SIEMENS

操作指南 • 12/2017

基于 S7-300/400 CPU 集成 PN 接口的 Modbus TCP 在 STEP7 的使用入门（V3.0）

https://support.industry.siemens.com/cs/cn/zh/view/109753995

Unrestricted

Copyright © Siemens
AG Copyright year
All rights reserved

目录

Copyright © Siemens
AG Copyright year
All rights reserved

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 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 地址报文包。

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 (Modbus Application Protocol)分 4 个域，共 7 个字节。

Copyright © Siemens AG Copyright year All rights reserved

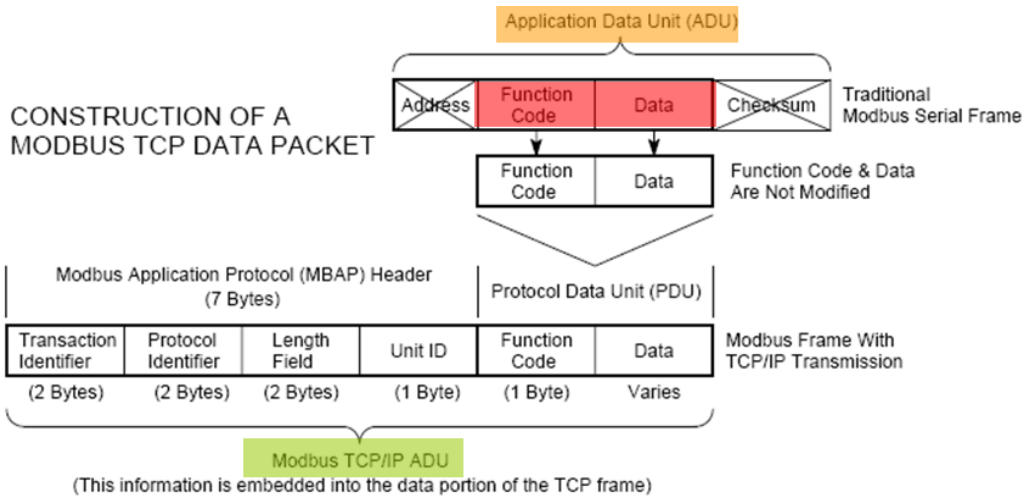

图 1-1 MBAP 报文头

域	长度	描述	客户机	服务器
Transaction ID	2字节	Modbus请求/响应事务处理的识别	客户机启动	服务器从接收的请求中重新复制
Protocol ID	2字节	0=Modbus协议	客户机启动	服务器从接收的请求中重新复制
Length	2字节	随后字节的数量	客户机启动（请求）	服务器（响应）启动
Unit ID	1字节	远程从站的识别ID	客户机启动	服务器从接收的请求中重新复制

图 1-2 MBAP 报文头说明

1.3 Modbus TCP 使用的端口号

（1） PLC 作为 Modbus 服务器时，按缺省协议使用 Port 502 通信端口，在 Modus 客户端程序中设置任意通信端口，

（2） PLC 作为 Modbus 客户端时，无须设置本机端口号；如要指定客户端端口号，为避免与其他通讯协议的冲突一般建议 2000 开始可以使用。

Copyright © Siemens AG Copyright year All rights reserved

2 S7-300/400 集成 PN 口 Modbus TCP 通讯概述

本文适用于带有集成 PN 接口的 SIMATIC S7-300、S7-400 CPU 和 IM 151-8 PN/DP CPU 的软件产品。相关指令允许在带有集成 PN 接口的 SIMATIC CPU 和支持 Modbus TCP 协议的设备之间进行通信。

根据客户端——服务器原理进行数据传输。传输过程中，可以将 SIMATIC S7 用作客户端，也可以用作服务器。

2.1 软件和硬件

在 STEP7 软件中使用 Modbus TCP 的指令，需要安装 MODBUS TCP PN-CPU 指令库，才可将 SIMATIC S7-300、S7-400 CPU 和 IM 151-8 PN/DP CPU 与支持 Modbus TCP 的通信伙伴进行通信，如下图 2-1 所示：

Product	Identification number	as of version
MODBUS/TCP PN CPU	6AV6676-6MB20-3AX0	3.0
FB 900 "MODBUSPN"		4.0
FB 901 "MOD_CLI"		2.0
FB 903 "MOD_SERV"		2.0

图 2-1 指令版本

下面例子将分别介绍如何配置 315-2PN/DP 为 Modbus TCP 的 Server，Client 与通信伙伴建立通信，测试例程中用到的软硬件如图 2-2 所示：

名称	数量	订货号
SIMATIC CPU315-2PN/DP(FW V3.2)	1	6ES7 315-2EH14-0AB0
SIMATIC STEP7 V5.6	1	6ES7 822-4CC11-0YA5
Modbus TCP PN-CPU software	1	6AV6 676-6MB20-3AX0
Modscan32 用于在 PC 中模拟 Modbus Client	1	网上免费下载
Modsim32 用于在 PC 中模拟 Modbus Server	1	网上免费下载

图 2-2 例程中用到的软硬件列表

2.2 Modbus TCP PN-CPU V3.0 软件选项包

当将软件包安装完集成到 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包

Copyright © Siemens AG Copyright year All rights reserved

“Modbus TCP PN-CPU V3.0”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 projects in "\Program Files\Siemens\Step7\Examples"
- the manual in "\Program Files\Siemens\Step7\S7manual\S7Comm"

图 2-3 块库、例程、英文手册的文件夹位置

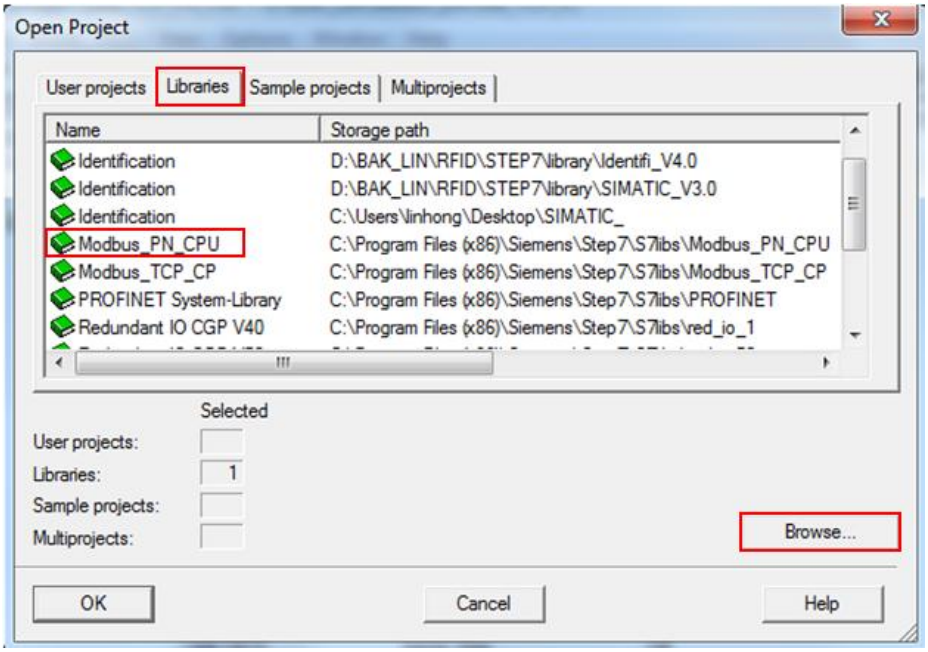

图 2-4 指令库(注：当找不到块库时，可以通过”Browse..”按钮来进行查找)

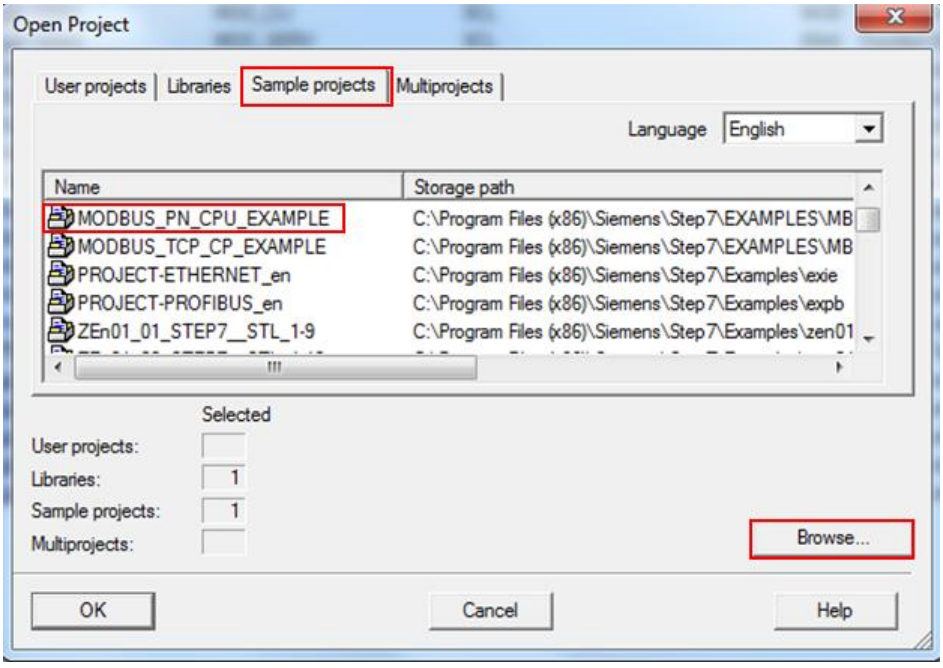

图 2-5 例程(注：当找不到例程时，可以通过”Browse..”按钮来进行查找)

Copyright © Siemens AG Copyright year All rights reserved

3 配置 PN CPU 作为 Modbus TCP Server 与通信伙伴建立通讯

下面以 S7-300 单站系统及 Modscan32 软件为例，详细介绍如何将 S7-300 单站系统通过 CPU 集成 PN 口配置为 Modbus TCP Server，Modscan32 为 Client 进行 Modbus TCP 通讯。

