

FUN DP-MODBUS 转换器

用户手册

版本：V2.01

发布日期：08/2017

大连德嘉工控设备有限公司

目录

1. 产品概述.....	3
2. 快速使用指南.....	4
3. 作为 modbus 主站.....	8
4. 作为 modbus 从站.....	31
5. Modbus RTU 协议简介.....	45
6. 与 Giant525 称重模块通.....	55

1 产品概述

在 modbus 侧为主站时：主要用于连接 modbus 从站仪表、及其它一些 modbus 从站设备，如：MODBUS 协议接口的变频器、电机启动保护装置、智能高低压。

在 modbus 侧为从站时：以 modbus 从站协议与其他 modbus 主站设备进行数据通讯。

增加了 USB 调试功能，可以利用串口助手进行 modbus 命令的调试

GSD 文件下载： [点击下载](#) （右键点击下载）

串口助手： [点击下载](#) （右键点击下载）

USB 芯片驱动： [点击下载](#) （右键点击下载）

- 调试方便，手段多样，尤其适用于初次使用者
- 它有 7 个指示灯，使你能更为清晰准确快捷的判断问题所在；
- 它在 modbus 主站方式时，通过不断循环显示的多个状态字，使你能够轻松发现各个从站设备及相应报文的故障性质

这些都是有别于其它厂家的特点，目的是使客户能用最短的时间迅速完成现场调试，立即发现问题，立即解决问题，绝不浪费你的宝贵时间。

2 快速使用指南

- 电器接口：RS485(2 线)。
- 安装方式：35mm 导轨安装。
- 支持的 DP-PROFIBUS 波特率：9.6K-1.5M（自适应）。
- 支持的 modbus 波特率：2400、4800、9600、14400、19200、38400、57600、115200。
- 校验位(8 位无校验 1 停止位、8 位偶校验 1 停止位、8 位奇校验 1 停止位、8 位无校验 2 停止位)可选。

与 DP-PROFIBUS 总线连接时，作为 DP 从站

与 MODBUS 连接时，可以选择为 MODBUS 主站或 MODBUS 从站，二者不可同时存在。

支持 MODBUS 通讯 01H、02H、03H、04H、05H、06H、0FH、10H 号功能。

作为 MODBUS 主站时，能带 Modbus 从站数：不确定，主要有两个条件的限制。

1、此模块最多能配置的 Modbus-RTU 报文数为 34 条；

2、最大的数据量（各从站之和）为输入输出各 220 字节。即使您现场的应用没有超过这个限制，还和 Modbus 的通讯波特率以及现场的环境有关。如果您现场环境很好，施工水平很高，在不超过前面两条限制的情况下可连接 10 台以上。

作为 MODBUS 从站时，PROFIBUS 输入/输出数量可自由设定，但要符合如下条件：

① $\text{Input Bytes} + \text{Output Bytes} \leq 230 \text{ Bytes}$

② $\text{Max Input Bytes} \leq 222 \text{ Bytes}$

③ $\text{Max Output Bytes} \leq 222 \text{ Bytes}$

MODBUS 存储区：

0XXXX 区（线圈）、1XXXX 区（离散量输入）、3XXXX 区（输入寄存器）、4XXXX 区（保持寄存器）

注：0XXXX, 1XXXX, 3XXXX, 4XXXX 中最左边的 0, 1, 3, 4 在实际的应用中是不用的，它只是告诉你该 MODBUS 存储区是线圈离散量输入、输入寄存器、保持寄存器。

当你使用 MODBUS 通讯 01H、05H、0FH 号功能时，实际地址 XXXX,就对应于 0XXXX 区（线圈）

当你使用 MODBUS 通讯 02H 号功能时,实际地址 XXXX,就对应于 1XXXX 区（离散量输入）

当你使用 MODBUS 通讯 03H、06H、10H 号功能时,实际地址 XXXX,就对应于 4XXXX 区（保持寄存器）

当你使用 MODBUS 通讯 04H 号功能时,实际地址 XXXX,就对应于 3XXXX 区（输入寄存器）

图1-2

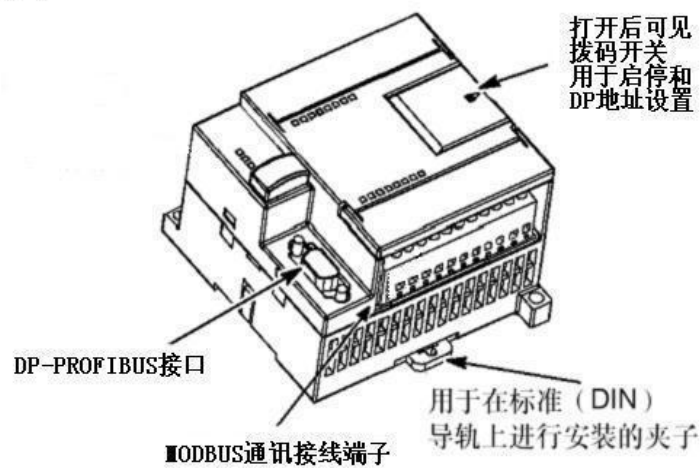
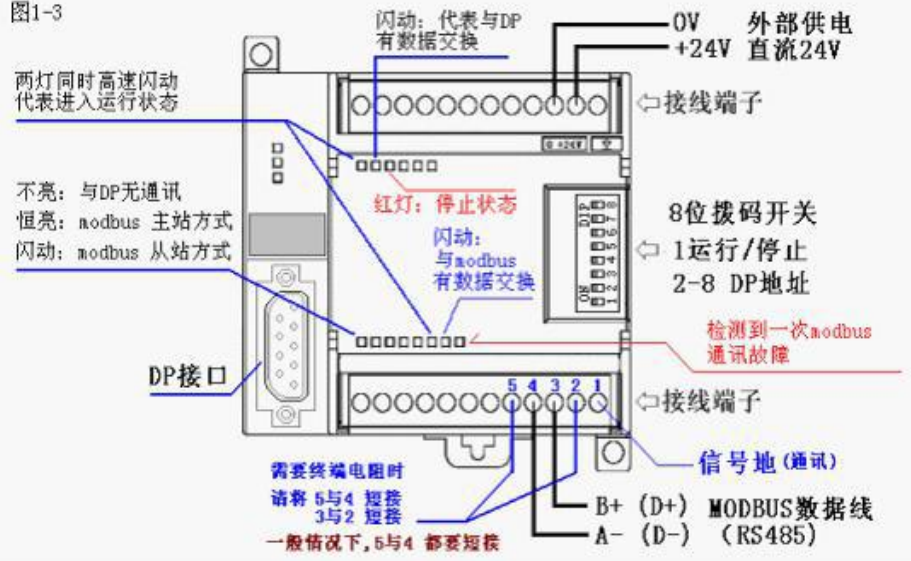


图1-3



拨码开关说明：

1 号拨码

ON 协议转换器进入运行状态，即工作状态。

OFF 协议转换器进入停止状态，此时既不与 DP 通讯、也不与 MODBUS 通讯。

2-8 号拨码，是 DP 地址设置开关，详见图 1-4：

2	3	4	5	6	7	8	DP 地址	2	3	4	5	6	7	8	DP 地址	2	3	4	5	6	7	8	DP 地址	2	3	4	5	6	7	8	DP 地址
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	64	1	1	0	0	0	0	0	96							
0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	1	65	1	1	0	0	0	0	1	97							
0	0	0	0	0	0	1	0	2	0	1	0	0	0	1	0	66	1	1	0	0	0	1	0	98							
0	0	0	0	0	0	1	1	3	0	1	0	0	0	1	1	67	1	1	0	0	0	1	1	99							
0	0	0	0	1	0	0	0	4	0	1	0	0	1	0	0	68	1	1	0	0	1	0	0	100							
0	0	0	0	1	0	1	0	5	0	1	0	0	1	0	1	69	1	1	0	0	1	0	1	101							
0	0	0	0	1	1	0	0	6	0	1	0	0	1	1	0	70	1	1	0	0	1	1	0	102							
0	0	0	0	1	1	1	0	7	0	1	0	0	1	1	1	71	1	1	0	0	1	1	1	103							
0	0	0	1	0	0	0	0	8	0	1	0	1	0	0	0	72	1	1	0	1	0	0	0	104							
0	0	0	1	0	0	0	1	9	0	1	0	1	0	0	1	73	1	1	0	1	0	0	1	105							
0	0	0	1	0	1	0	0	10	0	1	0	1	0	1	0	74	1	1	0	1	0	1	0	106							
0	0	0	1	0	1	1	0	11	0	1	0	1	0	1	1	75	1	1	0	1	0	1	1	107							
0	0	0	1	1	0	0	0	12	0	1	0	1	1	0	0	76	1	1	0	1	1	0	0	108							
0	0	0	1	1	0	1	0	13	0	1	0	1	1	0	1	77	1	1	0	1	1	0	1	109							
0	0	0	1	1	1	0	0	14	0	1	0	1	1	1	0	78	1	1	0	1	1	1	0	110							
0	0	0	1	1	1	1	0	15	0	1	0	1	1	1	1	79	1	1	0	1	1	1	1	111							
0	0	1	0	0	0	0	0	16	0	1	1	0	0	0	0	80	1	1	1	0	0	0	0	112							
0	0	1	0	0	0	0	1	17	0	1	1	0	0	0	1	81	1	1	1	0	0	0	1	113							
0	0	1	0	0	1	0	0	18	0	1	1	0	0	1	0	82	1	1	1	0	0	1	0	114							
0	0	1	0	0	1	1	0	19	0	1	1	0	0	1	1	83	1	1	1	0	0	1	1	115							
0	0	1	0	1	0	0	0	20	0	1	1	0	1	0	0	84	1	1	1	0	1	0	0	116							
0	0	1	0	1	0	1	0	21	0	1	1	0	1	0	1	85	1	1	1	0	1	0	1	117							
0	0	1	0	1	1	0	0	22	0	1	1	0	1	1	0	86	1	1	1	0	1	1	0	118							
0	0	1	0	1	1	1	0	23	0	1	1	0	1	1	1	87	1	1	1	0	1	1	1	119							
0	0	1	1	0	0	0	0	24	0	1	1	1	0	0	0	88	1	1	1	1	0	0	0	120							
0	0	1	1	0	0	0	1	25	0	1	1	1	0	0	1	89	1	1	1	1	0	0	1	121							
0	0	1	1	0	1	0	0	26	0	1	1	1	0	1	0	90	1	1	1	1	0	1	0	122							
0	0	1	1	0	1	1	0	27	0	1	1	1	0	1	1	91	1	1	1	1	0	1	1	123							
0	0	1	1	1	0	0	0	28	0	1	1	1	1	0	0	92	1	1	1	1	1	0	0	124							
0	0	1	1	1	0	1	0	29	0	1	1	1	1	0	1	93	1	1	1	1	1	0	1	125							
0	0	1	1	1	1	0	0	30	0	1	1	1	1	1	0	94	1	1	1	1	1	1	0	126							
0	0	1	1	1	1	1	0	31	0	1	1	1	1	1	1	95															

