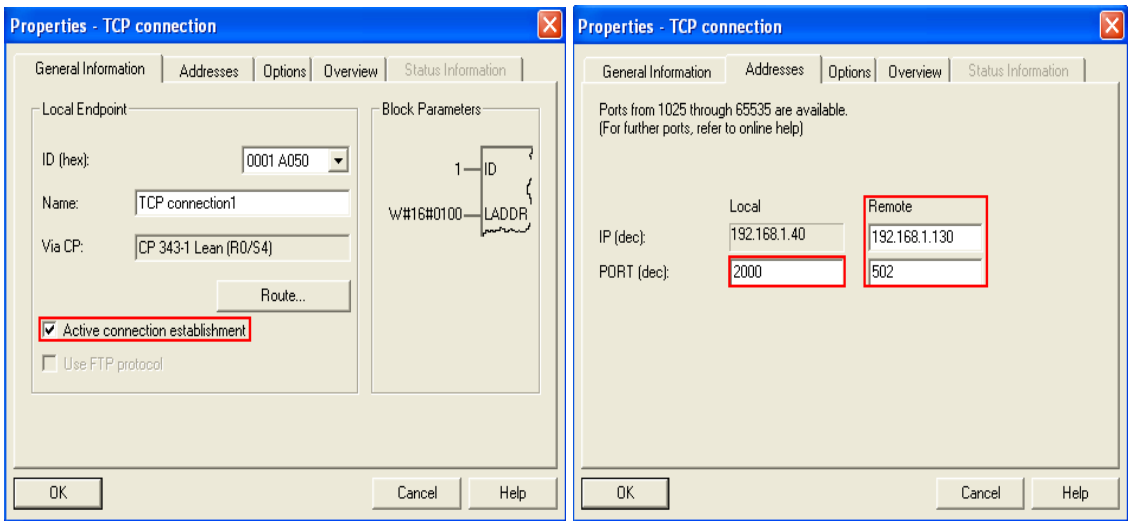
双击插入的 S7-300 站的“Hardware”，打开硬件组态，在硬件组态界面下分别插入机架，电源 PS307,CPU319-3PN/DP，CP343-1 Lean,本例中将 CPU 和 CP 的 IP 地址分别设为 192.168.1.30 及 192.168.1.40，并处在两条不同的网络中，如下图所示：