3.1 组态硬件

在 STEP7 中创建一个新项目（项目名称：MB_TCP_PN_V30），如图 3-1 所示：

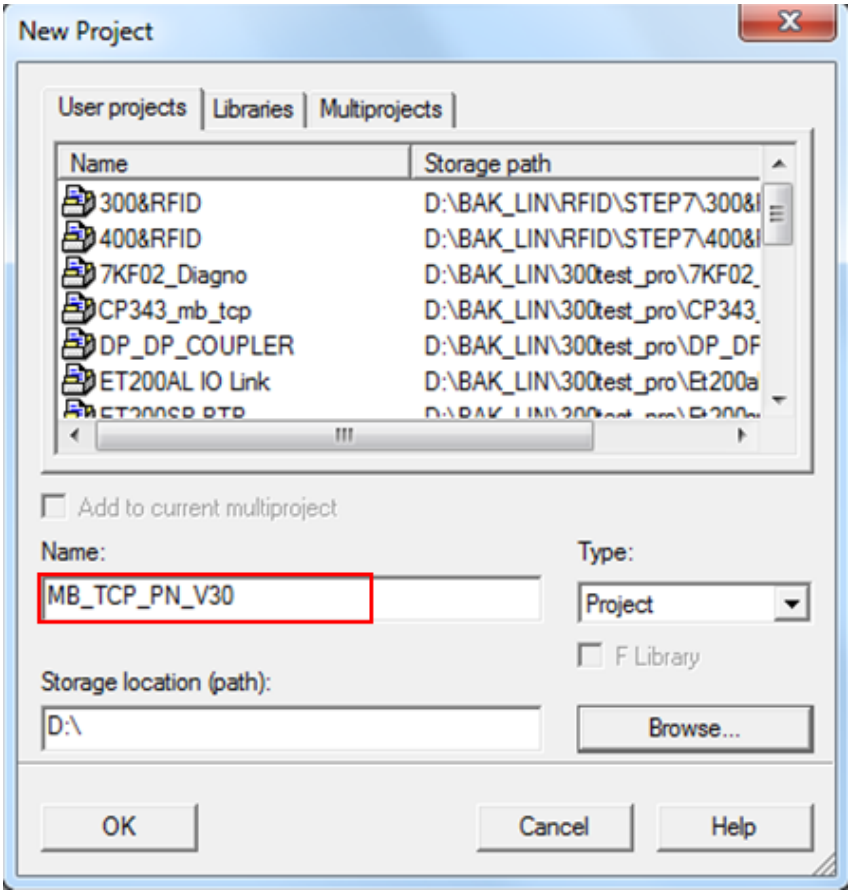

图 3-1 创建新项目

然后，插入一个新的“SIMATIC 300 Station”，如图 3-2 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

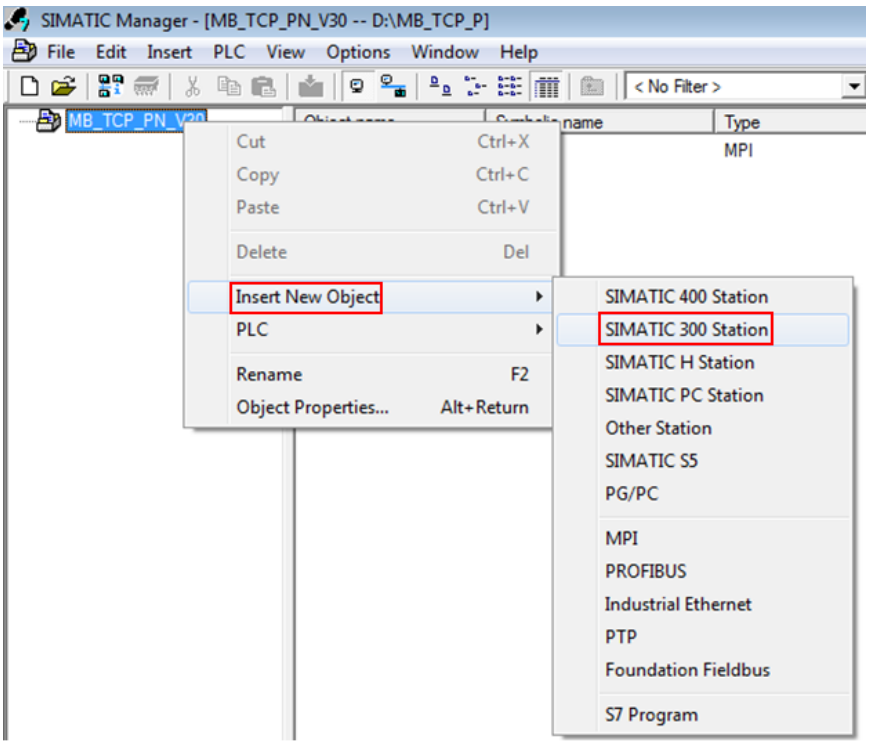

图 3-2 插入 PLC 站点

接着，打开硬件组态视图，插入 CPU 315-2PN/DP ，设置 IP 地址，如图 3-3 所示：

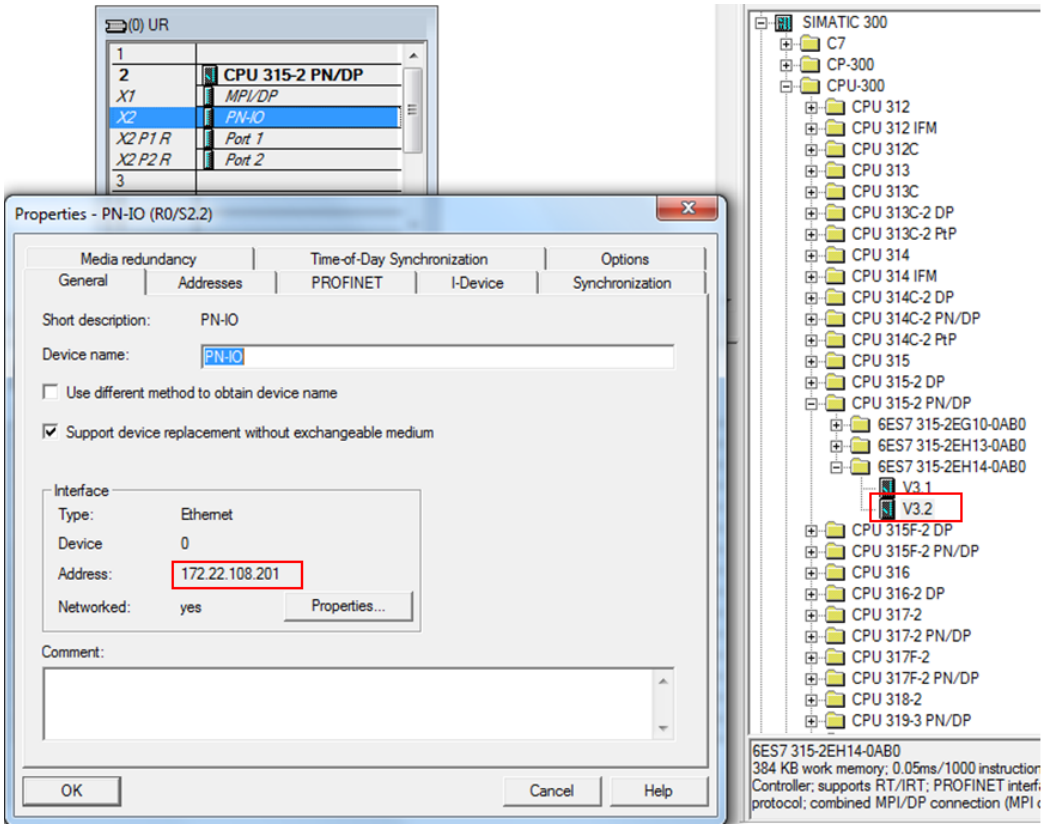

图 3-3 硬件组态

Copyright © Siemens AG Copyright year All rights reserved

3.2 例程说明

打开例程，从站点“SIMATIC 300（Server）”中拷贝所有程序块（注意，不要拷贝“System data”）到新建项目“MB_TCP_PN_V30”的站点“SIMATIC 300（1）”的 Blocks 中，如图 3-4 所示：

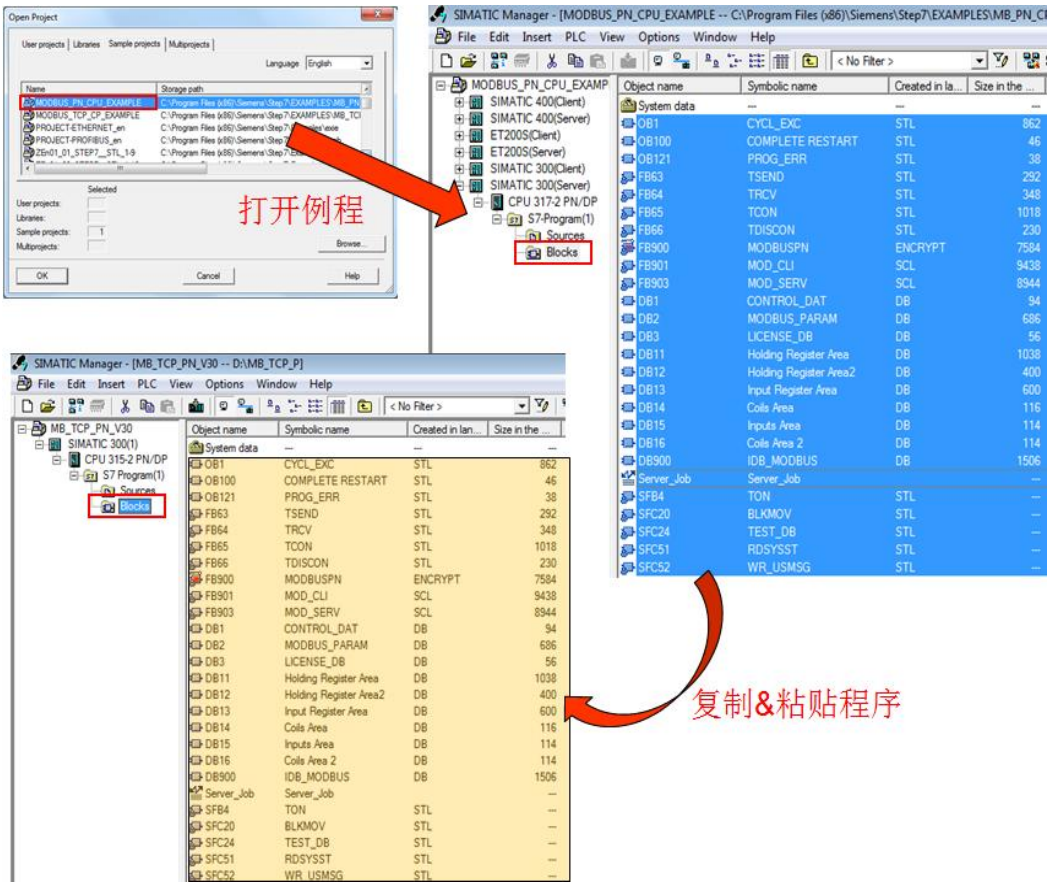

图 3-4 拷贝例程程序

（1）打开 OB1，查看指令“MODBUSPN”