注：1代表ON 0代表OFF

图1-4

Modbus RS485 拓扑结构

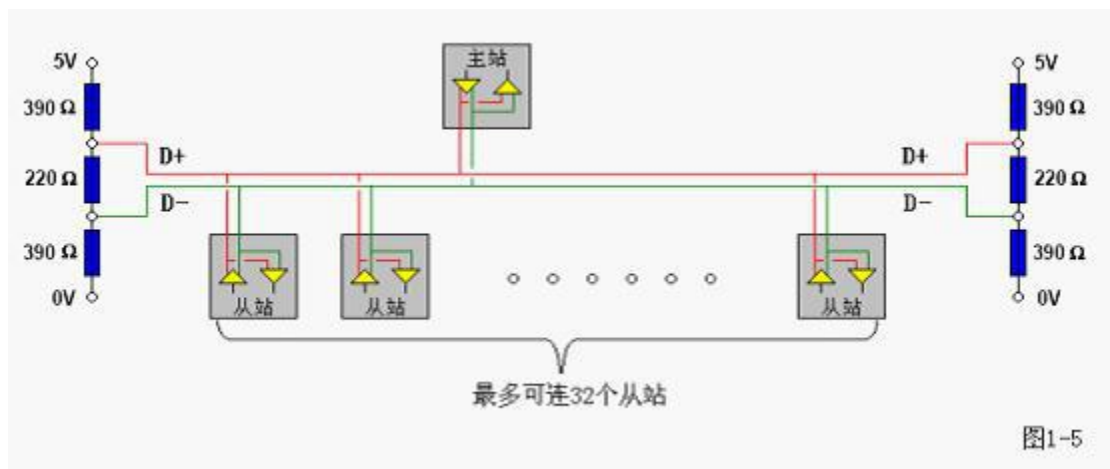
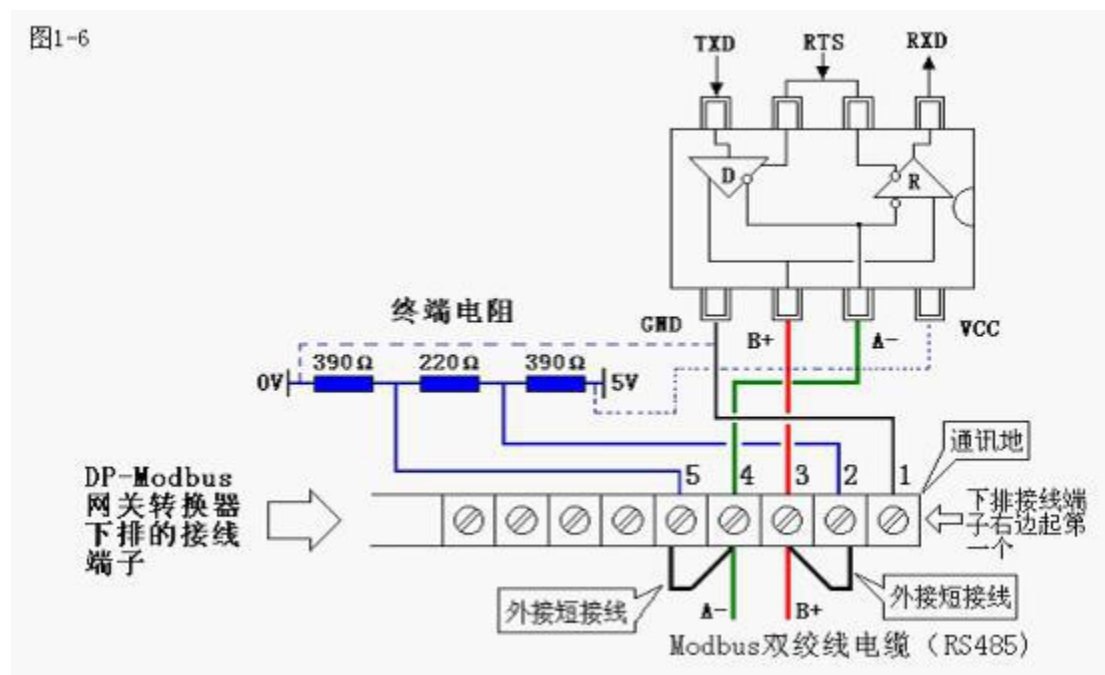


图1-5

DP-Modbus 网关转换器产品已将终端电阻集成到产品中，



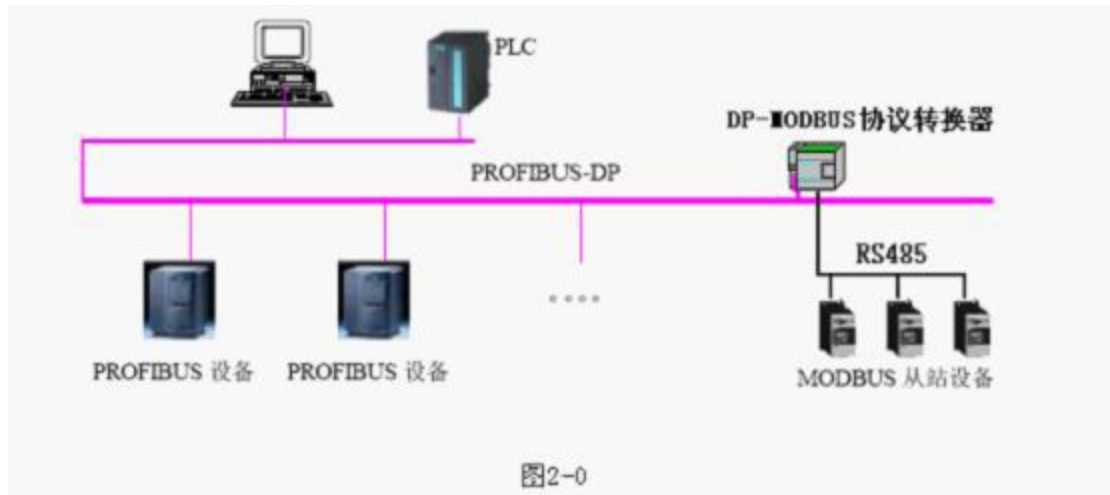
DP-Modbus 网关转换器既可以工作在 modbus 主站方式，也可工作在 modbus 从站方式，这是由 STEP7 硬件组态时设定的。

注：在 step7 中，一定要加入 OB82, OB86, OB121, OB122 这四个组织块 (Organization Block)，用于 DP 通讯的故障处理，程序可以为空。

下边章节，用户可根据实际应用情况有选择的阅读：

3 DP-Modbus 转换器作为 modbus 主站的使用说明

在 PROFIBUS 一侧只做 PROFIBUS 从站；在 MODBUS 一侧做 MODBUS 主站



该方式主要用于连接 modbus 从站仪表、及其它一些 modbus 从站设备，如：

MODBUS 协议接口的变频器、电机启动保护装置、智能高低压电器、电量测量装置、各种变送器、智能现场测量设备及仪表等等

1. 将大连德嘉国际电子提供的 GSD 文件 D_MASTER.GSD 拷贝到 Step7\S7data\gsd\目录下；产品图标 DS007_N.BMP 和 DS007_S.BMP 文件拷贝到 Step7\S7data\nsbmp\目录下

注：以上的详细目录在 XP 系统中分别是：

C:\Program Files\Siemens\Step7\S7DATA\GSD

C:\Program Files\Siemens\Step7\S7DATA\nsbmp

Win7 系统中分别是

C:\Program Files (x86)\Siemens\Step7\S7DATA\GSD

C:\Program Files (x86)\Siemens\Step7\S7DATA\NSBMP

2. 在 STEP7 上通过向导 ‘New Project’ Wizard 建立一个 “项目”，CPU 类型选择 CPU313C-2DP，项目名字叫 “MODBUS_MASTER”

3. 在 Step7 的硬件组态中设置

1) SIMATIC 300 Station → Hardware 双击，并在 HW Config 的菜单中选择 Option → Update Catalog 点击，将设备 GSD 文件加入设备 Catalog 中



图2-1

2) 配置 PROFIBUS: 双击 CPU 槽位中的 DP, →属性→new→Network Settings→187.5K→OK

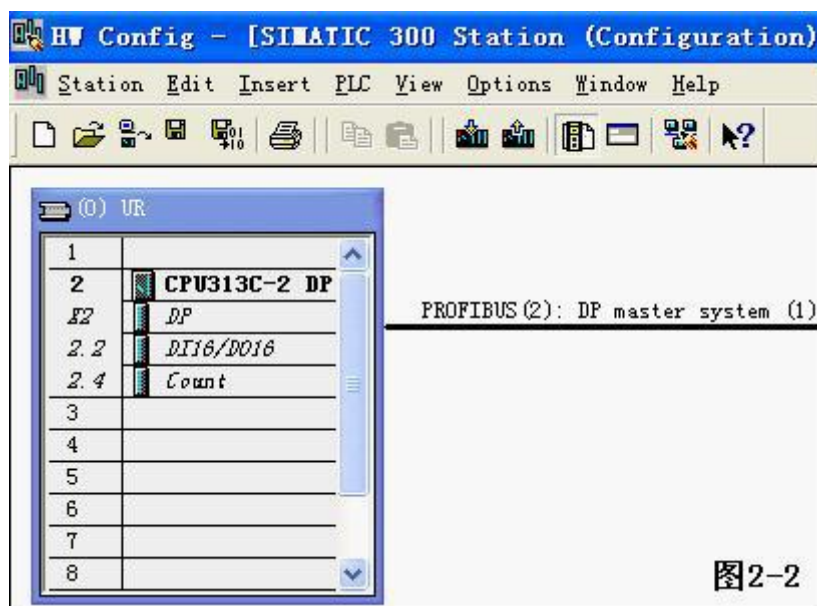


图2-2

- 3) 配置 DP-Modbus 协议转换器作为 PROFIBUS 从站点中 PROFIBUS(1) DP master system(1), 使其选中横线变黑, 打开 Hardware Catalog→PROFIBUS DP→Additional Field Devices→Gateway→DP slave/MODBUS master 双击; 然后选择 DP 从站站号, 本例选择从站站号为: 99→“OK”