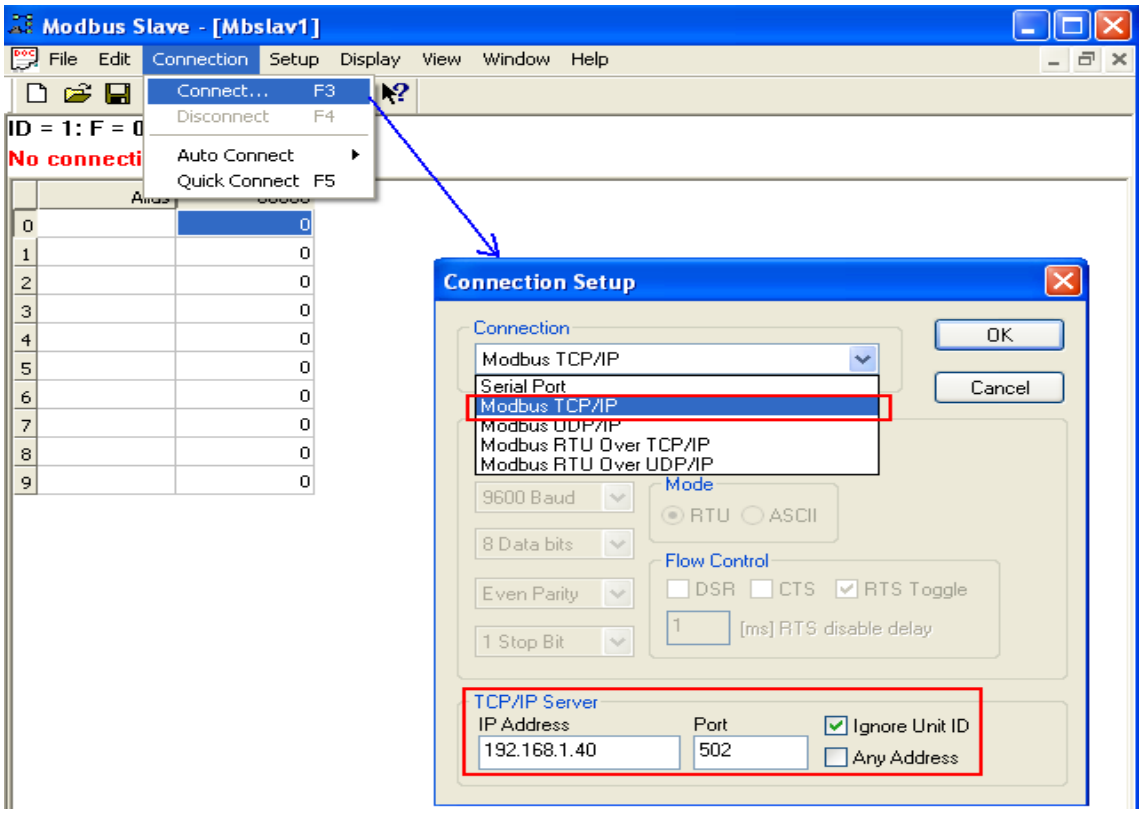
打开 Netpro 网络组态,选中 CPU319-3PN/DP,插入一个新连接，连接伙伴为 Unspecified，连接类型为 TCP Connection,如下图所示：



在打开的连接属性对话框中的“General Information”中由于 CP343-1 做 Client 主动连接，因此勾选“Active connection estabishment”选项,在“Adress”栏的 Local 项中填写 CP343-1 做 Client 的连接资源端口(**一般从 2000 以外开始以避免与别的协议资源冲突**)，在 Remote 栏由于是使用 Modbus Slave PC 测试软件为 Server，因此 IP Adreess 为 PC 机的 IP 地址(本例中为 192.168.1.130)，连接的 Port 号为 502，如下图所示：