在项目的 OB1 组织块中调用了 Modbus TCP 指令，如图 3-5 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

```
OB1 :  "Main Program Sweep (Cycle)"
Comment:
Network 1: cyclic call of FB MODBUSPN - S7 is server
      L     1
      T     "CONTROL_DAT".ID                          DB1.DBW0

      L     T#500MS
      T     "CONTROL_DAT".RECV_TIMEOUT                DB1.DBD2

      L     T#5S
      T     "CONTROL_DAT".CONN_TIMEOUT                DB1.DBD6

      CALL  "MODBUSPN" , "IDB_MODBUS"                 FB900 / DB900
       id              :="CONTROL_DAT".ID             DB1.DBW0
       db_param        :="MODBUS_PARAM"               DB2
       REG_KEY_DB      :="LICENSE_DB"                 DB3
       RECV_TIMEOUT    :="CONTROL_DAT".RECV_TIMEOUT   DB1.DBD2
       CONN_TIMEOUT    :="CONTROL_DAT".CONN_TIMEOUT   DB1.DBD6
       DISCONNECT      :="CONTROL_DAT".DISCONNECT     DB1.DBX10.0
       ENQ_ENR         :="CONTROL_DAT".ENQ_ENR        DB1.DBX10.1
       LICENSED        :="CONTROL_DAT".LICENSED       DB1.DBX10.2
       CONN_ESTABLISHED:="CONTROL_DAT".CONN_ESTABLISHED DB1.DBX10.3
       BUSY            :="CONTROL_DAT".BUSY           DB1.DBX10.4
       DONE_NDR        :="CONTROL_DAT".DONE_NDR       DB1.DBX10.5
       ERROR           :="CONTROL_DAT".ERROR          DB1.DBX10.6
       STATUS          :="CONTROL_DAT".STATUS         DB1.DBW12
       STATUS_FUNC     :="CONTROL_DAT".STATUS_FUNC    P#DB1.DBX14.0
       IDENT_CODE      :=
       Init_Error      :="CONTROL_DAT".Init_Error     DB1.DBX30.2
       Init_Status     :="CONTROL_DAT".Init_Status    DB1.DBW32
       UNIT            :="CONTROL_DAT".UNIT           DB1.DBB24
       DATA_TYPE       :="CONTROL_DAT".DATA_TYPE      DB1.DBB25
       START_ADDRESS   :="CONTROL_DAT".START_ADDRESS  DB1.DBW26
       LENGTH          :="CONTROL_DAT".LENGTH         DB1.DBW28
       WRITE_READ      :="CONTROL_DAT".WRITE_READ     DB1.DBX30.0
       Init            :="CONTROL_DAT".Init           DB1.DBX30.1
```

图 3-5 调用 Modbus TCP 指令

以下为部分管脚说明（其它管脚信息请查看指令库手册）：

id：连接 ID 必须与参数 DB 中相关的 id 参数相同。

db_param：参数 DB 块，包含此 modbus 块实例的连接参数和 modbus 数据参数。CPU 决定该参数的取值范围。DB 编号 0 为系统保留，不允许使用。以纯文本格式输入 DB 编号“DBxy”。

REG_KEY_DB：具有可用于授权的注册表项的数据块。

RECV_TIMEOUT：对从耦合伙伴接收数据进行监视。超出监视时间后，将发出错误信号并终止连接。 最小值为 20 ms。

在“S7 为服务器”模式下将 RECV_TIMEOUT 设置为 < 20 ms，则使用默认值 1.2 s。RECV_TIMEOUT 监视 TCP 流的运行系统。不考虑各个客户端请求之间的中断。

Copyright © Siemens AG Copyright year All rights reserved

CONN_TIMEOUT：监视调用建立或终止所用的时间。如果在组态的监视时间内无法成功建立或终止连接，则会在输出 STATUS 中显示相应的错误消息。最小值为 100 ms。

在“S7 为服务器”模式下，如果将 CONN_TIMEOUT 设置为 < 100 ms，则会使用默认值 5 s。

Init：在参数中有上升沿时，初始化 Modbus 块。只有当前没有作业正在运行时，才能执行初始化。必须通过 ENQ_ENR = FALSE 和 BUSY = FALSE 在程序中确保此条件。

（2）参数数据块 DB2

参数数据块 DB2（名称 MODBUS_PARAM），该参数 DB 块可分为两部分理解，偏移量 0~63 字节为 TCP 连接参数的设置区域，偏移量 64~129 为 modbus 数据区域的设置。

注意，如需修改 DB 块中的数据，请将 DB 块切换到数据视图“Data view”，在“Actual value”列中进行修改，如图 3-6 所示：

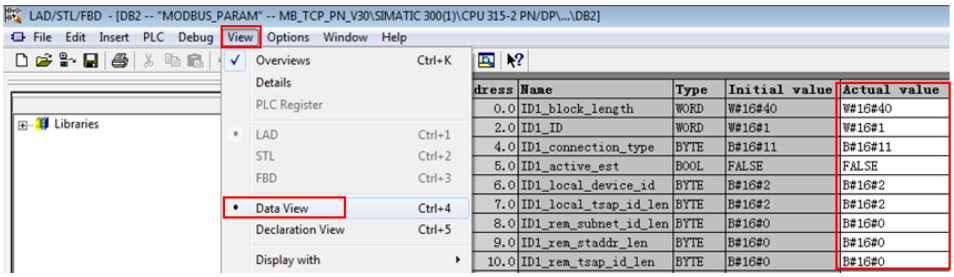

图 3-6 将 DB 块切换到数据视图

①TCP 连接参数的设置，如图 3-7 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

Address	Name	Type	Initial value
0.0		STRUCT	
+0.0	ID1_block_length	WORD	W#16#40
+2.0	ID1_ID	WORD	W#16#1
+4.0	ID1_connection_type	BYTE	B#16#11
+5.0	ID1_active_est	BOOL	FALSE
+6.0	ID1_local_device_id	BYTE	B#16#2
+7.0	ID1_local_tsap_id_len	BYTE	B#16#2
+8.0	ID1_rem_subnet_id_len	BYTE	B#16#0
+9.0	ID1_rem_staddr_len	BYTE	B#16#0
+10.0	ID1_rem_tsap_id_len	BYTE	B#16#0
+11.0	ID1_next_staddr_len	BYTE	B#16#0
+12.0	ID1_local_tsap_id	ARRAY[1..16]	B#16#1, B#16#F6
*1.0		BYTE	
+28.0	ID1_rem_subnet_id	ARRAY[1..6]	6 (B#16#0)
*1.0		BYTE	
+34.0	ID1_rem_staddr	ARRAY[1..6]	6 (B#16#0)
*1.0		BYTE	
+40.0	ID1_rem_tsap_id	ARRAY[1..16]	16 (B#16#0)
*1.0		BYTE	
+56.0	ID1_next_staddr	ARRAY[1..6]	6 (B#16#0)
*1.0		BYTE	
+62.0	ID1_spare	WORD	W#16#0

图 3-7 TCP 连接参数的设置

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID1_ID：每个 PN CPU 与通信伙伴之间的连接都需要一个连接 ID。如果有多个通信伙伴，则每个逻辑连接会使用不同的连接 ID。该连接 ID 在参数数据块中包含的“连接参数块”中组态。连接 ID 唯一地描述 CPU 与链接伙伴之间的连接，取值范围为 1 到 4095。必须在此处输入参数块中的连接 ID；该 ID 在整个 CPU 中必须唯一。

ID1_connection_type：建立连接的连接类型通过 TCON 指令定义。CPU 决定必须要设置的值。

TCP（兼容模式）：B#16#01，针对 CPU 315 或 317 <= FW V2.3 。

TCP：B#16#11，针对 CPU 315 或 317 >= FW V2.4、IM 151-8 PN/DP CPU、CPU314C、CPU319、CPU412、CPU414 和 CPU416。

ID1_active_est：该参数表示连接建立类型，主动或被动。Modbus 客户端负责建立主动连接而 Modbus 服务器负责建立被动连接。

主动连接的建立：TRUE

被动连接的建立：FALSE

ID1_local_device_id：定义所用 PN CPU 的 IE 接口。根据不同的 PN CPU 类型，需要不同的设置。

Copyright © Siemens
AG Copyright year
All rights reserved

CPU 类型	local_device_id
IM 151-8 PN/DP CPU	B#16#1
CPU 314C、315 或 317	B#16#2
CPU 319	B#16#3
CPU 412、414 或 CPU 416	B#16#5

ID1_local_tsap_id_len：参数 ID1_local_tsap_id（本地端口号）的长度。

主动连接的建立：0

被动连接建立：2

ID1_local_tsap_id：使用该参数设置本地端口号。

表示类型会因 ID1_connection_type 参数不同而有所不同。CPU 决定值范围。端口号在 CPU 中必须唯一。

对于 ID1_connection_type=B#16#01： local_tsap_id[1] local_tsap_id[2] local_tsap_id[3-16]	 用十六进制格式表示的端口号 low byte 用十六进制格式表示的端口号 high byte B#16#00
对于 ID1_connection_type=B#16#11： local_tsap_id[1] local_tsap_id[2] local_tsap_id[3-16]	 用十六进制格式表示的端口号 high byte 用十六进制格式表示的端口号 low byte B#16#00

本例中，CPU 为 315-2PN，connection_type B#16#11，端口号设置为 502（16#01F6），则对应于 local_tsap_id[1]= 16#01，local_tsap_id[2]= 16#F6。

②modbus 数据区域的设置，如图 3-8 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

Address	Name	Type	Initial valu	Comment
+64.0	ID1_server_client	BOOL	TRUE	
+64.1	ID1_single_write	BOOL	FALSE	
+64.2	ID1_connect_at_startup	BOOL	FALSE	
+65.0	ID1_reserved	BYTE	B#16#0	
+66.0	ID1_data_type_1	BYTE	B#16#3	
+68.0	ID1_db_1	WORD	W#16#B	11
+70.0	ID1_start_1	WORD	W#16#0	0
+72.0	ID1_end_1	WORD	W#16#1F3	499
+74.0	ID1_data_type_2	BYTE	B#16#3	
+76.0	ID1_db_2	WORD	W#16#C	12
+78.0	ID1_start_2	WORD	W#16#2D0	720
+80.0	ID1_end_2	WORD	W#16#384	900
+82.0	ID1_data_type_3	BYTE	B#16#4	
+84.0	ID1_db_3	WORD	W#16#D	13
+86.0	ID1_start_3	WORD	W#16#2D0	720
+88.0	ID1_end_3	WORD	W#16#3E8	1000
+90.0	ID1_data_type_4	BYTE	B#16#0	
+92.0	ID1_db_4	WORD	W#16#0	
+94.0	ID1_start_4	WORD	W#16#0	
+96.0	ID1_end_4	WORD	W#16#0	
+98.0	ID1_data_type_5	BYTE	B#16#1	
+100.0	ID1_db_5	WORD	W#16#E	14
+102.0	ID1_start_5	WORD	W#16#280	640
+104.0	ID1_end_5	WORD	W#16#4E2	1250
+106.0	ID1_data_type_6	BYTE	B#16#2	
+108.0	ID1_db_6	WORD	W#16#F	15
+110.0	ID1_start_6	WORD	W#16#6A4	1700
+112.0	ID1_end_6	WORD	W#16#8FC	2300
+114.0	ID1_data_type_7	BYTE	B#16#1	
+116.0	ID1_db_7	WORD	W#16#10	16
+118.0	ID1_start_7	WORD	W#16#6A4	1700
+120.0	ID1_end_7	WORD	W#16#8FC	2300
+122.0	ID1_data_type_8	BYTE	B#16#0	
+124.0	ID1_db_8	WORD	W#16#0	
+126.0	ID1_start_8	WORD	W#16#0	
+128.0	ID1_end_8	WORD	W#16#0	