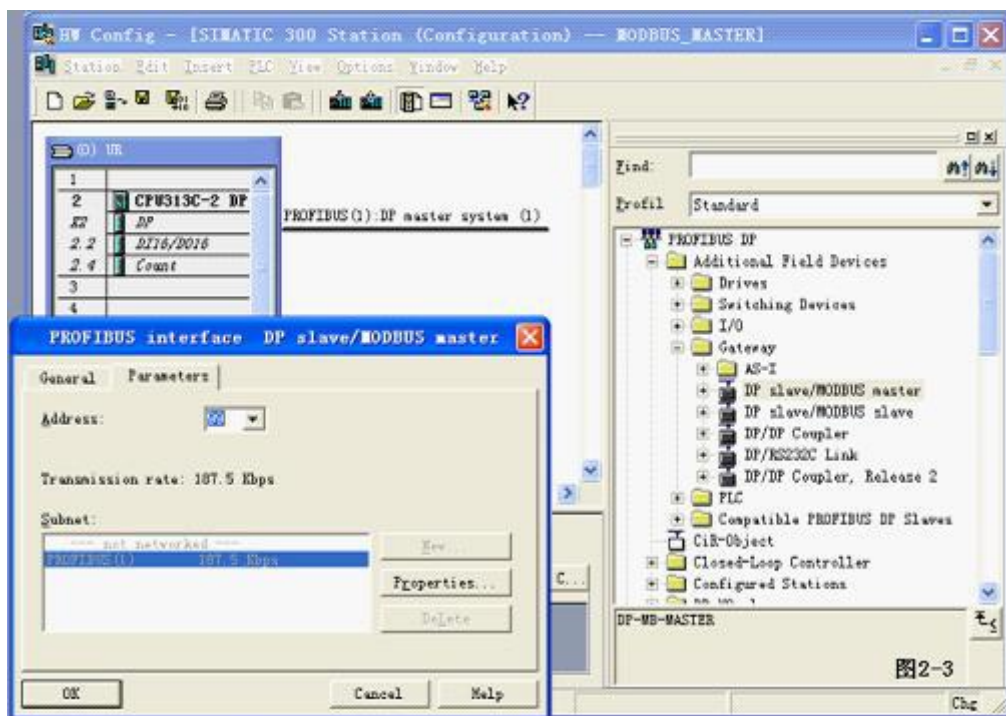


图2-3

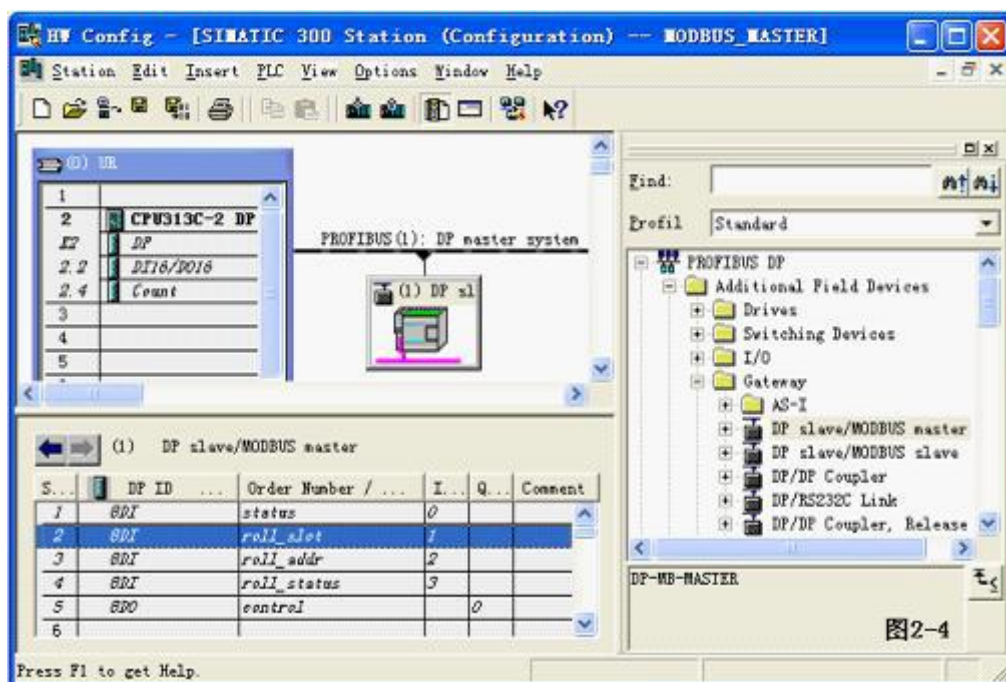


图2-4

- 4) 配置 DP-Modbus 协议转换器的 modbus 侧 RS485 接口双击 DP-Modbus 图标, 出现如图 2-5 的窗口, 选择 Parameter Assignment。

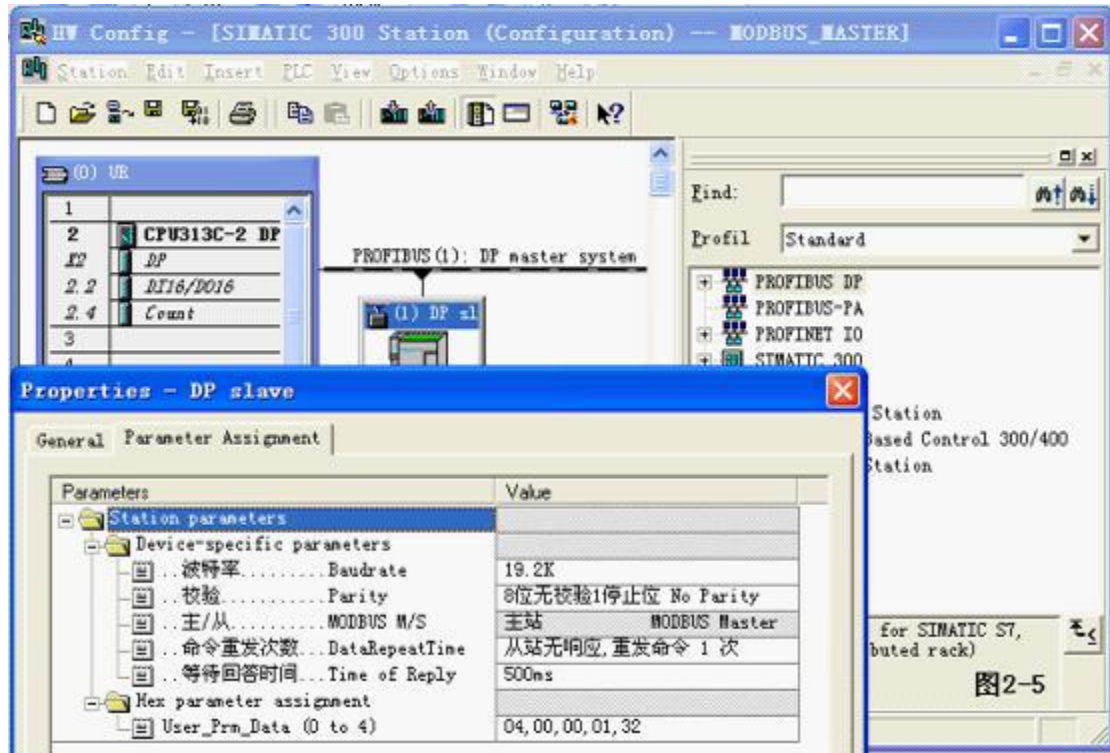


图2-5

“波特率”和“校验”：必须设置的和您要连接的 Modbus 从站设备的一致，否则 DP-Modbus 协议转换器和您要连接的设备无法通讯。

“主/从”：产品设置成主站，使用 GSD 文件 D_MASTER.GSD，只能选择 MODBUS 主站方式。

“命令重发次数”：当从站设备对当前命令无响应时，DP-Modbus 协议转换器可以进行命令重发，或直接发送下一条 modbus 命令。一般选择[从站无响应，直接发送下一条命令]或[从站无响应，重发命令一次]

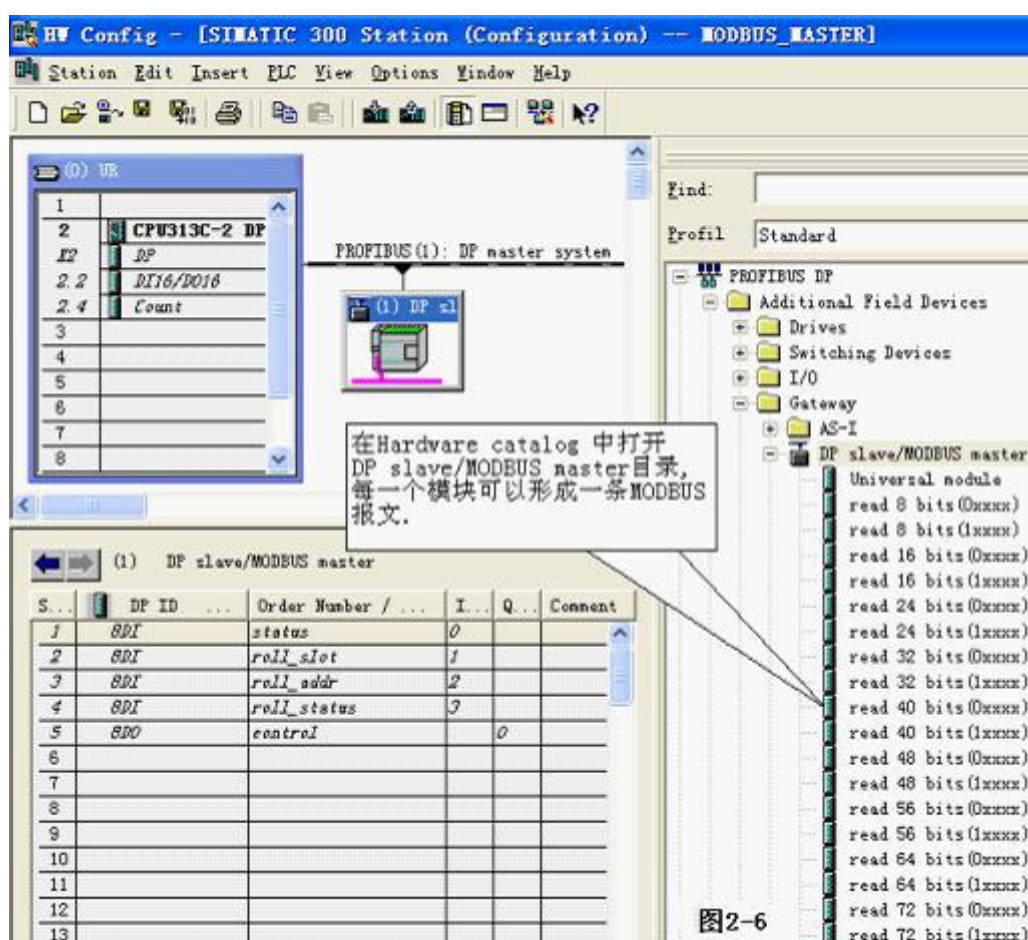
“等待回答时间”：DP-Modbus 协议转换器发出 MODBUS 报文后等待 MODBUS 设备回答的时间。当 MODBUS 设备超过“等待回答时间”时间还没有回答，DP-Modbus 协议转换器停止等待，再次重发报文或发送下一条 MODBUS 报文。一般选择 150 ms，当然越小越好，但这会使从站来不及响应，造成通讯故障，因此要合理选择。

5) Modbus 报文队列的配置

a. 在 Hardware catalog 中打开 DP slave/MODBUS master 目录

DP slave/MODBUS master 有 1#~39# 共 39 个槽（逻辑上，非物理设备）1#、2#、3#、4#、5#槽已占用，剩下 34 个槽提供用户使用。每个槽可以用来插入一条 MODBUS 通信报文，所以一共可以插入 34 条 MODBUS(报文)。

DP slave/MODBUS master 的每一个 MODBUS 模块对应一种功能的 MODBUS 报文，可双击插入某一槽中。



b. 举例说明在 6#槽中插入“read 24 bits(0xxxx)” MODBUS 的 01h 功能报文，即：读取 24 个输出线圈 XXXX(或 0XXXX) 状态。

第一步：选中6#槽，然后双击“read 24 bits (0xxxx)”