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”及“Any Adress”选项，如下图所示：

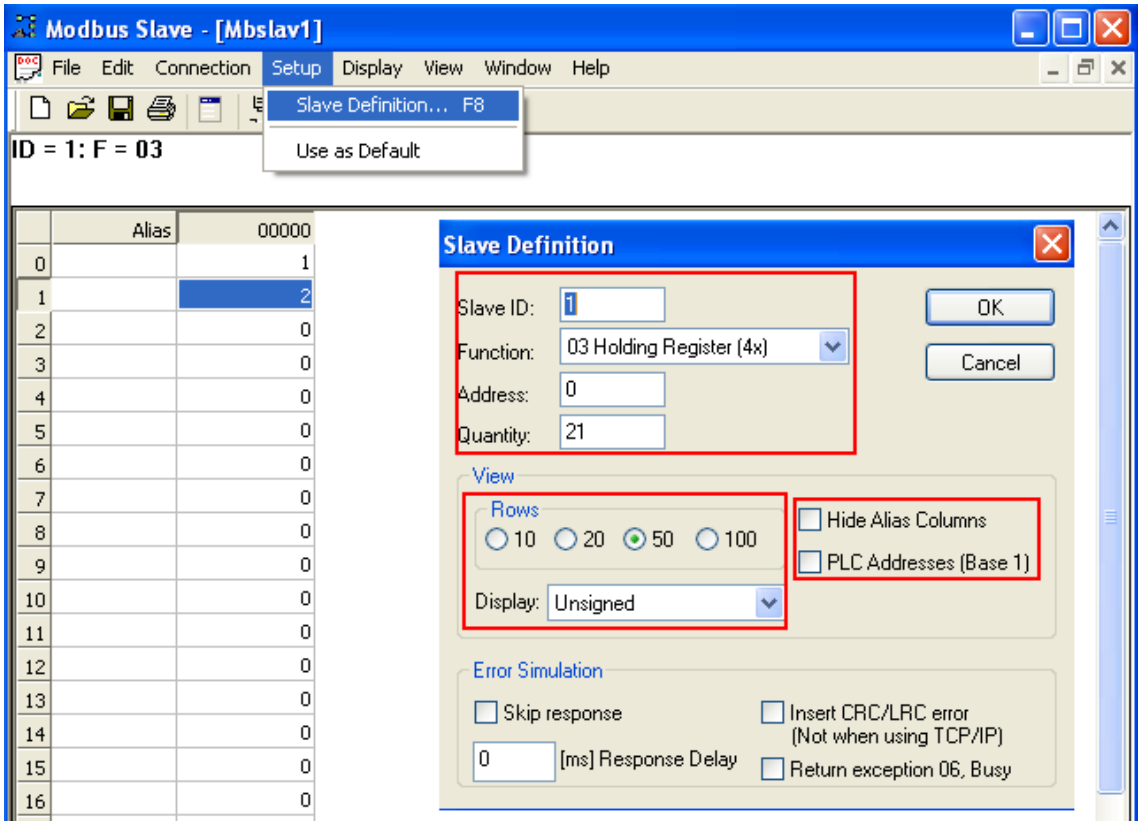


（说明-“**Ignore Unit ID**”及“**Any Adress**”选项的含义如下：
Ignore Unit ID-在一些厂商的 PLC 的程序或网关忠可能会用到 Unit ID 以指定处理类型