图 3-8 modbus 数据区域的设置

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID1_server_client：S7 是服务器=TRUE；S7 是客户端=FALSE。

ID1_single_write：在“客户端”操作模式才有效。

ID1_connect_at_startup：如果将 ID1_connect_at_startup 设置为 TRUE，将在 CPU 重新启动后立即建立连接。此种情况下，只有正确建立连接 (CONN_ESTABLISHED = TRUE) 后才能启动数据请求，否则将在 ERROR 和 STATUS 中显示相应的错误。

设置为 FALSE：如果 ENQ_ENR，则连接建立。

设置为 TRUE：重新启动后立即建立连接。

ID1_data_type_x：指定该数据块中映射的 MODBUS 数据类型。如果在 ID1_data_type_x 中输入值 16#0，则不使用相应的区域。

Copyright © Siemens
AG Copyright year
All rights reserved

标识符	数据类型	数据宽度
16#0	未使用区域	
16#1	线圈	Bit
16#2	输入	Bit
16#3	保持寄存器	Word
16#4	输入寄存器	Word

Modbus 数据类型	DATA_TYPE	功能	长度	功能代码
线圈	1	读取	任意	1
线圈	1	写入	1	5
线圈	1	写入	1	15
线圈	1	写入	> 1	15
输入	2	读取	任意	2
保持寄存器	3	读取	任意	3
保持寄存器	3	写入	1	6
保持寄存器	3	写入	1	16
保持寄存器	3	写入	> 1	16
输入寄存器	4	读取	任意	4

图 3-9 不同的数据类型与 modbus 功能代码的关系

ID1_db_x：指定映射 MODBUS 寄存器或下面定义的位值的数据块。DB 编号 0 为系统保留，不允许使用。

DB 编号：1 到 65535（W#16#0001 到 W#16#FFFF）。

ID1_start / end_x：start 指定 DB 的数据字 0 中映射的第一个 Modbus 地址。end 参数定义最后一个 MODBUS 地址。

对于寄存器访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字编号如下计算：DBW 编号 = (end – start) * 2

对于位访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字节编号如下计算：DBB 编号 = (end – start + 7) / 8

定义的数据区不得重叠。end 参数不得小于 start。如果发生错误，指令启动将中止并提示错误。如果两个值相同，则将分配一个 Modbus 地址（1 个寄存器或 1 个位值）。

Copyright © Siemens AG Copyright year All rights reserved

注意：数据块必须比已组态数据所需的长度多两个字节。最后的两个字节供内部使用。

例程中设置的 DB 块和 modbus 地址的对应关系，如图 3-10 所示：

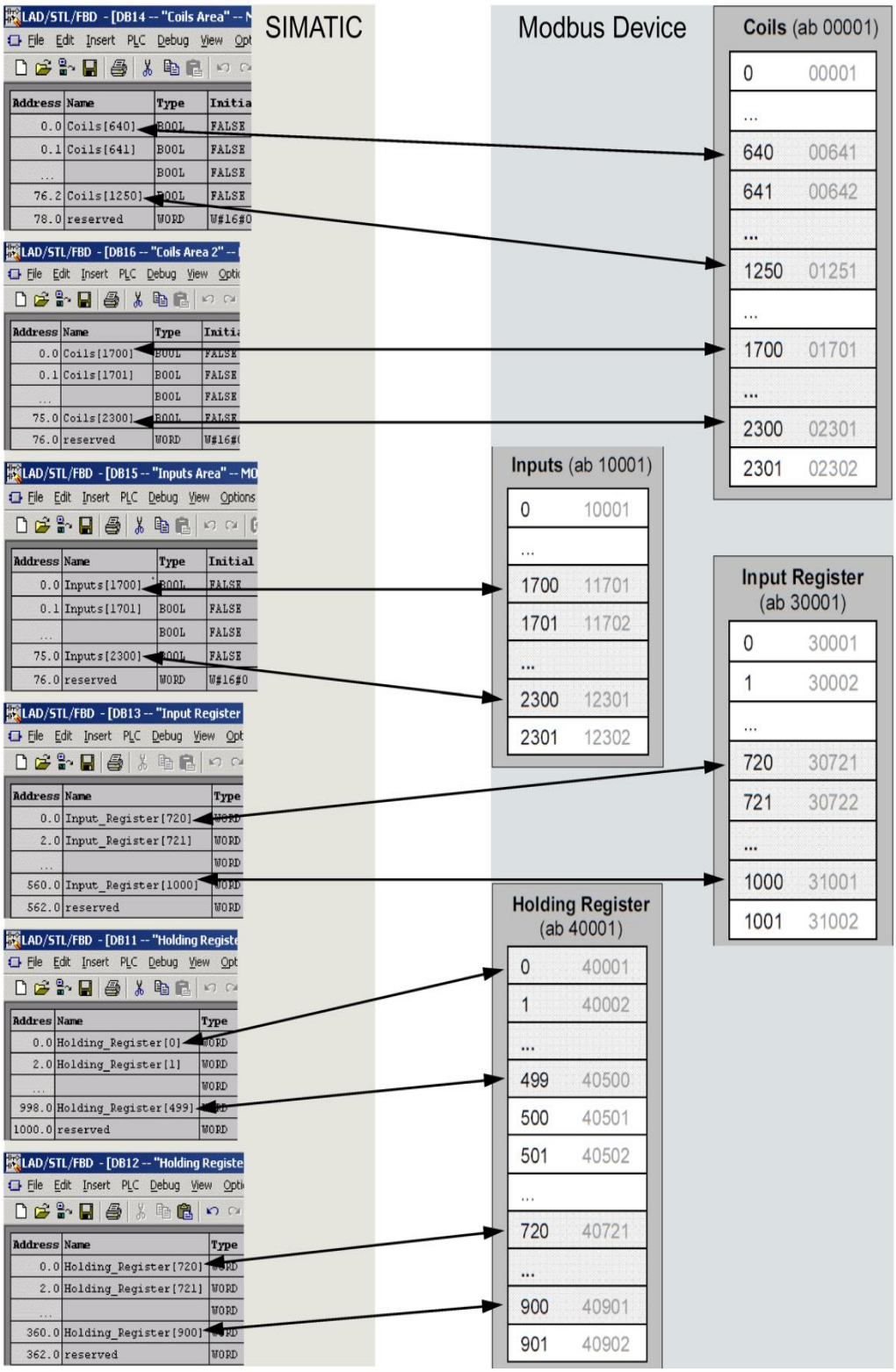

图 3-10 DB 块和 modbus 地址的对应关系

Copyright © Siemens AG Copyright year All rights reserved

（3）授权密钥数据块

DB3 为授权密钥数据块（名称 LICENSE_DB），用于填写通过西门子授权中心申请到的 17 个字符，如图 3-11 所示：

Address	Name	Type	Initial value	Actual value	Comment
0.0	REG_KEY	STRING [17]	'insert REG_KEY'	'insert REG_KEY'	Registration Key

图 3-11 授权密钥数据块

授权密钥的申请方法，请查看指令库手册“SIMATIC Modbus/TCP Communication via the integrated PN interface of the CPU”的第 5 章。

由于在获取授权密钥前，“MODBUSPN”指令是无授权状态，会使 CPU 报错而停机。而为了读取 CPU 的“IDENT_CODE”码，需要 CPU 运行起来，则必须添加编程错误组织块 OB121。

（4）启动组织块

启动组织块 OB100（名称 COMPLETE RESTART），该 OB 块在 CPU 启动时置位“MODBUSPN”指令的初始化位 Init，如图 3-12 所示：

```
OB100 :  "Complete Restart"
Comment:
Network 1: Initialization of "MODBUSPN"
    // for initialization
        SET
        S     "CONTROL_DAT".Init          DB1.DBX30.1
```

图 3-12 置位“MODBUSPN”指令的初始化位 Init

3.3 通信测试

将项目下载到 CPU 中，打开 Modsan32 应用程序，下面以保持寄存器为例介绍通信测试过程。

首先，通过变量监控表，查看作为 server 端的 PLC 的状态，如图 3-13 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

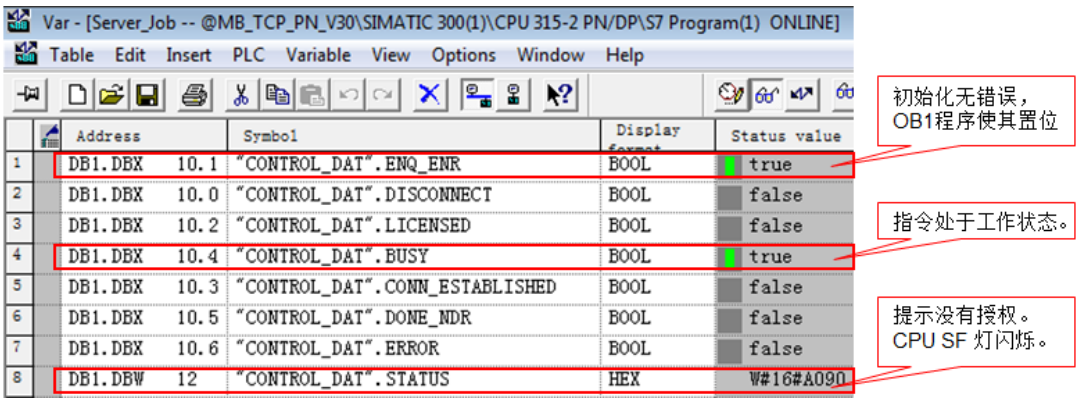

图 3-13 初始化完成后的状态

然后，在 ModScan32 的 Connection 菜单下选择 connect，并设置 ModScan32 访问作为 server 端的 PLC 的 IP 地址和端口号，如图 3-14 所示：