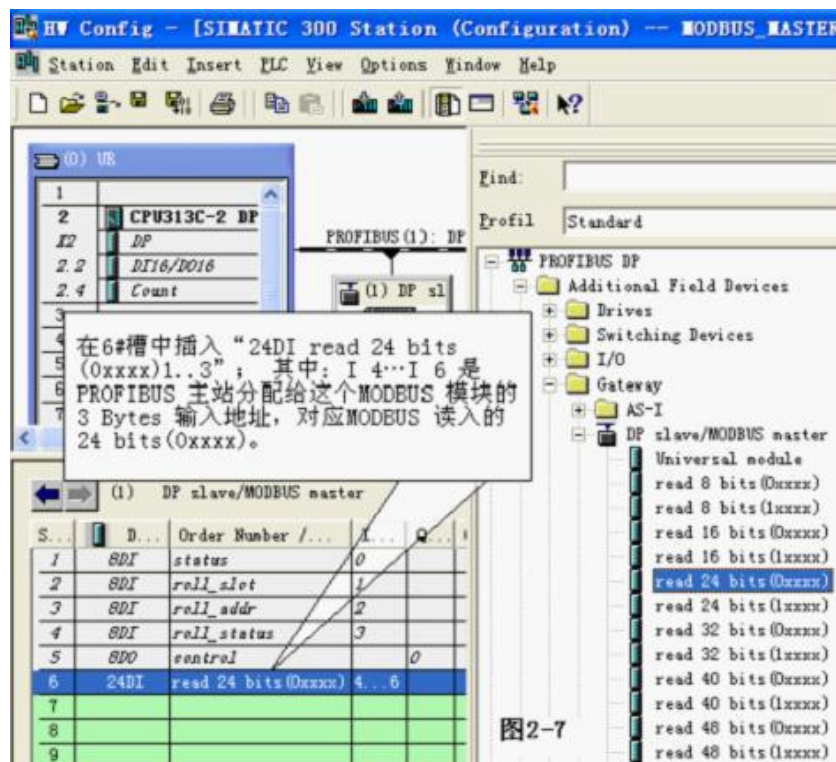


图2-7

第二步：进一步设定 MODBUS 参数:双击6#槽中的“24 DI read 24 bits(0xxxx) 4..6”；选择“Parameter Assigment”，完成“从站地址”和“起始地址”的参数设定，

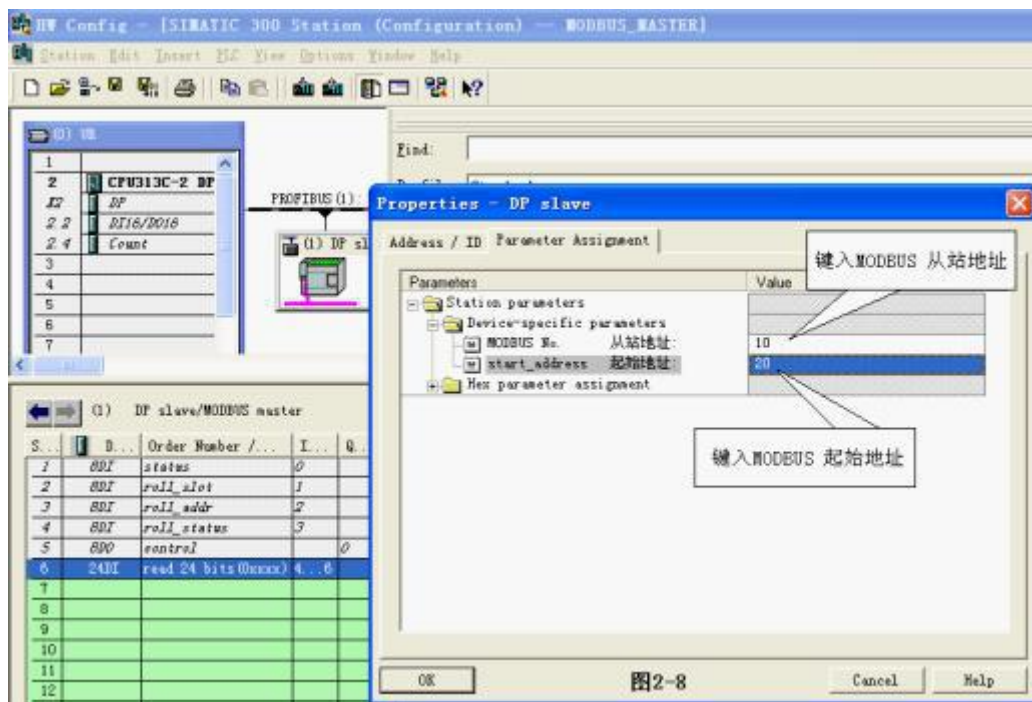


图2-8

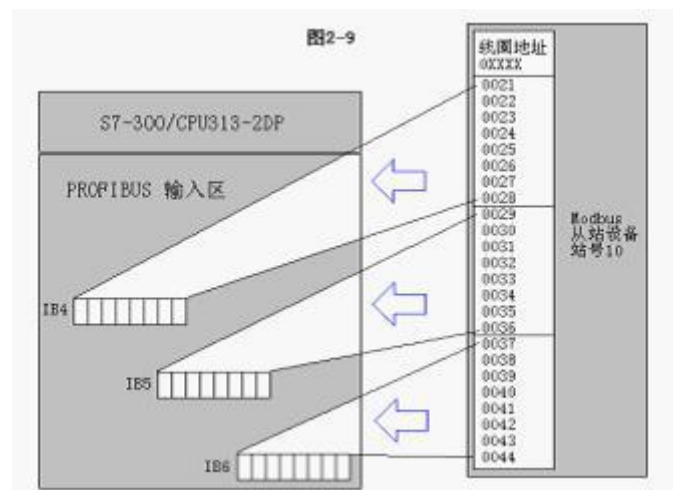
从站地址：指该 MODBUS 报文发送到 MODBUS 设备从站的地址，对应该 MODBUS 报文的第一个字节。

起始地址：本例指要读取的 0XXXX 起始地址，注意：报文中线圈起始地址 0000 对应设备中 00001 地址，其他顺延。

“MODBUS 从站地址：” => 键入 MODBUS 从站地址 10

start address 起始地址：” => 键入欲读取的输出线圈 0XXXX 的起始地址 00021，本例设置地址为 20

PROFIBUS 地址与 MODBUS 地址对应关系：



STEP7 中在线监测 IB4、IB5、IB6：

IB4、IB5、IB6 中的显示的值，就是 6#槽 MODBUS 的 01H 命令读回的 MODBUS 线圈 00021-00044 的状态。

	Address	Symbol	Display format	Status value
1	IB 4		BIN	2#0000_0000
2	IB 5		BIN	2#0000_0000
3	IB 6		BIN	2#0000_0000

c. 举例说明在 7#槽中插入“read 4 Words (3xxxx)”

MODBUS 的 04h 功能报文，即读从站输入寄存器 xxxx（或 3xxxx）值。

第一步：选中 7#槽，然后双击“read 4 Words (3xxxx)”。7#槽中插入“read 4 Words (3xxxx) IB256..IB263”

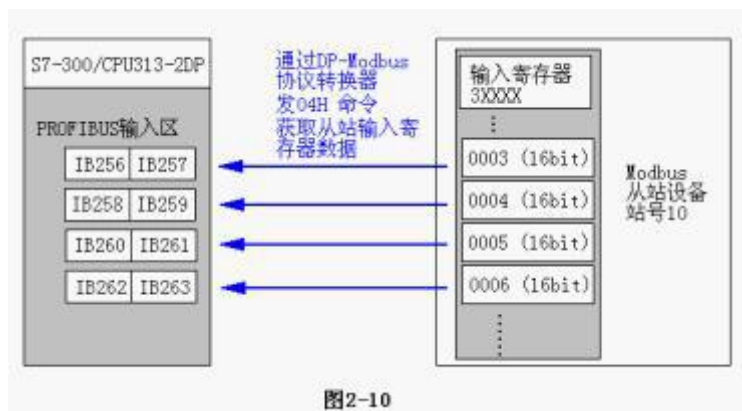
第二步：进一步设定 MODBUS 参数：双击 7#槽中的“read 4 Words (3xxxx)”，选择“Parameter Assigement”，完成“从站地址=10”和“起始地址=2”的参数设定。

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，本例为 10

起始地址：本例指要读取的 3XXXX 起始地址，注意：报文中寄存器起始地址 0000 对应设备中 30001 地址，其他顺延。

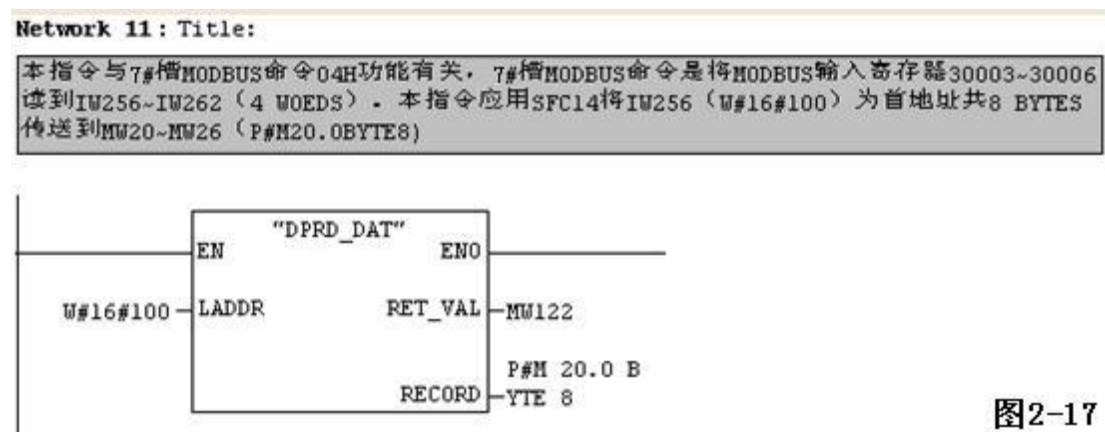
本例中的 2 对应设备中“输入寄存器 0003 地址”，也就是 30003 的地址[3XXXX]

PROFIBUS 地址与 MODBUS 地址对应关系：



在 STEP7 中对应的程序：

应用 SFC14 将 IW256-IW262 传送到 MW20-MW26；IW256-IW262 中的数据是 7#槽 MODBUS 的 04H 命令从 MODBUS 输入寄存器 30003-30006 读到的。



STEP7 在线监测可以看到 MW20-MW26 数据：1234、5678、9ABC、DEF1；这组数据来自 MODBUS30003-30006：

4	MW	20	HEX	W#16#1234
5	MW	22	HEX	W#16#5678
6	MW	24	HEX	W#16#9ABC
7	MW	26	HEX	W#16#DEF1

d. 举例说明在 8#槽中插入 “Write 16 bits (0xxxx)”

MODBUS 的 0Fh 功能报文，即将 16 个连续线圈 XXXX（或 0XXXX）强置为 ON/OFF 状态。

第一步：选中 8#槽，然后双击 “Write 16 bits (0xxxx)” 。8#槽中插入

“16D0 Write 16 bits (0xxxx) 1..2”