Any Adress-确认 Modbus Slave 是否侦听网络中任何 IP 地址还是指定的 IP 地址）

4.3 FB100(FB MODBUS)读写保持寄存器通讯测试

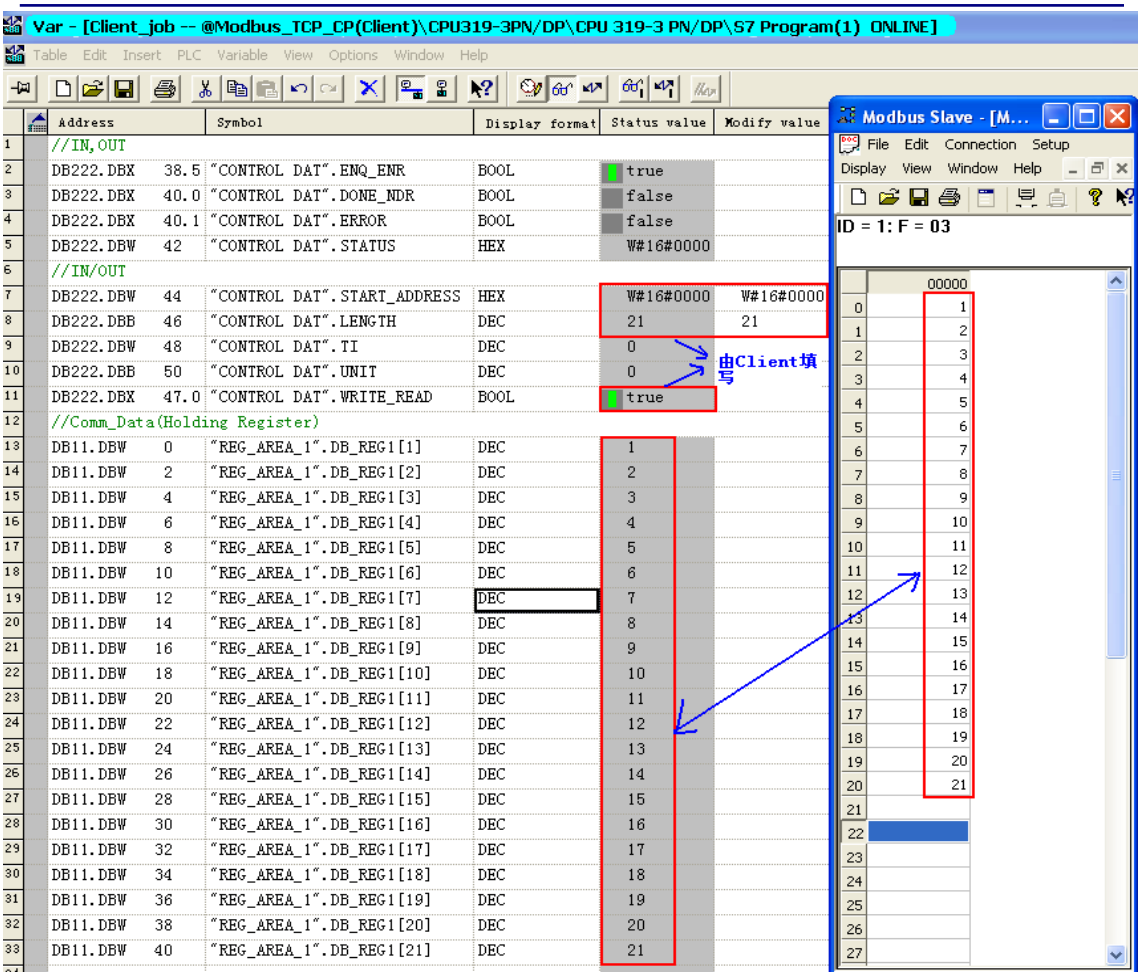
由于也是同样调用 FB100 (FB MODBUS),因此相关参数及 SIMATIC S7 DB 区与 Modbus 寄存器的地址偏移关系请参考 3.3 章节的说明。