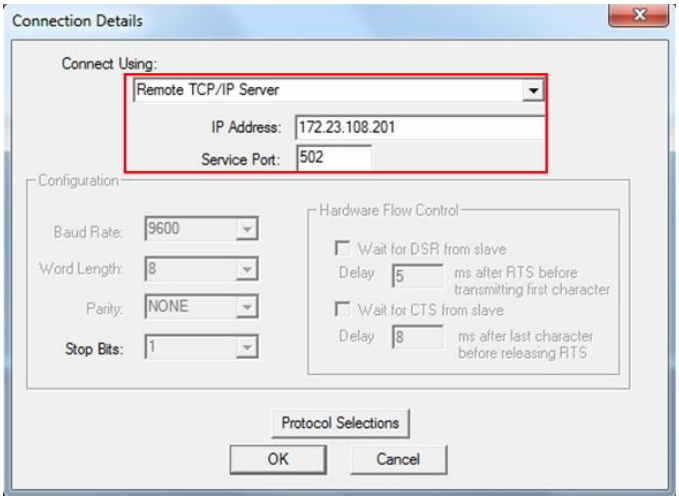

图 3-14 Connection 菜单下选择 connect

最后，在 Modscan32 的数据定义界面中设置需要访问的 Modbus 起始地址及长度（本测试中，Modscan32 使用数据类型 3，访问保持寄存器起始地址为 40001 的 10 个字），建立与 CPU 集成 PN 口的通信连接，可以看到双方可以建立通信连接（变量 CONN_ESTABLISHED=TRUE 为已建立连接的状态），并进行数据读取，如图 3-15 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

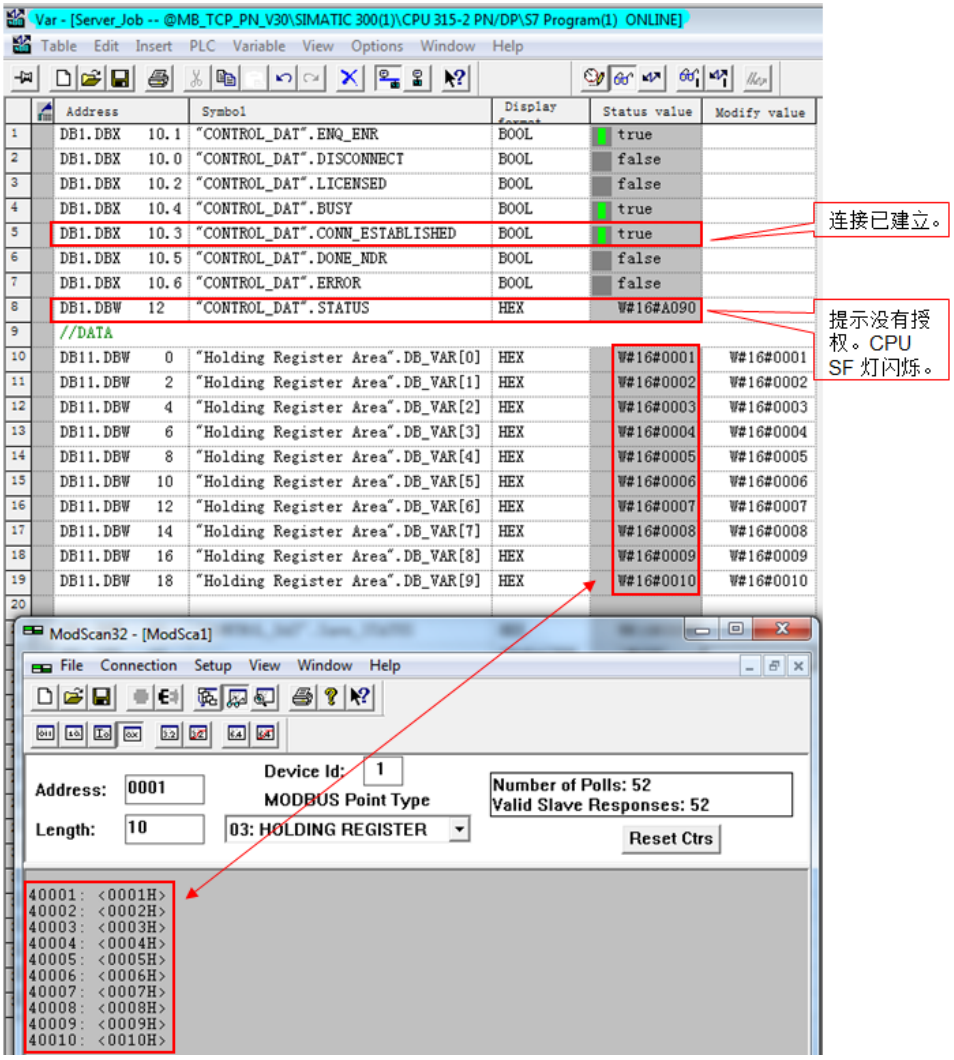

图 3-15 通信测试

使用功能块“MODBUSPN”的一些注意事项：

1）S7-300CPU 的集成 PN 口通过功能块“MODBUSPN”支持与多个 Modbus 客户端的通信，支持的个数取决于 CPU 所支持的 TCP 连接数，必须为每一个客户端连接分别调用一次功能块“MODBUSPN”，其背景数据块、ID、端口号等参数必须唯一。

2）S7-300CPU 的集成 PN 口可以同时作为 Modbus TCP 的 Server 及 Client。

3）S7-300CPU 的集成 PN 口支持多协议，除了运行 Modbus TCP 协议外，同时可以运行 PROFINET、TCP/IP、S7 等协议。

Copyright © Siemens AG Copyright year All rights reserved

4 配置 PN CPU 作为 Modbus TCP Client 与通信伙伴建立通讯

下面以 S7-300 单站系统及 ModSim32 软件为例，详细介绍如何将 S7-300 单站系统 CPU 的集成 PN 口配置为 Client，ModSim32 为 Server 进行 Modbus TCP 通讯。

4.1 组态硬件

插入一个新的“SIMATIC 300 Station”，如图 4-1 所示：

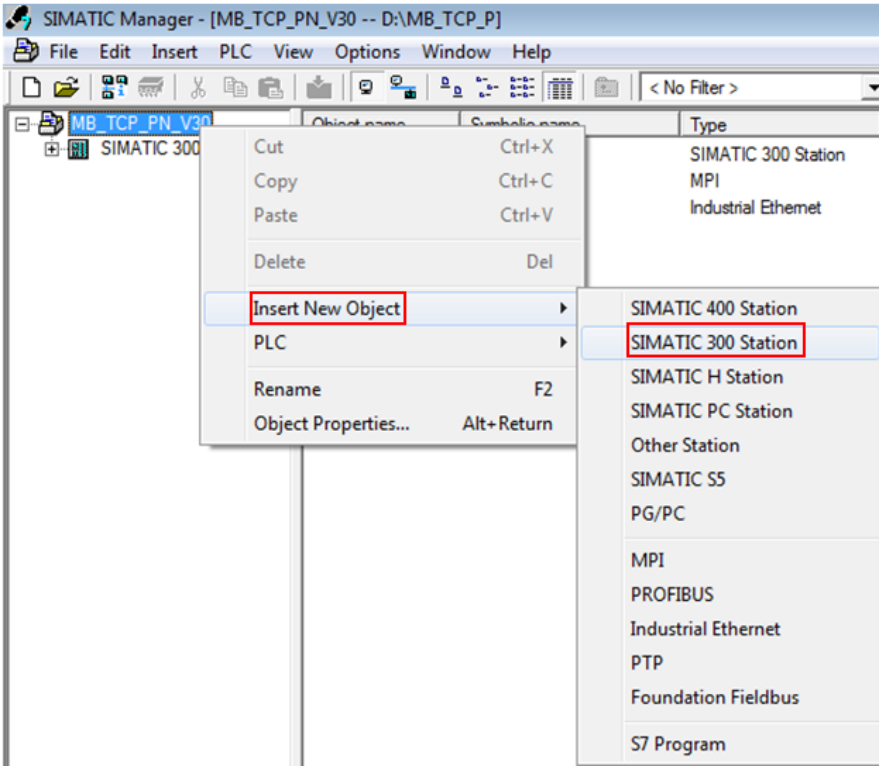

图 4-1 插入 PLC 站点

接着，打开硬件组态视图，插入 CPU 315-2PN/DP，设置 IP 地址，如图 4-2 所示：

Copyright © Siemens
AG Copyright year
All rights reserved

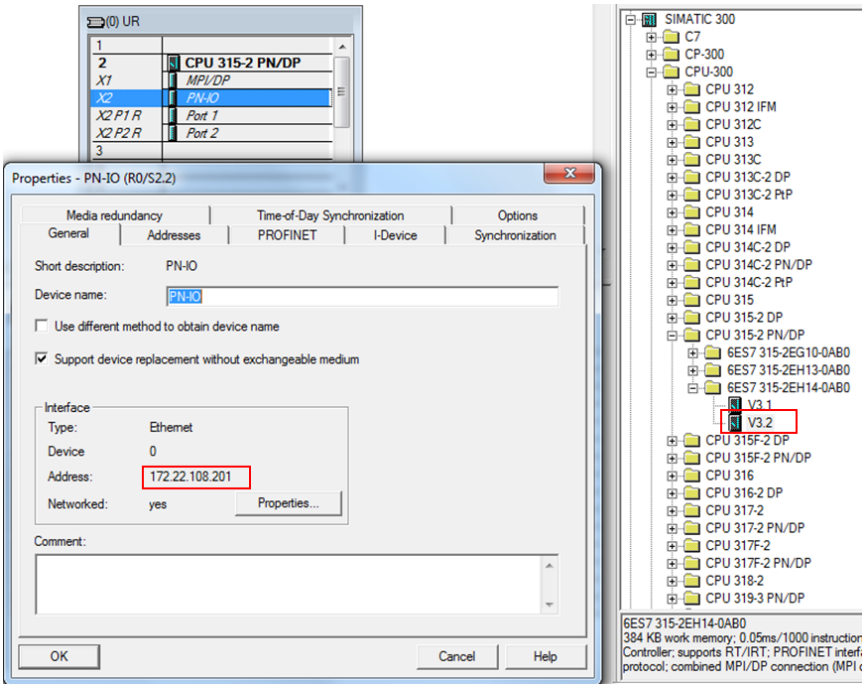

图 4-2 硬件组态

4.2 例程说明

打开例程，从站点“SIMATIC 300（Client）”中拷贝所有程序块（注意，不要拷贝“System data”）到新建项目“MB_TCP_PN_V30”的站点“SIMATIC 300（2）”的 Blocks 中，如图 4-3 所示：