第二步：进一步设定 MODBUS 参数：双击 8#槽中的 “Write 16 bits (0xxxx)” ，选择

“Parameter Assigement”，完成 “从站地址=10”、

起始地址=20”参数的设定。

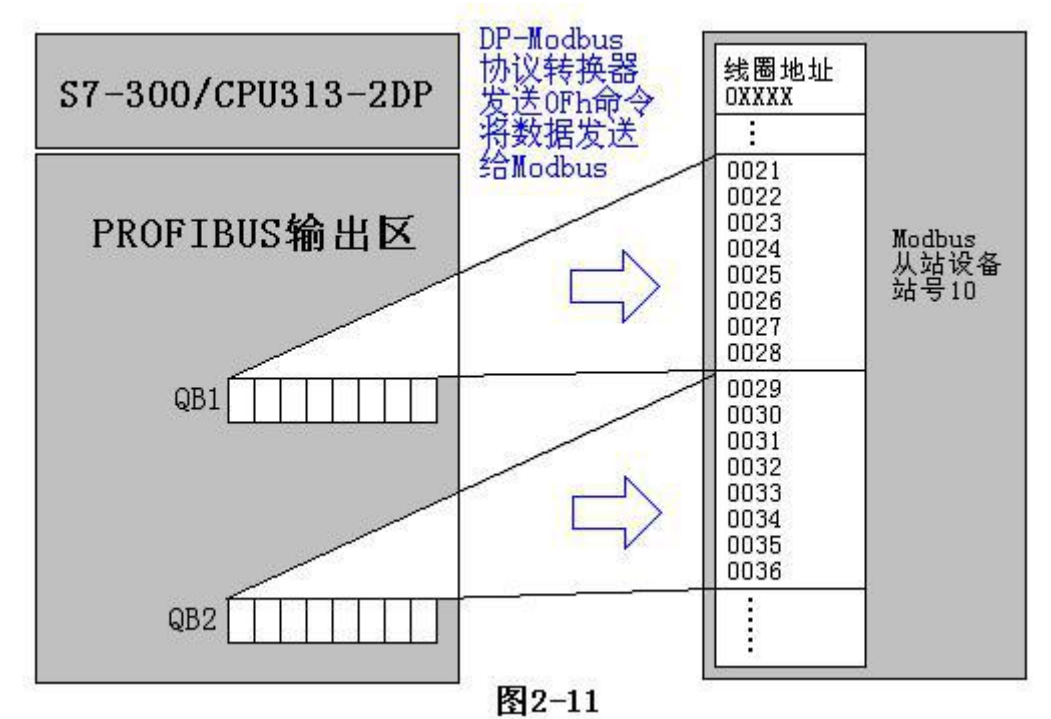
从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，本例为 10

起始地址：指要写入的 0xxxx 起始地址，注意：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。本例中的 20 对应设备中 “线圈 0021 地址”，也就是 00021 的地址 [0XXXX]

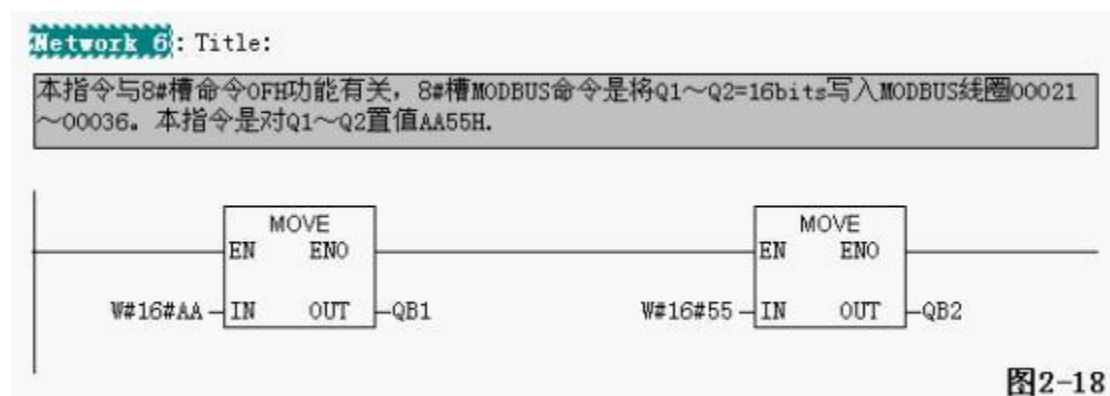
numbers 计数个数=16” 是模块缺省设置的，指要写入的输出线圈的个数，请不要改变！切记！

PROFIBUS 地址与 MODBUS 地址对应关系：

其中 Q1、Q2 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输出地址，共 2 Bytes，对应本 MODBUS 模块写入 MODBUS 设备的 16 个连续线圈，该 MODBUS 模块将 PROFIBUS 主站中 Q1、Q2 中 2Bytes (16 bits)值写入 MODBUS 设备的 0XXXX 数据区，起始地址本例为 00020；即将 PROFIBUS 的 Q1、Q2 写入 MODBUS 设备的 “线圈地址 0021-0036” 中，也就是 00021-00036[0XXXX]。



在 STEP7 中对应的程序:



e. 举例说明在 9#槽中插入 “write 4 Words (4xxxx)”

MODBUS 的 10h 功能报文，即预置从站 4 个保持寄存器 xxxx(或 4xxxx) 值。

第一步：选中 9#槽，然后双击 “write 4 Words (4xxxx)” 。9#槽中插入
“write 4 Words (4xxxx) QB256···QB263”

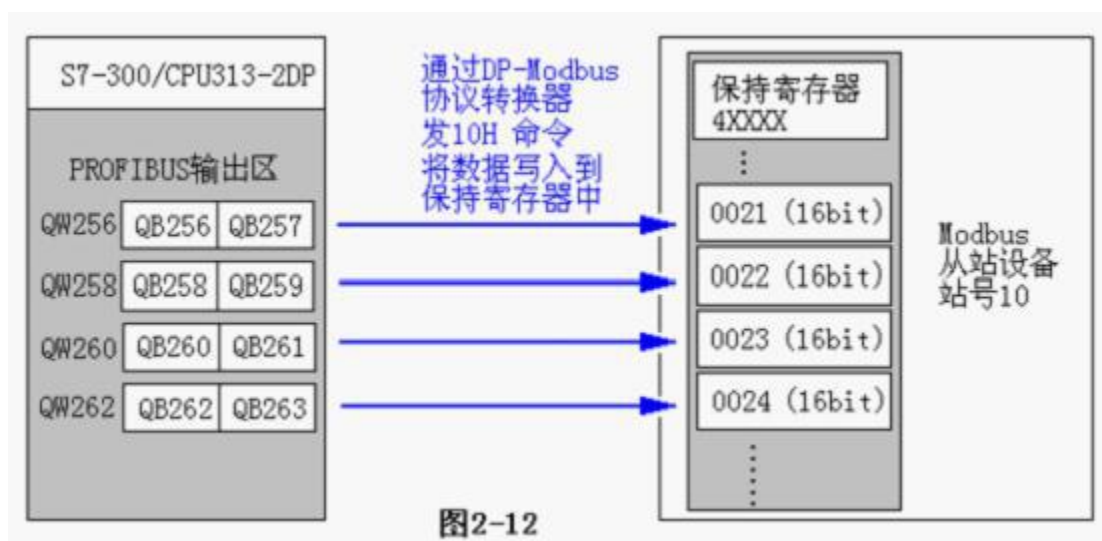
第二步：进一步设定 MODBUS 参数：双击 9#槽中的 “write 4 Words (4xxxx)” ， 选择
“Parameter Assigement”， 完成 “从站地址=10” 和 “起始地址=20” 的参数设定

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，本例为 10

起始地址：本例指要写入的 4XXXX 起始地址，注意：报文中保持寄存器起始地址 00000 对应设备中 40001 地址，其他顺延。本例中的 20 对应设备中 “保持寄存器 0021 地址”，也就是 40021 的地址[4XXXX]

PROFIBUS 地址与 MODBUS 地址对应关系：

其中 QB256..QB263 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输出地址共 8 Bytes，对应本 MODBUS 报文写到 MODBUS 设备中的 4 Words (4xxxx)



在 STEP7 中对应的程序:

Network 9 : Title:

本指令与9#槽MODBUS命令10H功能有关, 9#槽MODBUS命令是将QW256~QW262(4 WORDS)写入MODBUS保持寄存器40021~40024; 本指令应用SFC15将MW10为首地址 (P#M10.0 BYTE 8)共8 BYTES写入QW256(W#16#100), MW10~MW16的数据在上一级置入。

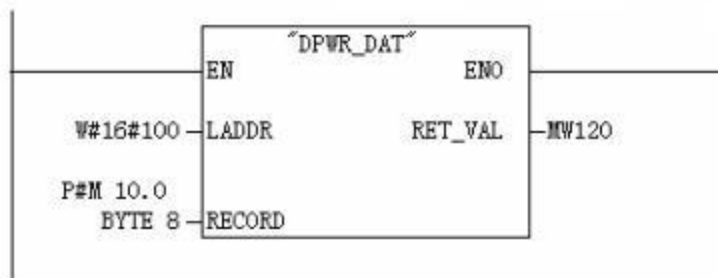


图2-19

f. 举例说明在10#槽中插入“Force single bit (05H Command)” MODBUS 的05h 功能报文, 即强置从站单线圈 XXXX (或 OXXXX) 值。

第一步: 选中10#槽, 然后双击“Force single bit (05H Command)”。10#槽中插入“8D0 Force single bit (05H Command) ”

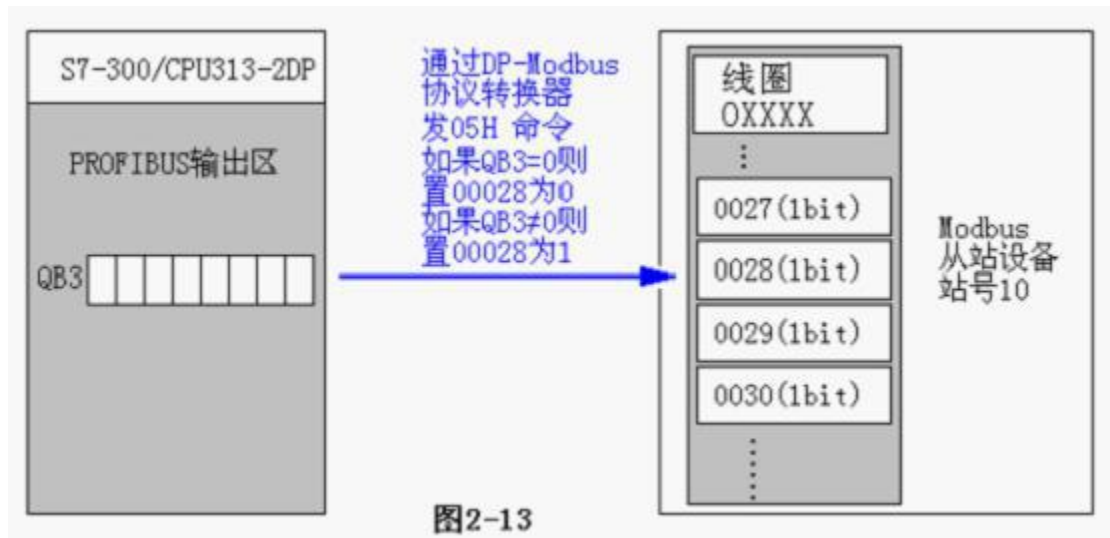
第二步: 进一步设定 MODBUS 参数: 双击10#槽中的“Force single bit (05H Command)”, 选择“Parameter Assigement”, 完成“从站地址=10”和“起始地址=27”的参数设定。

从站地址: 指本 MODBUS 报文发送到的 MODBUS 从站的地址, 本例为 10

起始地址: 本例指要写入的 0xxxx 起始地址。注意: 报文中线圈起始地址 00000 对应设备中 00001 地址, 其他顺延。本例中的 27 对应设备中“线圈 0028 地址”, 也就是 00028 的地址 [OXXXX]