下载网络组态及程序到 CPU 中，使能参数 ENQ_ENR=1，在 Modbus Slave 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”、“Return Exception 06,Busy”选项，如下图所示：



(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)

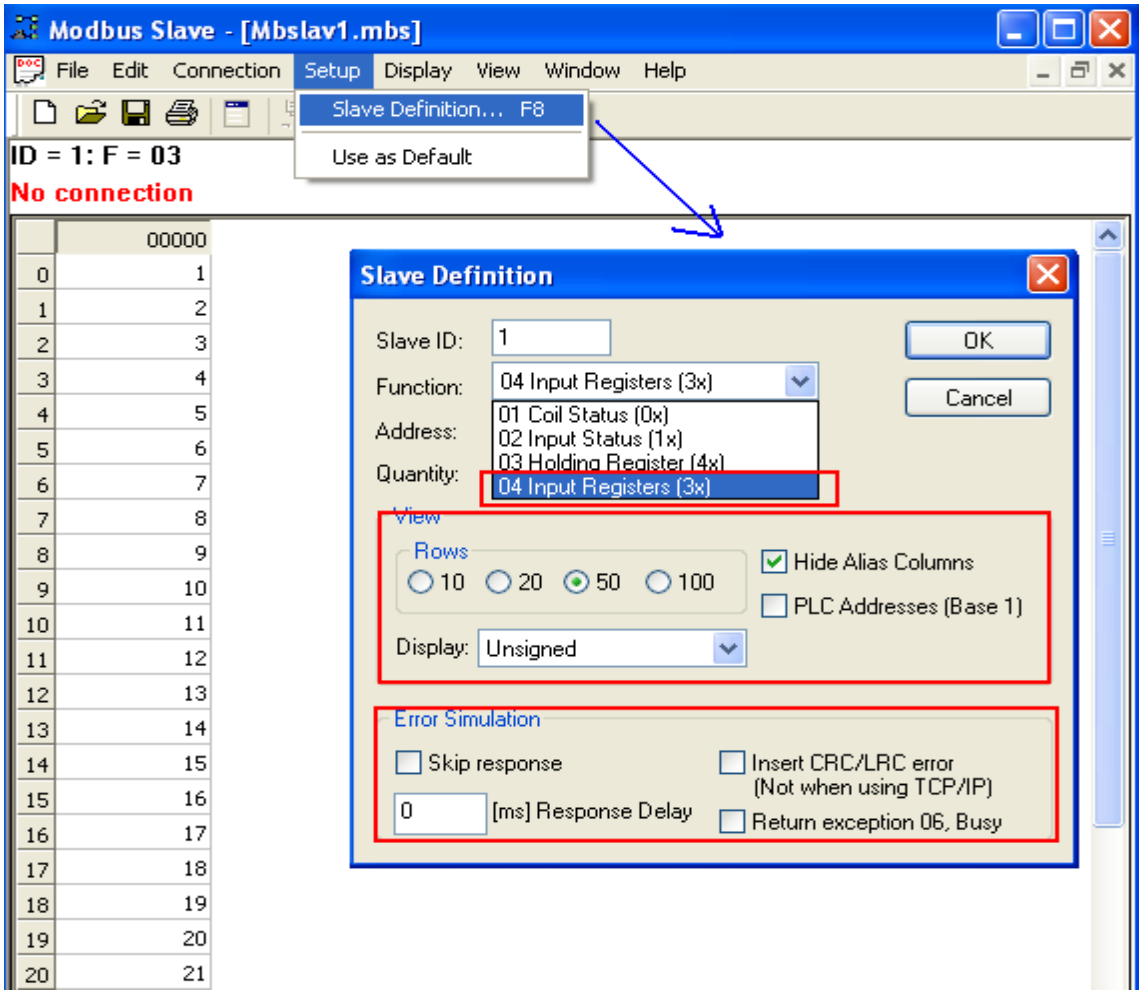
在 Step7 的项目程序中新建一个变量监控表，插入需要监控的参数和数据区变量，可以看到 Modsbus Slave 软件与 CP343-1 的数据通讯已经建立起来了，双方可以进行正常的保持寄存器数据读写操作，如下图所示：