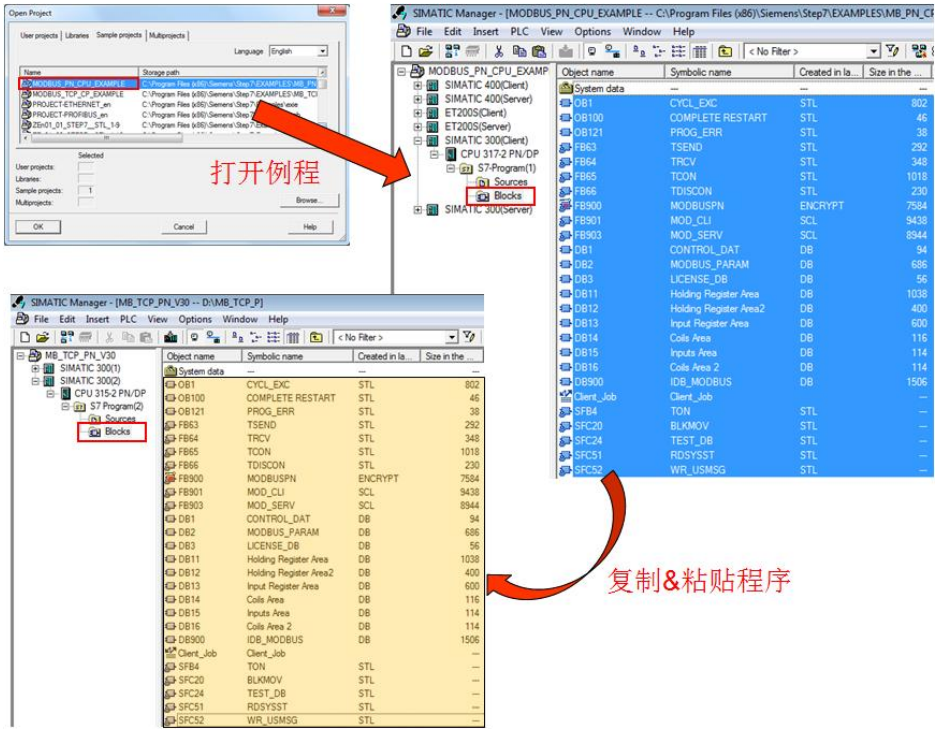

图 4-3 拷贝例程程序

Copyright © Siemens AG Copyright year All rights reserved

（1）打开 OB1，查看指令“MODBUSPN”

在项目的 OB1 组织块中调用了 Modbus TCP 指令，如图 4-4 所示：

```
OB1 :  "Main Program Sweep (Cycle)"
Comment:

Network 1: cyclic call of FB MODBUSPN - S7 is client
      L     1
      T     "CONTROL_DAT".ID                              DB1.DBW0

      L     T#500MS
      T     "CONTROL_DAT".RECV_TIMEOUT                    DB1.DBD2

      L     T#5S
      T     "CONTROL_DAT".CONN_TIMEOUT                    DB1.DBD6

      CALL  "MODBUSPN" , "IDB_MODBUS"                     FB900 / DB900
       id               :="CONTROL_DAT".ID                DB1.DBW0
       db_param         :="MODBUS_PARAM"                  DB2
       REG_KEY_DB       :="LICENSE_DB"                    DB3
       RECV_TIMEOUT     :="CONTROL_DAT".RECV_TIMEOUT      DB1.DBD2
       CONN_TIMEOUT     :="CONTROL_DAT".CONN_TIMEOUT      DB1.DBD6
       DISCONNECT       :="CONTROL_DAT".DISCONNECT        DB1.DBX10.0
       ENQ_ENR          :="CONTROL_DAT".ENQ_ENR           DB1.DBX10.1
       LICENSED         :="CONTROL_DAT".LICENSED          DB1.DBX10.2
       CONN_ESTABLISHED:="CONTROL_DAT".CONN_ESTABLISHED   DB1.DBX10.3
       BUSY             :="CONTROL_DAT".BUSY              DB1.DBX10.4
       DONE_NDR         :="CONTROL_DAT".DONE_NDR          DB1.DBX10.5
       ERROR            :="CONTROL_DAT".ERROR             DB1.DBX10.6
       STATUS           :="CONTROL_DAT".STATUS            DB1.DBW12
       STATUS_FUNC      :="CONTROL_DAT".STATUS_FUNC       P#DB1.DBX14.0
       IDENT_CODE       :=
       Init_Error       :="CONTROL_DAT".Init_Error        DB1.DBX30.2
       Init_Status      :="CONTROL_DAT".Init_Status       DB1.DBW32
       UNIT             :="CONTROL_DAT".UNIT              DB1.DBB24
       DATA_TYPE        :="CONTROL_DAT".DATA_TYPE         DB1.DBB25
       START_ADDRESS    :="CONTROL_DAT".START_ADDRESS     DB1.DBW26
       LENGTH           :="CONTROL_DAT".LENGTH            DB1.DBW28
       WRITE_READ       :="CONTROL_DAT".WRITE_READ        DB1.DBX30.0
       Init             :="CONTROL_DAT".Init              DB1.DBX30.1
```

图 4-4 调用 Modbus TCP 指令

以下为部分管脚说明（其它管脚信息请查看在线帮助）：

id：连接 ID 必须与参数 DB 中相关的 id 参数相同。

db_param：参数 DB 块，包含此 modbus 块实例的连接参数和 modbus 数据参数。CPU 决定该参数的取值范围。DB 编号 0 为系统保留，不允许使用。以纯文本格式输入 DB 编号“DBxy”。

REG_KEY_DB：具有可用于授权的注册表项的数据块。

RECV_TIMEOUT：对从耦合伙伴接收数据进行监视。超出监视时间后，将发出错误信号并终止连接。 最小值为 20 ms。

Copyright © Siemens
AG Copyright year
All rights reserved

在“S7 为客户端”模式下将 RECV_TIMEOUT 设置为 < 20 ms，则会出现相应的错误消息，并会拒绝激活的作业。

CONN_TIMEOUT：监视调用建立或终止所用的时间。如果在组态的监视时间内无法成功建立或终止连接，则会在输出 STATUS 中显示相应的错误消息。最小值为 100 ms。

在“S7 为客户端”模式下，如果 connect_at_startup = TRUE，则过低的组态 CONN_TIMEOUT 会被设置为默认值 5 s。在循环模式下，如果 CONN_TIMEOUT 太小，则会输出错误消息，并会拒绝激活的作业。

UNIT：（Unit Identifier）表示链接伙伴的唯一分配。如果转换器下游有多个通过不同 UNIT 编号进行寻址的串行设备，则通常需要该参数。

在“S7 为客户端”功能中，UNIT 参数为输入参数。需根据要求设置该输入。指令会对请求消息应用该值，并在接收响应时对该值进行检查。

DATA_TYPE：指示当前消息帧处理的 Modbus 数据类型。

START_ADDRESS：首个写入或读取的 Modbus 地址。

LENGTH：写入或读取的 Modbus 值的数目。

对于读取功能，保持和输入寄存器每个消息帧最多支持 125 个寄存器。线圈和输入最多支持 2000 个位。

对于写入功能，保持寄存器最多支持 123 个寄存器，而线圈最多支持 1968 个位。

通过请求消息处理的寄存器或位值必须位于一个数据块中。

WRITE_READ：定义是否要执行读取或写入功能。如果输入/输出具有值 FALSE，则其为读取功能。值 TRUE 定义写入功能。

只能对保持寄存器和线圈进行写入。输入寄存器和输入为只读。

Init：在参数中有上升沿时，初始化 Modbus 块。只有当前没有作业正在运行时，才能执行初始化。必须通过 ENQ_ENR = FALSE 和 BUSY = FALSE 在程序中确保此条件。

（2）参数数据块 DB2

参数数据块 DB2（名称 MODBUS_PARAM），该参数 DB 块可分为两部分理解，偏移量 0~63 字节为 TCP 连接参数的设置区域，偏移量 64~129 为 modbus 数据区域的设置。

Copyright © Siemens AG Copyright year All rights reserved

注意，如需修改 DB 块中的数据，请将 DB 块切换到数据视图“Data view”，在“Actual value”列中进行修改，如图 4-7 所示：

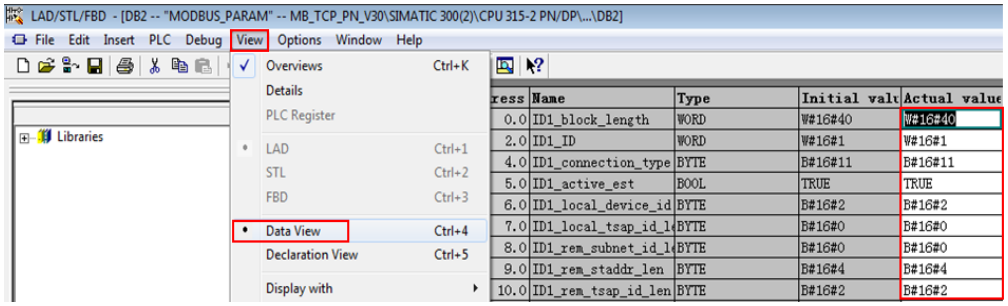

图 4-7 将 DB 块切换到数据视图

①TCP 连接参数的设置，如图 4-8 所示：

Address	Name	Type	Initial value
0.0		STRUCT	
+0.0	ID1_block_length	WORD	W#16#40
+2.0	ID1_ID	WORD	W#16#1
+4.0	ID1_connection_type	BYTE	B#16#11
+5.0	ID1_active_est	BOOL	TRUE
+6.0	ID1_local_device_id	BYTE	B#16#2
+7.0	ID1_local_tsap_id_len	BYTE	B#16#0
+8.0	ID1_rem_subnet_id_len	BYTE	B#16#0
+9.0	ID1_rem_staddr_len	BYTE	B#16#4
+10.0	ID1_rem_tsap_id_len	BYTE	B#16#2
+11.0	ID1_next_staddr_len	BYTE	B#16#0
+12.0	ID1_local_tsap_id	ARRAY[1..16]	B#16#0
*1.0		BYTE	
+28.0	ID1_rem_subnet_id	ARRAY[1..6]	6 (B#16#0)
*1.0		BYTE	
+34.0	ID1_rem_staddr	ARRAY[1..6]	B#16#A, B#16#0, B#16#0, B#16#2
*1.0		BYTE	
+40.0	ID1_rem_tsap_id	ARRAY[1..16]	B#16#1, B#16#F6
*1.0		BYTE	
+56.0	ID1_next_staddr	ARRAY[1..6]	6 (B#16#0)
*1.0		BYTE	
+62.0	ID1_spare	WORD	W#16#0