PROFIBUS 地址与 MODBUS 地址对应关系: 见图

其中 QB3 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输出地址, 共 1 Byte, 对应本 MODBUS 模块写入 MODBUS 设备的单线圈 OXXXX, 该 MODBUS 模块根据 QB3 的值, 发送 MODBUS/05H 号命令, 将 MODBUS 设备的单线圈 OXXXX 置 1 或置 0。本例单线圈起始地址为 0027, 如果: QB3=0, 发单线圈 00028 置 0 命令; 若 Q3≠0, 发单线圈 00028 置 1 命令, 见下图:



在 STEP7 中对应的程序:

利用 I4.1 给 QB3 置 00/FF, 10#槽 MODBUS 05H 命令, 根据 QB3=00/FF, 将线圈 00028 置 0 或置 1。

Network 7: Title:

I4.1=按钮K1,用来选择置QB3=00/FF.本指令与10#槽MODBUS命令05H功能有关,10#槽MODBUS命令是:若QB3=0,将线圈00028(配置中起始地址=0027)置0;若QB3=FF,将线圈00028置1

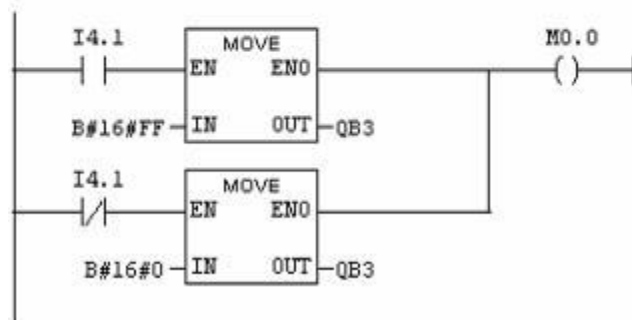


图2-20

g. 举例说明在 7#槽中插入 “set single word (06H command)”

MODBUS 的 06H 功能报文，即预置单保持寄存器 XXXX（或 4XXXX）的值。

第一步：选中 11#槽，然后双击 “set single word (06H command)”。11#槽中插入
“1A0 set single word (06H command) QB264…QB265”

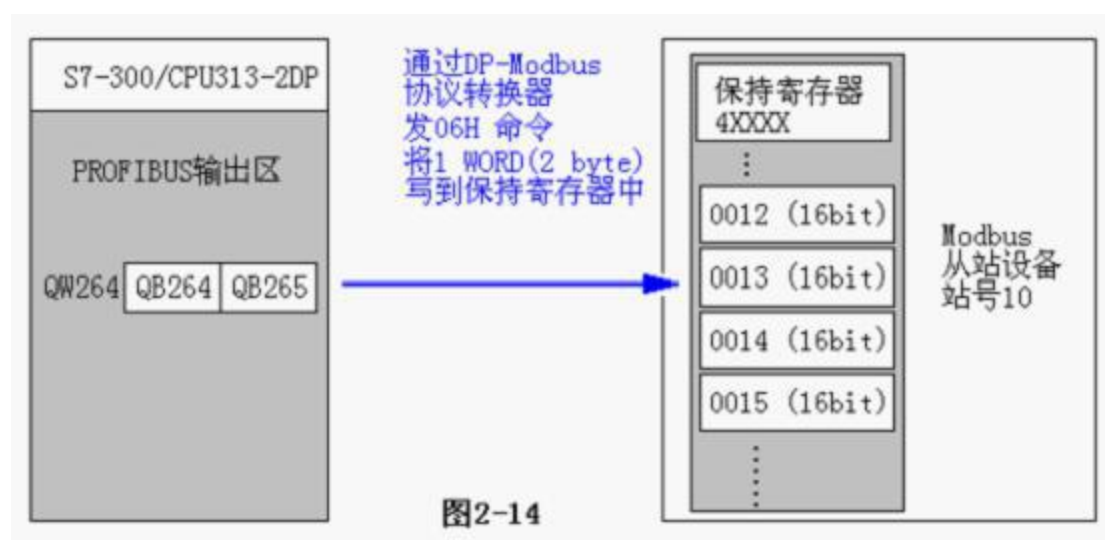
第二步：进一步设定 MODBUS 参数，双击 11#槽中的 “set single word (06H command)”，
选择 “Parameter Assigement”，完成 “从站地址=10” 和 “起始地址=12” 的参数设定

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，本例为 10

起始地址：本例指要写入的 4XXXX 起始地址，注意：报文中保持寄存器起始地址 0000 对应设备中 40001 地址，其他顺延。本例中的 12 对应设备中 “保持寄存器 0013 地址”，也就是 40013 的地址[4XXXX]

PROFIBUS 地址与 MODBUS 地址对应关系：

见图，其中 QB264..QB265 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输出地址共 2 Bytes，对应本 MODBUS 报文写到 MODBUS 设备中的 40013(4xxxx) 1 Word，见图 2-14：



在 STEP7 中对应的程序:

利用 I4.3 给 QW264 置值; 11#槽 MODBUS 06H 命令将 QW264 写到 MODBUS 保持寄存器 40013。

Network 10: Title:

I4.3=按钮K3, 用来选择置QW264 (1 WORDS) 为4040或1111, 本指令与11#槽MODBUS命令06H功能有关, 11#槽MODBUS命令是将QW264的数据写入MODBUS保持寄存器40013。(MODBUS起始地址配置为: 0012)

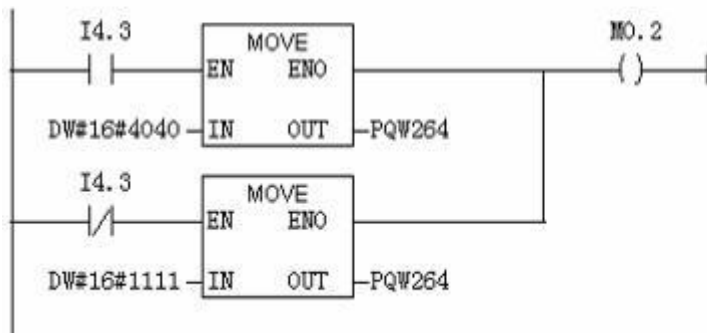


图2-21

h. “编译存盘”系统配置完毕

至此, 系统配置完毕, 可以编译存盘” Save and Compile” →退出, 见图 2-15:

4. 通信控制字与通信调试状态字

从 DP slave/Modbus master 的硬件配置中可以看到 1#-5#槽被接口占用, 1#-4#为通信调试状态字, 5#为通信控制字。1#槽是一个字节输入, 用作接口 MODBUS 通信的总状态字 status, 本例中占用 PROFIBUS 输入地址 IB0。总状态字 status: 是指所有报文的故障的汇总

D7:	D6:	D5:	D4:DP-Modbus	D3-D0:
parity_err	CRC_err	time out	connect	CODE_err

D7	[1:parity_err 奇偶校验错	0:正常]
D6	[1:CRC 校验错	0:正常]
D5	[1:modbus 从站现在规定应答时间内无响应	0:正常]
D4	[1:与 DP-Modbus 建立通讯连接	0:还未与 DP-Modbus 连接]
D3-D0	[XXXX:CODE_err 返回 modbus 从站异常码	0:正常]

2#-4#槽则是指某一条报文的故障信息：这是我们有别与其它厂家的优点

2#槽 roll_slot(循环滚动槽号) 是一个字节输入，用于循环显示配置插槽号，本例中占用 PROFIBUS 输入地址 IB1，它从 6#插槽到 11#插槽不断轮循，每 3 秒更新一次，与 3#槽和 4#槽配合使用，用于指示 3#槽和 4#槽中所显示的状态是针对 6#槽-11#槽的哪一条报文。

3#槽 roll_addr(循环滚动报文 modbus 从站地址)，它每 3 秒更新一次，与 2#槽配合使用，告诉调试人员当前显示的报文 modbus 从站地址。本例中占用 PROFIBUS 输入地址 IB2。

4#槽 roll_status(循环滚动报文命令返回信息)，它每 3 秒更新一次，与 2#槽配合使用，告诉调试人员当前显示的报文通讯状态。

本例中占用 PROFIBUS 输入地址 IB3。

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC 校验错	应答时间内无响应		modbus 从站异常码

5#槽是一个字节输出，用作接口 MODBUS 通信的控制字 control，本例中占用 PROFIBUS 输出地址 QB0，见上图 2-15。该字的最高位 D7，也就是本例的 Q0.7 如果置“1”，它将根据数据的变化进行寄存器的写操作，如果数据未发生任何变化则对 modbus 从站不进行寄存器写操作（仅对 0x06 0x10 功能码有效），这针对于一些仪表的系统参数设置是有次数限制的 FLASH 类型而专门设计的。而对于频繁变化的数据写操作请一定不要使用该控制位，即 D7 应为“0”。

通信控制字 control

D7:change write	D6:预留	D5:预留	D4:预留	D3:预留	D2:预留	D1:预留	D0:预留
-----------------	-------	-------	-------	-------	-------	-------	-------

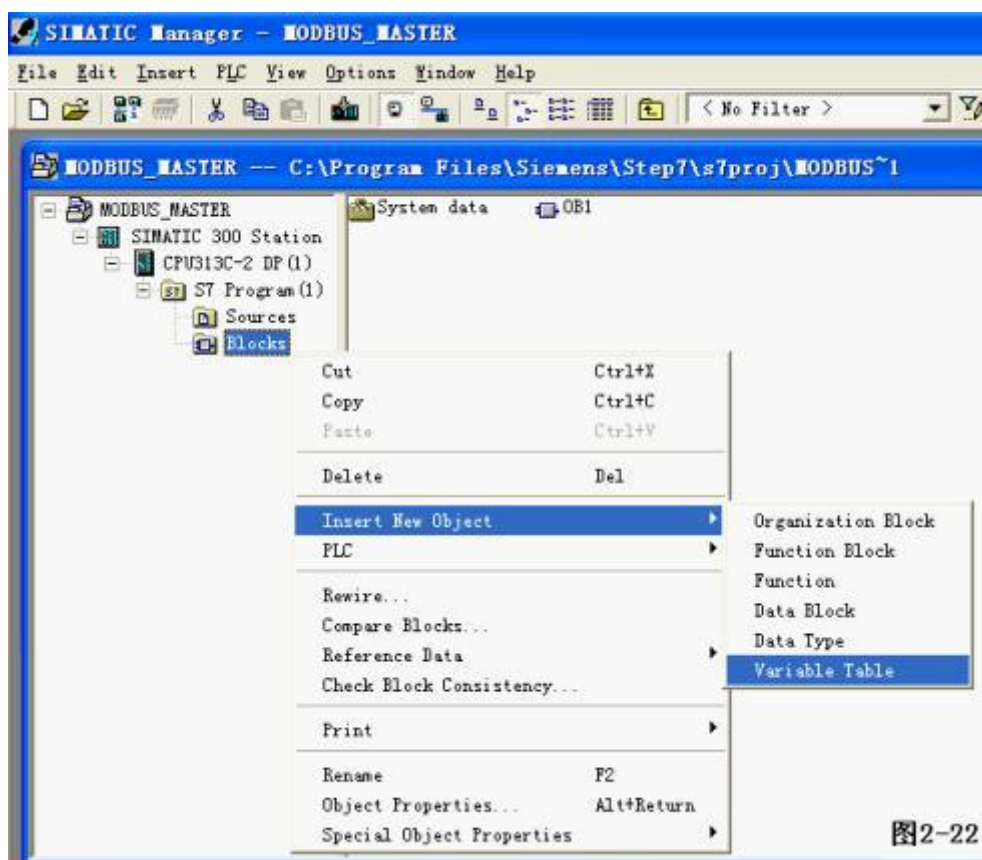
D7: 为“1”时,对 0x05 (只有最新版的模块,带 USB 口的,才有 0x05 功能码)、0x06 、 0x10 功能码的寄存器写操作时,只有数据发生变化时,才执行写操作,否则不向 modbus 从站发送写报文(仅对 0x06 、 0x10 功能码)