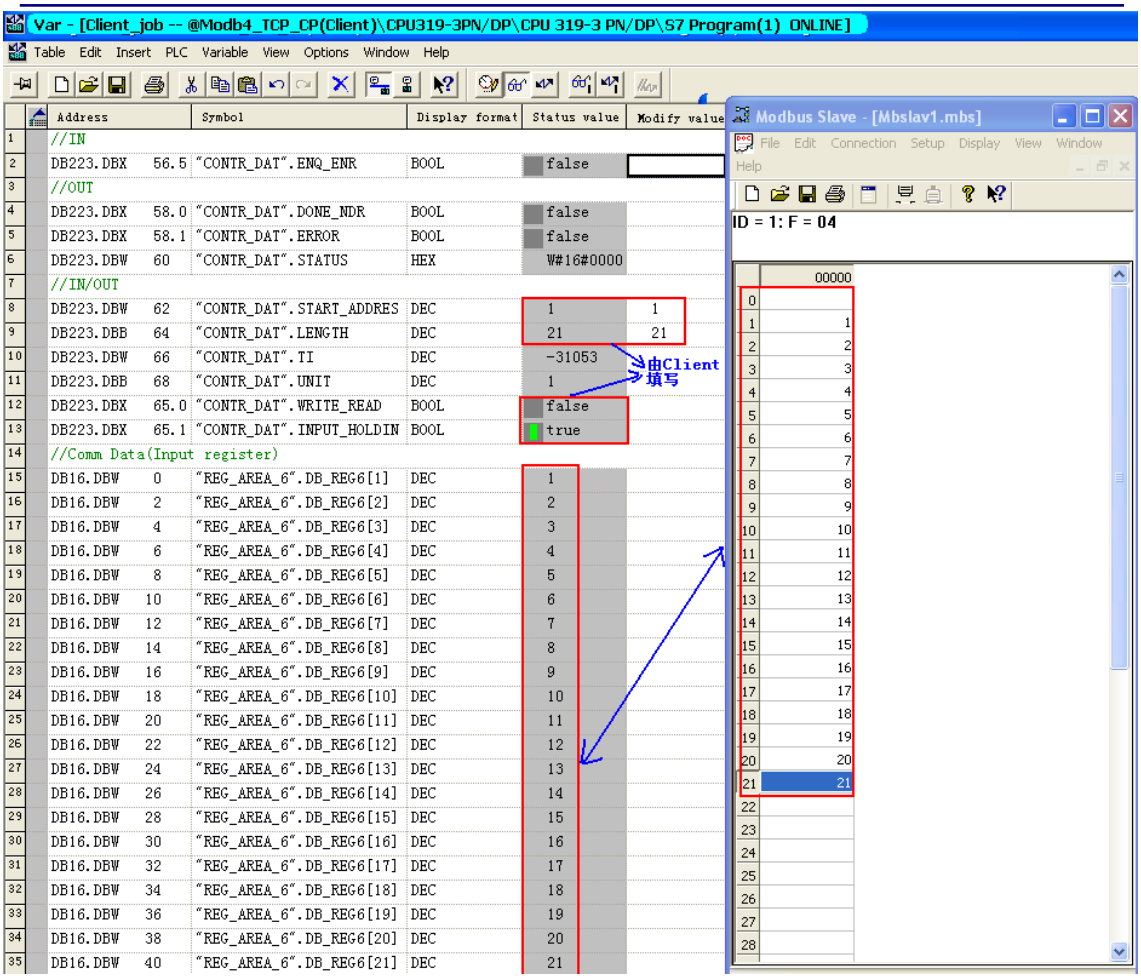
4.4 FB101(FB MODB4)读输入寄存器通讯测试

FB101 的相关参数说明请参考 V3.4 章节的说明。

打开 Modbus Slave 软件，在 Modbus Slave 的“Set up->Slave Definition“中进行相关参数设置(参考 V4.3 章节说明)，此时应该将寄存器的类型选择为输入寄存器“Input Regidter(3x) ”，如下图所示:



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 CP343-1 的数据通讯已经建立起来了，双方可以进行正常的输入寄存器数据读取操作，如下图所示：



5 CP 进行 Modbus TCP 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 CP343-1 进行 Modbus TCP 通讯，因此在实际的第三方设备与 CP343-1 进行通讯时需要注意以下几点：

1) 由于订货号 2XV9450-1MB00 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

更多关于通过 CP343-1 或 CP443-1 进行 Modbus TCP 通讯的详细信息请参考以下连接中的文档：

http://support.automation.siemens.comCNllisapi.dllcsfetch22660304Open_Modbus_TCP_for_NCM_CP_English.pdffunc=cslib.csFetch&nodeid=29522835