图 4-8 TCP 连接参数的设置

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID1_ID：每个 PN CPU 与通信伙伴之间的连接都需要一个连接 ID。如果有多个通信伙伴，则每个逻辑连接会使用不同的连接 ID。该连接 ID 在参数数据块中包含的“连接参数块”中组态。连接 ID 唯一地描述 CPU 与链接伙伴之间的连接，取值范围为 1 到 4095。必须在此处输入参数块中的连接 ID；该 ID 在整个 CPU 中必须唯一。

ID1_connection_type：建立连接的连接类型通过 TCON 指令定义。CPU 决定必须要设置的值。

Copyright © Siemens
AG Copyright year
All rights reserved

TCP（兼容模式）：B#16#01，针对 CPU 315 或 317 <= FW V2.3 。

TCP：B#16#11，针对 CPU 315 或 317 >= FW V2.4、IM 151-8 PN/DP CPU、CPU314C、CPU319、CPU412、CPU414 和 CPU416。

ID1_active_est：该参数表示连接建立类型，主动或被动。Modbus 客户端负责建立主动连接而 Modbus 服务器负责建立被动连接。

主动连接的建立：TRUE

被动连接的建立：FALSE

ID1_local_device_id：定义所用 PN CPU 的 IE 接口。根据不同的 PN CPU 类型，需要不同的设置。

CPU 类型	local_device_id
IM 151-8 PN/DP CPU	B#16#1
CPU 314C、315 或 317	B#16#2
CPU 319	B#16#3
CPU 412、414 或 CPU 416	B#16#5

ID1_rem_ staddr_len：指定 rem_staddr 参数的长度，该参数为通信伙伴的 IP 地址。如果要通过未指定的连接进行通信，则不为伙伴指定 IP 地址。

未指定的连接：B#16#0

指定的连接：B#16#4

ID1_rem_tsap_id_len：参数 rem_tsap_id 的长度和远程通信伙伴的端口号。

主动连接的建立：2

被动连接建立：0

ID1_rem_ staddr：在此字节数组中输入远程通信伙伴的 IP 地址。使用未指定的连接时，不输入 IP 地址。表示类型取决于 connection_type 参数。示例：IP 地址 192.168.0.1：

对于 connection_type B#16#01：	
rem_staddr[1] =	B#16#01 (1)
rem_staddr[2] =	B#16#00 (0)
rem_staddr[3] =	B#16#A8 (168)

Copyright © Siemens AG Copyright year All rights reserved

rem_staddr[4] = rem_staddr[5-6]=	B#16#C0 (192) B#16#00（保留）
对于 connection_type B#16#11： rem_staddr[1] = rem_staddr[2] = rem_staddr[3] = rem_staddr[4] = rem_staddr[5-6]=	 B#16#C0 (192) B#16#A8 (168) B#16#00 (0) B#16#01 (1) B#16#00（保留）

ID1_rem_tsap_id：使用该参数设置 remote 端口号。表示类型会因 ID1_connection_type 参数不同而有所不同。CPU 决定值范围。

对于 connection_type B#16#01： rem_tsap_id[1] rem_tsap_id[2] rem_tsap_id[3-16]	 用十六进制格式表示的端口号 low byte 用十六进制格式表示的端口号 high byte B#16#00
对于 connection_type B#16#11： rem_tsap_id[1] rem_tsap_id[2] rem_tsap_id[3-16]	 用十六进制格式表示的端口号 high byte 用十六进制格式表示的端口号 low byte B#16#00

本例中，CPU 为 315-2PN，connection_type B#16#11，远程伙伴的 IP 地址为：172.23.108.245（16#AC，16#17，16#6C，16#F5），端口号设置为 502（16#01F6），则对应于 rem_tsap_id[1]= 16#01，rem_tsap_id[2]= 16#F6。修改参数 DB 块的实际值列，如图 4-9 所示：

Address	Name	Type	Initial value	Actual value
34.0	ID1_rem_staddr[1]	BYTE	B#16#A	B#16#AC
35.0	ID1_rem_staddr[2]	BYTE	B#16#0	B#16#16
36.0	ID1_rem_staddr[3]	BYTE	B#16#0	B#16#6C
37.0	ID1_rem_staddr[4]	BYTE	B#16#2	B#16#F5
38.0	ID1_rem_staddr[5]	BYTE	B#16#0	B#16#0
39.0	ID1_rem_staddr[6]	BYTE	B#16#0	B#16#0
40.0	ID1_rem_tsap_id[1]	BYTE	B#16#1	B#16#1
41.0	ID1_rem_tsap_id[2]	BYTE	B#16#F6	B#16#F6

图 4-9 设置远程伙伴的 IP 地址和端口号

Copyright © Siemens AG Copyright year All rights reserved

②modbus 数据区域的设置，如图 4-10 所示：

Address	Name	Type	Initial valu	Comment
+64.0	ID1_server_client	BOOL	FALSE	
+64.1	ID1_single_write	BOOL	FALSE	
+64.2	ID1_connect_at_startup	BOOL	FALSE	
+65.0	ID1_reserved	BYTE	B#16#0	
+66.0	ID1_data_type_1	BYTE	B#16#3	
+68.0	ID1_db_1	WORD	W#16#B	11
+70.0	ID1_start_1	WORD	W#16#0	0
+72.0	ID1_end_1	WORD	W#16#1F3	499
+74.0	ID1_data_type_2	BYTE	B#16#3	
+76.0	ID1_db_2	WORD	W#16#C	12
+78.0	ID1_start_2	WORD	W#16#2D0	720
+80.0	ID1_end_2	WORD	W#16#384	900
+82.0	ID1_data_type_3	BYTE	B#16#4	
+84.0	ID1_db_3	WORD	W#16#D	13
+86.0	ID1_start_3	WORD	W#16#2D0	720
+88.0	ID1_end_3	WORD	W#16#3E8	1000
+90.0	ID1_data_type_4	BYTE	B#16#0	
+92.0	ID1_db_4	WORD	W#16#0	
+94.0	ID1_start_4	WORD	W#16#0	
+96.0	ID1_end_4	WORD	W#16#0	
+98.0	ID1_data_type_5	BYTE	B#16#1	
+100.0	ID1_db_5	WORD	W#16#E	14
+102.0	ID1_start_5	WORD	W#16#280	640
+104.0	ID1_end_5	WORD	W#16#4E2	1250
+106.0	ID1_data_type_6	BYTE	B#16#2	
+108.0	ID1_db_6	WORD	W#16#F	15
+110.0	ID1_start_6	WORD	W#16#6A4	1700
+112.0	ID1_end_6	WORD	W#16#8FC	2300
+114.0	ID1_data_type_7	BYTE	B#16#1	
+116.0	ID1_db_7	WORD	W#16#10	16
+118.0	ID1_start_7	WORD	W#16#6A4	1700
+120.0	ID1_end_7	WORD	W#16#8FC	2300
+122.0	ID1_data_type_8	BYTE	B#16#0	
+124.0	ID1_db_8	WORD	W#16#0	
+126.0	ID1_start_8	WORD	W#16#0	
+128.0	ID1_end_8	WORD	W#16#0	

图 4-10 modbus 数据区域的设置

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID1_server_client：S7 是服务器=TRUE；S7 是客户端=FALSE。

ID1_single_write：在“客户端”操作模式下，如果参数 ID1_single_write = TRUE，则功能代码 5 和 6 用于执行长度为 1 的写入作业。如果 ID1_single_write = FALSE，则功能代码 15 和 16 用于所有写入作业。

ID1_connect_at_startup：如果将 ID1_connect_at_startup 设置为 TRUE，将在 CPU 重新启动后立即建立连接。此种情况下，只有正确建立连接

Copyright © Siemens AG Copyright year All rights reserved

(CONN_ESTABLISHED = TRUE) 后才能启动数据请求，否则将在 ERROR 和 STATUS 中显示相应的错误。

设置为 FALSE：如果 ENQ_ENR，则连接建立。

设置为 TRUE：重新启动后立即建立连接。

ID1_data_type_x：指定该数据块中映射的 MODBUS 数据类型。如果在 ID1_data_type_x 中输入值 16#0，则不使用相应的区域。

标识符	数据类型	数据宽度
16#0	未使用区域	
16#1	线圈	Bit
16#2	输入	Bit
16#3	保持寄存器	Word
16#4	输入寄存器	Word

Modbus 数据类型	DATA_TYPE	功能	长度	single_write	功能代码
线圈	1	读取	任意	不相关	1
线圈	1	写入	1	TRUE	5
线圈	1	写入	1	FALSE	15
线圈	1	写入	> 1	不相关	15
输入	2	读取	任意	不相关	2
保持寄存器	3	读取	任意	不相关	3
保持寄存器	3	写入	1	TRUE	6
保持寄存器	3	写入	1	FALSE	16
保持寄存器	3	写入	> 1	不相关	16
输入寄存器	4	读取	任意	不相关	4

图 4-11 不同的数据类型与 modbus 功能代码的关系

ID1_db_x：指定映射 MODBUS 寄存器或下面定义的位值的数据块。DB 编号 0 为系统保留，不允许使用。

DB 编号：1 到 65535（W#16#0001 到 W#16#FFFF）。

ID1_start / end_x：start 指定 DB 的数据字 0 中映射的第一个 Modbus 地址。end 参数定义最后一个 MODBUS 地址。

Copyright © Siemens AG Copyright year All rights reserved

对于寄存器访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字编号如下计算：DBW 编号 = (end – start) * 2

对于位访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字节编号如下计算：DBB 编号 = (end – start + 7) / 8

定义的数据区不得重叠。end 参数不得小于 start。如果发生错误，指令启动将中止并提示错误。如果两个值相同，则将分配一个 Modbus 地址（1 个寄存器或 1 个位值）。