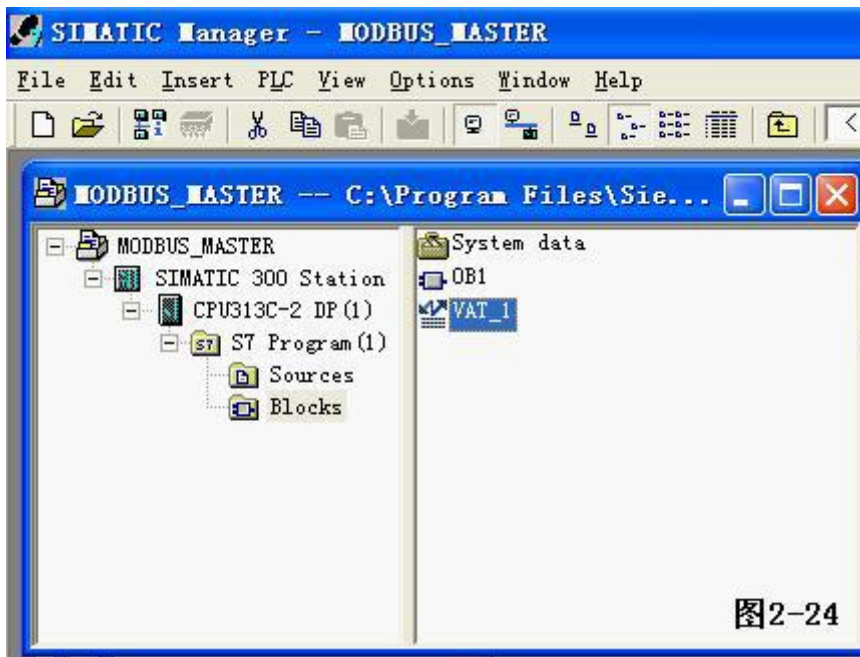
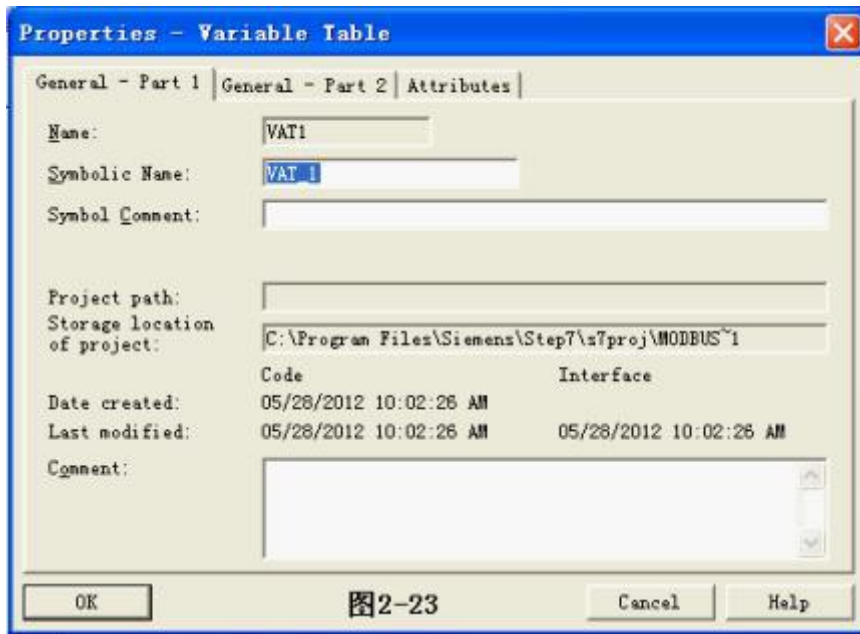
D7: 为“0”时,如果槽位中定义了 0x06 、 0x10 功能码的寄存器写操作,则周期性地发送写报文给 modbus 从站。(一般至少一秒一次,这与通讯波特率,报文条数,及等待应答时间有关)。

注: DP-MODBUS 转换器的“启停控制”不是通过通信控制字 control 进行控制的。而是由拨码开关的 1 号拨码进行启停控制。

5. 调试

安下图所示,Block->Insert New Object->Variable Table-> OK







用鼠标双击[VAT_1]， 然后

- (1)、 在 address 中写入 IB0， 在 Display format 中选 Binary 后回车[return]
- (2)、 在 address 中写入 IB1， 在 Display format 中选 Decimal 后回车[return]
- (3)、 在 address 中写入 IB2， 在 Display format 中选 Decimal 后回车[return]

(4) 、在 address 中写入 IB3，在 Display format 中选 Binary 后回车[return]

然后点击  存盘 save

之后就可以点击  在线监控本例的 status[对应 IB0] 、oll_slot[对应 IB1]、roll_addr[对应 IB2] 、roll_status [对应 IB3]

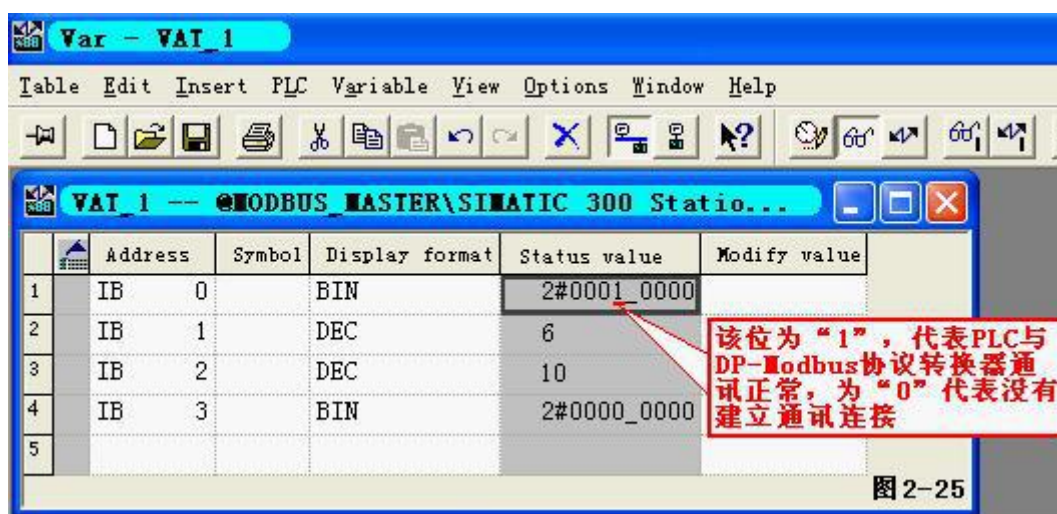


图 2-25

roll_slot 、roll_addr 、roll_status 每三秒刷新一次，并指向下一个槽号，从 6#槽到最后一个槽，不断循环。

举例说明：

1) 如果 roll_slot[本例 IB1]=6 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]=2#0010_0000(二进制表示 binary)

它的实际意义是：6#槽报文的 modbus 从站地址是 10，[2#0010_0000]

(D7 D6 D5 D4_D3 D2 D1 D0) 中的 D5=1，说明 从站 10 在应答时间内无响应。

roll_status

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

可能出现的问题是：

A: 从站设备 10, 不存在、或没有联接、或线路问题、或未接终端电阻。

B: 从站设备 10 的波特率与主站 (DP-Modbus 协议转换器) 不一致。

C: 等待回答时间设置过短, 可以改为 500ms 试一下, 见图 2-5【等待回答时间】。

2) 如果 roll_slot[本例 IB1]=7 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#0100_0000(二进制表示 binary)

它的实际意义是: 7#槽报文的 modbus 从站地址是 10, [2#0100_0000]

(D7 D6 D5 D4_D3 D2 D1 D0) 中的 D6=1, 说明 从站 10 的应答报文出现 CRC 校验错。

roll_status

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

可能出现的问题是线路问题、或未接终端电阻、或通讯线路有强干扰。

3) 如果 roll_slot[本例 IB1]=8 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#1000_0000(二进制表示 binary)

它的实际意义是: 8#槽报文的 modbus 从站地址是 10, [2#1000_0000]

(D7 D6 D5 D4_D3 D2 D1 D0) 中的 D7=1, 说明 从站 10 的应答报文出现奇偶校验错。

roll_status

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

4) 如果 roll_slot[本例 IB1]=9 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#0000_0001(二进制表示 binary)

它的实际意义是：9#槽报文的 modbus 从站地址是 10， [2#0000_0001]

(D7 D6 D5 D4_D3 D2 D1 D0) 中的D0=1,说明 从站 10 不支持 9#槽报文的 功能码 。

roll_status

D7:parity_err

D6:CRC_err

D5:time out

D4:预留

D3-D0:CODE_err

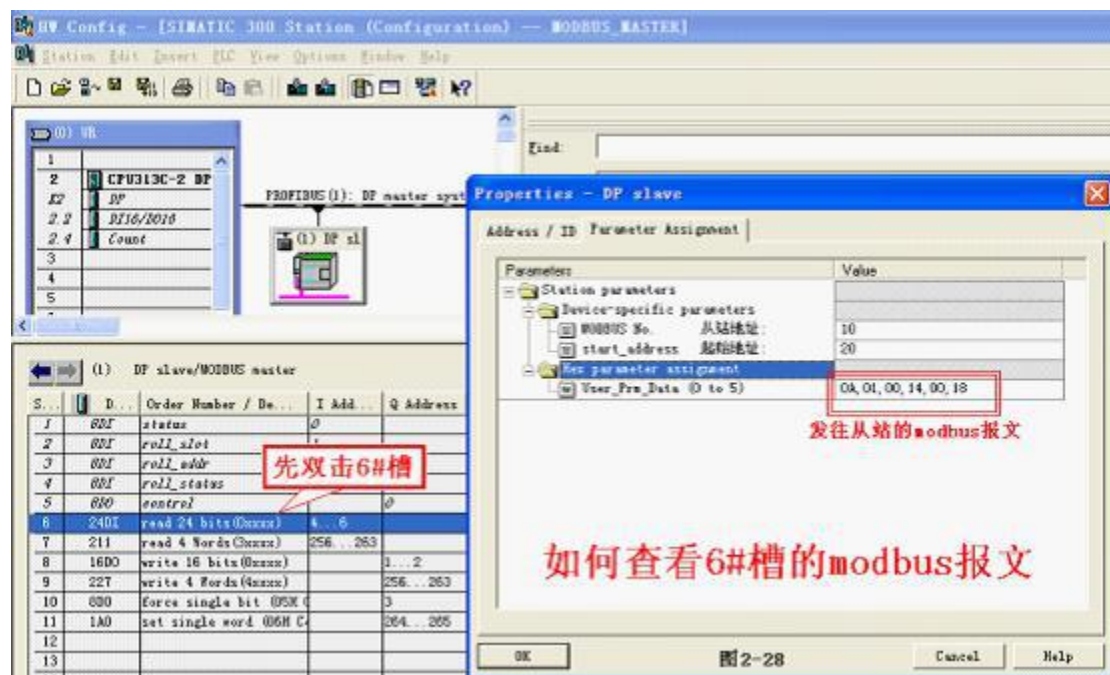
奇偶校验错

CRC校验错

应答时间内无响应

modbus从站异常码

Modbus 从站发回异常码 01，表明不支持该报文的 功能码，请检查 9#槽报文，参见图 2-28，[查看 6#槽 modbus 报文举例]