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 CP 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
	FB MODBUS 故障	
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: (END_x – START_x + 1)　2 其他可能的原因: ·参数初始化错误(CP 为 Client 时) ·客户端请求报文时错误的地址区域(CP 为 Server)	扩展 DB 区域 当 CP 为 Client 时,修改参数 START-ADRESS 或者 LENGTH 当 CP 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INPUT_HOLDING 及 WRITE_READ 均被置1，不可能对输入寄存器进行写操作	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,0-125 用于读,1-100 用于写	CP 为 Client 时： 修改参数 LENGTH CP 为 Server 时： 修改 Client 请求的寄存器号
A006	DB1-DB8 中对应的寄存器地址范围不存在	CP 为 Client 时： 修改参数 START-ADRESS 或者 LENGTH CP 为 Server 时： 修改 Client 请求或修改参数 DB_x
A007	CP 为 Client 时： 参数MONITOR监控时间设置无效，范围为1-999	修改参数 MONITOR
A008	接收监控超时,可能的原因： 连接未建立或通讯伙伴为准备好	检查通讯伙伴的参数设置
A009	非 0 的协议标识符被接收或者当 CP 为 Client 时,接收标识符 TI 与发送不一致,该故障也指示数据同步失败，可能在 CPU 重起时发生	修正通讯伙伴的报文，当 CP 为 Server 时确保参数 MONTIOR 的监控时间不超过 Client 的监控时间
A00A	CP 为 Client 时： 接收参数 UNIT 与发送的不一致	检查通讯伙伴的参数设置
A00B	CP 为 Client 时： 接收与发送功能码不一致 CP 为 Server 时： 无效的功能码被接收	CP 为 Client 时： 检查通讯伙伴的数据报文格式 CP 为 Server 时： 注意 FB MODBUS 仅支持功能码 FC03、16;FB MODB4 支持功能码 FC03、04、16
A00C	接收到的字节长度与寄存器号不	检查通讯伙伴的数据报文格式

	匹配	
A00D	仅在 CP 为 Client 时发生: 响应的 MODBUS 寄存器地址于请求的不一致	检查通讯伙伴的数据报文格式
A00E	MODBUS 报文报头的长度与寄存器号　不匹配	检查通讯伙伴的数据报文格式
A00F	仅在 CP 为 Server 时发生： 尝试给一个带写保护的区域写值	修改客户端的请求或禁止写保护
A010	参数 DB1-DB8 中有重复使用的 DB 块	修改为单独的 DB
A01A	数据被破坏或者报头中错误的长度： 字节 4 的前缀不等于 0	检查通讯伙伴的数据报文格式
A01B	仅在 CP 为 Client 时发生: 额外的功能码 FC01 被接收	通讯伙伴不支持该功能请求
A01C	仅在 CP 为 Client 时发生: 额外的功能码 FC02 被接收	修改参数 START-ADRESS 或者 LENGTH
A01D	仅在 CP 为 Client 时发生: 未知的功能码被接收	检查通讯伙伴的数据报文格式
A01E	CP 接收了无效的数据，数据同步失败	检查通讯伙伴的数据报文格式
A012	DB1 与 DB2 中出现寄存器地址叠加	统一类型的寄存器地址不能有叠加情况
A013	DB1 与 DB3 中出现寄存器地址叠加	
A014	DB1 与 DB4 中出现寄存器地址叠加	
A015	DB1 与 DB5 中出现寄存器地址叠加	
A023	DB2 与 DB3 中出现寄存器地址叠加	
A024	DB2 与 DB4 中出现寄存器地址叠加	
A025	DB2 与 DB5 中出现寄存器地址叠加	
A034	DB3 与 DB4 中出现寄存器地址叠加	
A035	DB3 与 DB5 中出现寄存器地址叠加	
A045	DB4 与 DB5 中出现寄存器地址叠加	
A067	DB6 与 DB7 中出现寄存器地址叠加	
A068	DB6 与 DB8 中出现寄存器地址叠加	

A078	DB7 与 DB8 中出现寄存器地址叠加	
FC/SFC 故障		
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
8186	ID 参数无效 当在 OB1 及 FB100 中使用同一 ID 号不同的背景 DB 多次调用 FB MODBUS/MODB4 时也会产生该故障	确保 Netpro 中的一个 ID 号只能用于 FB MODBUS/MODB4 的一次调用
SFC24 故障		
80A1	DB=0 或超出了 CPU 允许的范围	选择有效的 DB
80A2	DB 块在 CPU 中不存在	DB_x 参数中的 DB 块必须创建并下载到 CPU 中
80A3	DB 块被创建为“Unlinked”类型	DB 块不能创建为“Unlinked”类型

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/10805868/130000
"找答案"Net版区：http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1031

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。