注意：数据块必须比已组态数据所需的长度多两个字节。最后的两个字节供内部使用。

例程中设置的 DB 块和 modbus 地址的对应关系，如图 4-12 所示：

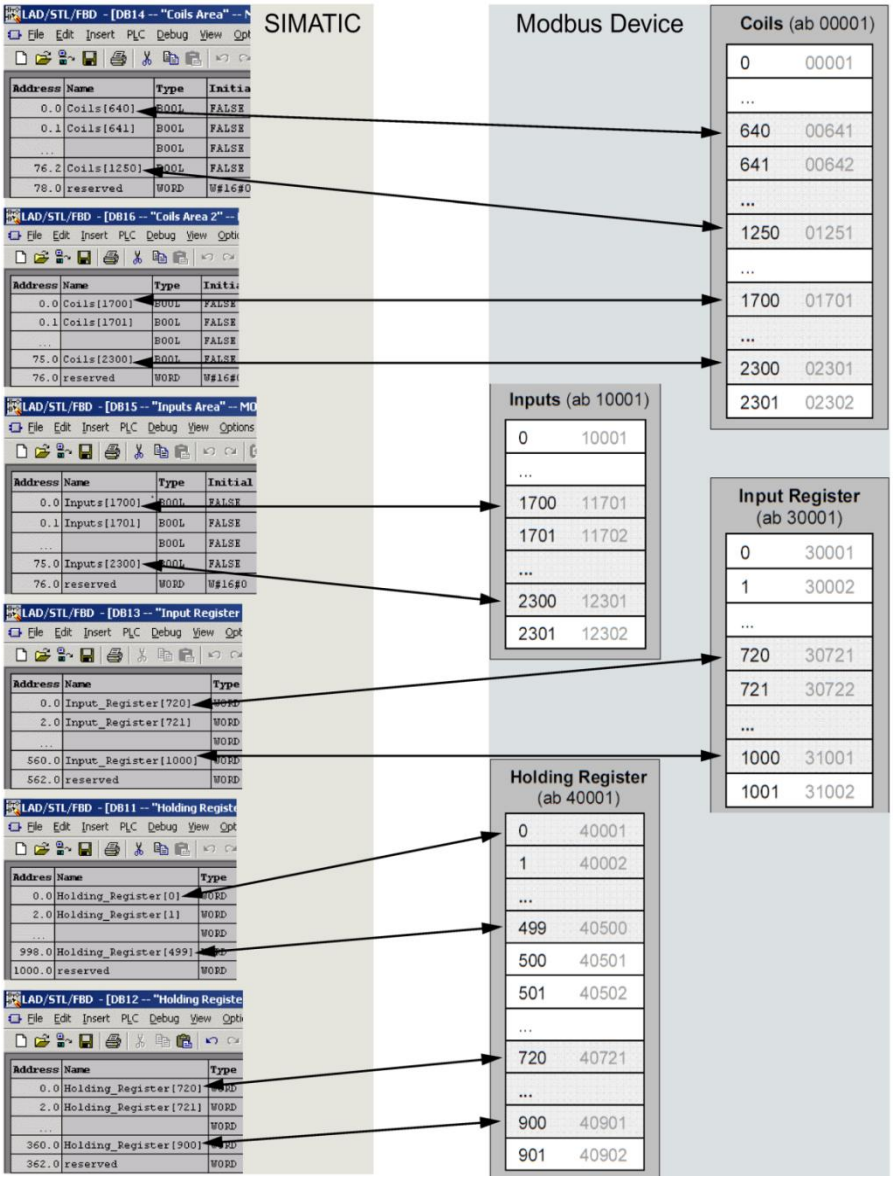

图 4-12 DB 块和 modbus 地址的对应关系

Copyright © Siemens AG Copyright year All rights reserved

（3）授权密钥数据块

DB3 为授权密钥数据块（名称 LICENSE_DB），用于填写通过西门子授权中心申请到的 17 个字符，如图 4-13 所示：

Address	Name	Type	Initial value	Actual value	Comment
0.0	REG_KEY	STRING [17]	'insert REG_KEY'	'insert REG_KEY'	Registration Key

图 4-13 授权密钥数据块

授权密钥的申请方法，请查看指令库手册“SIMATIC Modbus/TCP Communication via the integrated PN interface of the CPU”的第 5 章。

由于在获取授权密钥前，“MODBUSPN”指令是无授权状态，会使 CPU 报错而停机。而为了读取 CPU 的“IDENT_CODE”码，需要 CPU 运行起来，则必须添加编程错误组织块 OB121。

（4）启动组织块

启动组织块 OB100（名称 COMPLETE RESTART），该 OB 块在 CPU 启动时置位“MODBUSPN”指令的初始化位 Init，如图 4-14 所示：

```
OB100 :  "Complete Restart"
Comment:
Network 1: Initialization of "MODBUSPN"
    // for initialization
        SET
        S     "CONTROL_DAT".Init          DB1.DBX30.1
```

图 4-14 置位“MODBUSPN”指令的初始化位 Init

4.3 通信测试

将项目下载到 CPU 中，打开 ModSim32 应用程序，下面以保持寄存器为例介绍通信测试过程。

首先，在 ModSim32 的 Connection 菜单下选择 Connect——>Modbus/TCP Svr，并设置 ModSim32 作为 server 端的端口号，如图 4-15 所示：

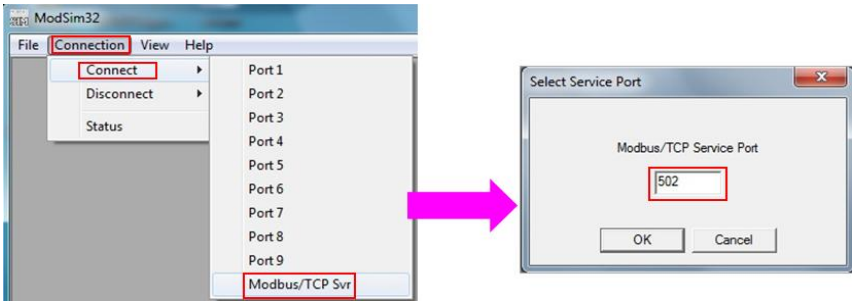

图 4-15 设置 ModSim32 作为 server 端的端口号

Copyright © Siemens AG Copyright year All rights reserved

然后，需要置位“ENQ_ENR”，作为 modbus TCP 的 client 端的 PLC 将创建连接，并发送读取寄存器的请求（本测试中，PLC 访问 Modsim32 定义的数据类型 3，保持寄存器起始地址为 40001 开始的 10 个字），可以看到双方可以建立通信连接（变量 CONN_ESTABLISHED= TRUE 为已建立连接的状态），并进行数据读取，如图 4-16 所示：

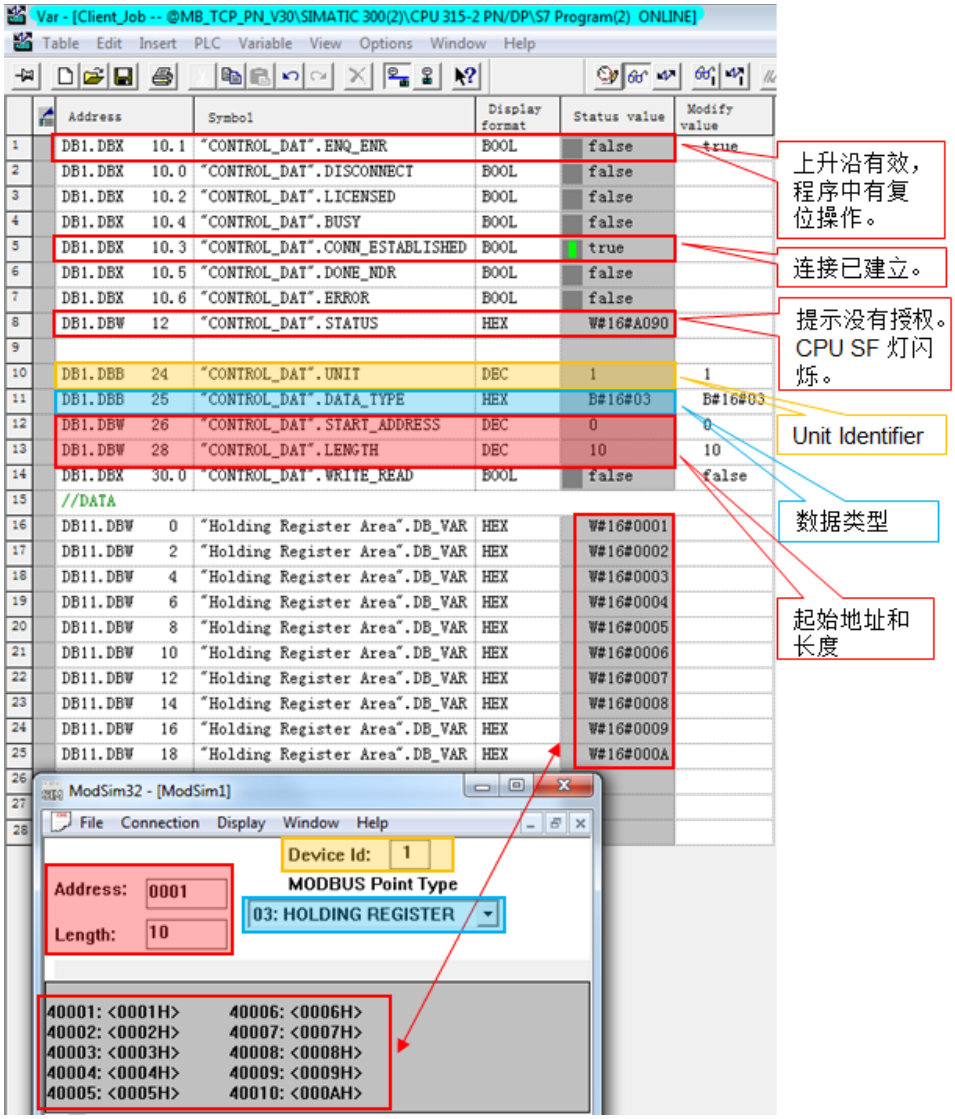

图 4-16 通信测试

使用功能块“MODBUSPN”的一些注意事项：

1）S7-300CPU 的集成 PN 口通过功能块“MODBUSPN”支持与多个 Modbus 服务器的通信，支持的个数取决于 CPU 所支持的 TCP 连接数，必须为每一个服务器连接分别调用一次功能块“MODBUSPN”，其背景数据块、ID 必须唯一，必须指定唯一的服务器 IP 地址。

2）S7-300CPU 的集成 PN 口可以同时作为 Modbus TCP 的 Server 及 Client。

3）S7-300CPU 的集成 PN 口支持多协议，除了运行 Modbus TCP 协议外，同时可以运行 PROFINET、TCP/IP、S7 等协议。

Copyright © Siemens AG Copyright year All rights reserved

Copyright © Siemens AG Copyright year All rights reserved

5 相关资料链接

S7-300/S7-400 中 Modbus/TCP 块需要多少个授权?

http://support.automation.siemens.com/CN/view/zh/103709414

如何在 SIMATIC S7 上建立 OPEN MODBUS/TCP 通讯，如何查找相关信息?

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

Simatic S7-300/S7-400：创建 Modbus/TCP 通信连接数据的向导

https://support.industry.siemens.com/cs/cn/zh/view/60735352

Manual of SIMATIC Modbus/TCP Communication via the integrated PN interface of the CPU

https://support.industry.siemens.com/cs/cn/en/view/109745065

Block library for Modbus/TCP communication over the integrated PN interface of a SIMATIC CPU

https://support.industry.siemens.com/cs/cn/en/view/109745187