5) 如果 roll_slot[本例 IB1]=9 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#0000_0011(二进制表示 binary)

它的实际意义是：9#槽报文的 modbus 从站地址是 10, [2#0000_0011]

(D7 D6 D5 D4 D3 D2 D1 D0) 中的 D1=1, D0=1, 说明 9#槽报文输入或输出数量有误或超限。

roll_status

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

6) 如果 roll_slot[本例 IB1]=9 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#0000_0010(二进制表示 binary)

它的实际意义是：9#槽报文的 modbus 从站地址是 10, [2#0000_0010]

(D7 D6 D5 D4 D3 D2 D1 D0) 中的 D1=1, 说明 9#槽报文起始地址或终止地址有误或超限。

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

Modbus 从站发回异常码 02, 表明报文起始地址或终止地址有误或超限, 请检查 9#槽报文, 参见图 2-28

7) 如果 roll_slot[本例 IB1]=9 (十进制表示 DEC)

roll_addr[本例 IB2]=10 (十进制表示 DEC)

roll_status[本例 IB3]= 2#0000_0100(二进制表示 binary)

它的实际意义是：9#槽报文的 modbus 从站地址是 10，[2#0000_0100]

(D7 D6 D5 D4_D3 D2 D1 D0) 中的 D2=1, 说明 modbus 从站设备异常，无法响应。

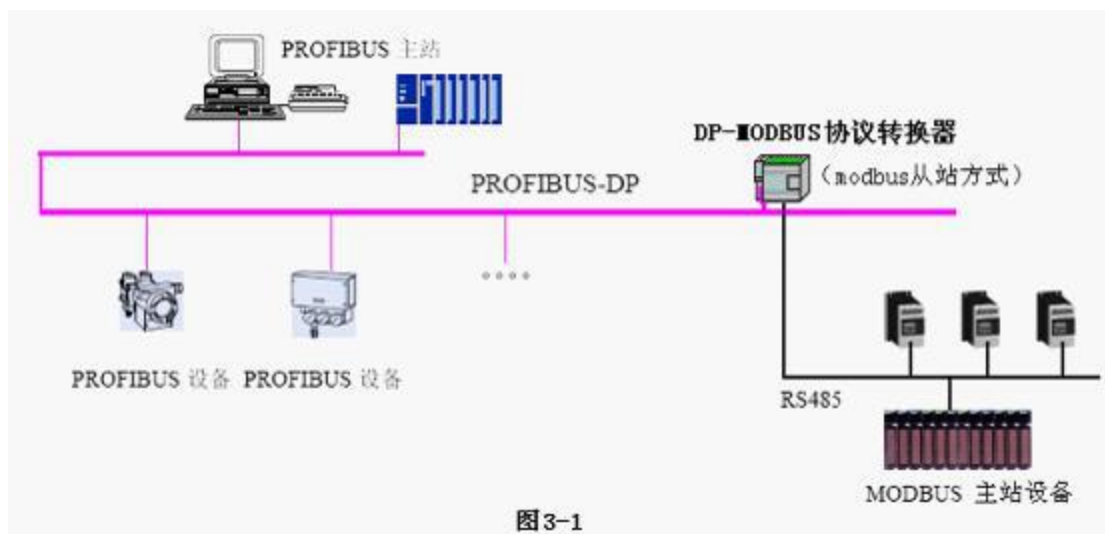
roll_status

D7:parity_err	D6:CRC_err	D5:time out	D4:预留	D3-D0:CODE_err
奇偶校验错	CRC校验错	应答时间内无响应		modbus从站异常码

Modbus 从站发回异常码 04，表明 modbus 从站设备异常，无法响应，请联络 modbus 从站设备厂家！

4 DP-Modbus 转换器作为 modbus 从站的使用说明

作为 modbus 从站的主要功能就是为其他 modbus 主站（如：PLC, 上位机等）提供 modbus 从站应答服务，支持 01H、02H、03H、04H、05H、06H、0FH、10H 号功能。



1. 将大连德嘉提供的 GSD 文件 D_SLAVE.GSD 拷贝到 Step7\S7data\gsd\目录下；产品图标 DS007_N.BMP 和 DS007_S.BMP 文件拷贝到 Step7\S7data\nsbmp\ 目录下：

注：以上的详细目录在 XP 系统中分别是：

C:\Program Files\Siemens\Step7\S7DATA\GSD

C:\Program Files\Siemens\Step7\S7DATA\nsbmp

Win7 系统中分别是

C:\Program Files (x86)\Siemens\Step7\S7DATA\GSD

C:\Program Files (x86)\Siemens\Step7\S7DATA\NSBMP

2. 在 STEP7 上通过向导 ‘New Project’ Wizard 建立一个“项目”，CPU 类型选择 CPU313C-2DP，项目名字叫“MODBUS_SLAVE”

3. 在 STEP7 的硬件组态中的设置：

1) SIMATIC 300 Station→Hardware 双击，并在 HW Config 的菜单中选择 Option→Update Catalog 点击，将设备 GSD 文件加入设备 Catalog 中，见图 3-2。



图3-2

2) 配置 PROFIBUS：双击 CPU 槽位中的 DP，→属性→new→Network Settings→187.5K→OK，如图 3-3

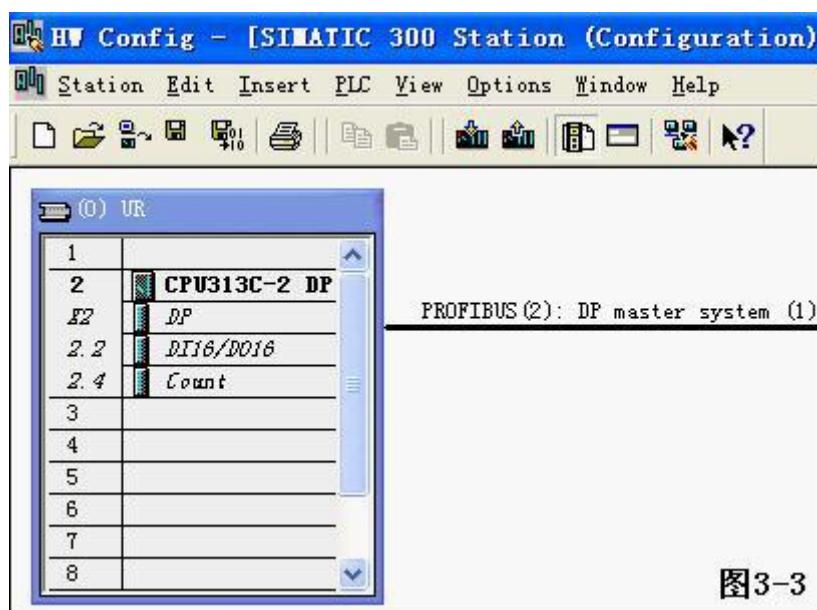


图3-3

3) 配置 DP-Modbus 协议转换器作为 PROFIBUS 从站

选中 PROFIBUS(1) DP master system(1), 使其选中横线变黑, 打开 Hardware Catalog → PROFIBUS DP → Additional Field Devices → Gateway → DP slave/MODBUS slave 双击; 然后选择 DP 从站站号, 本例选择从站站号为: 100 → “OK”

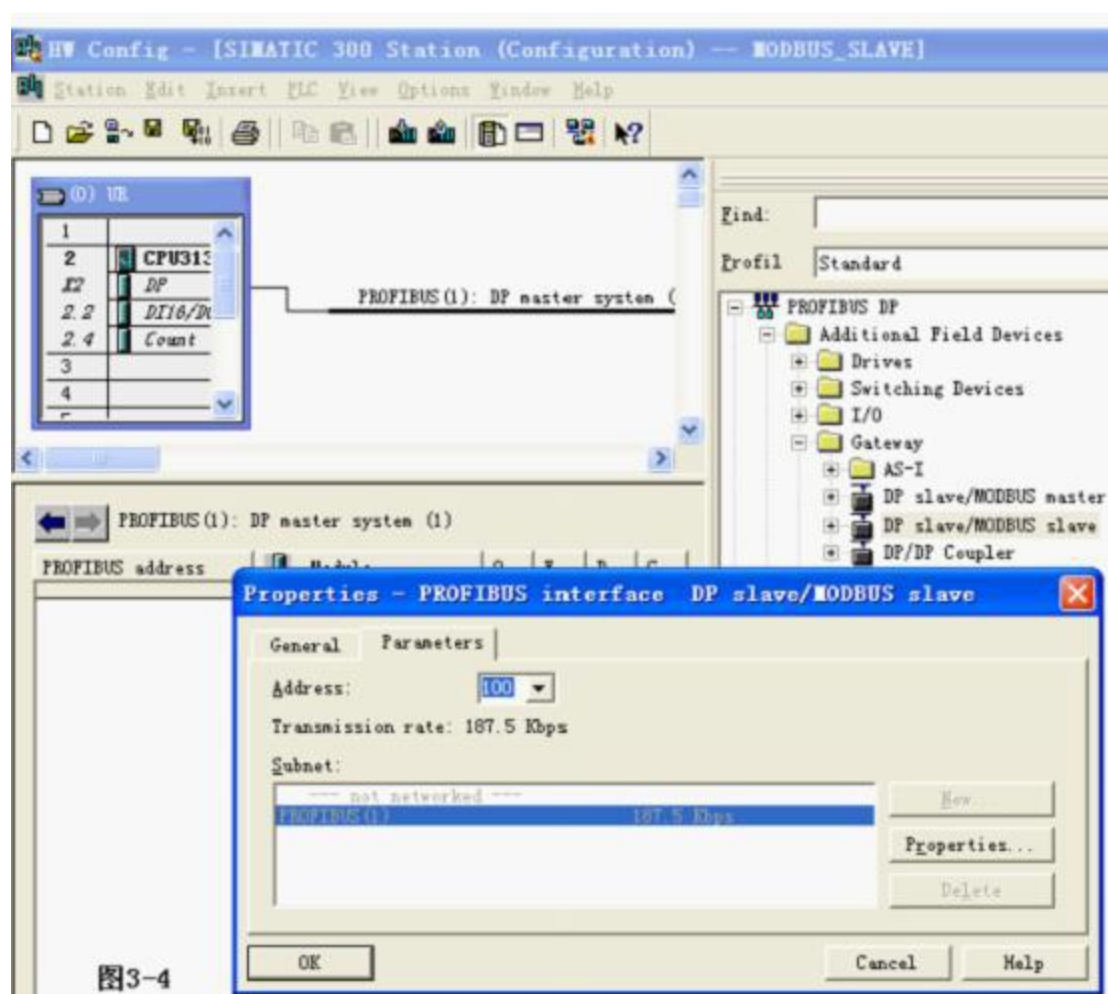
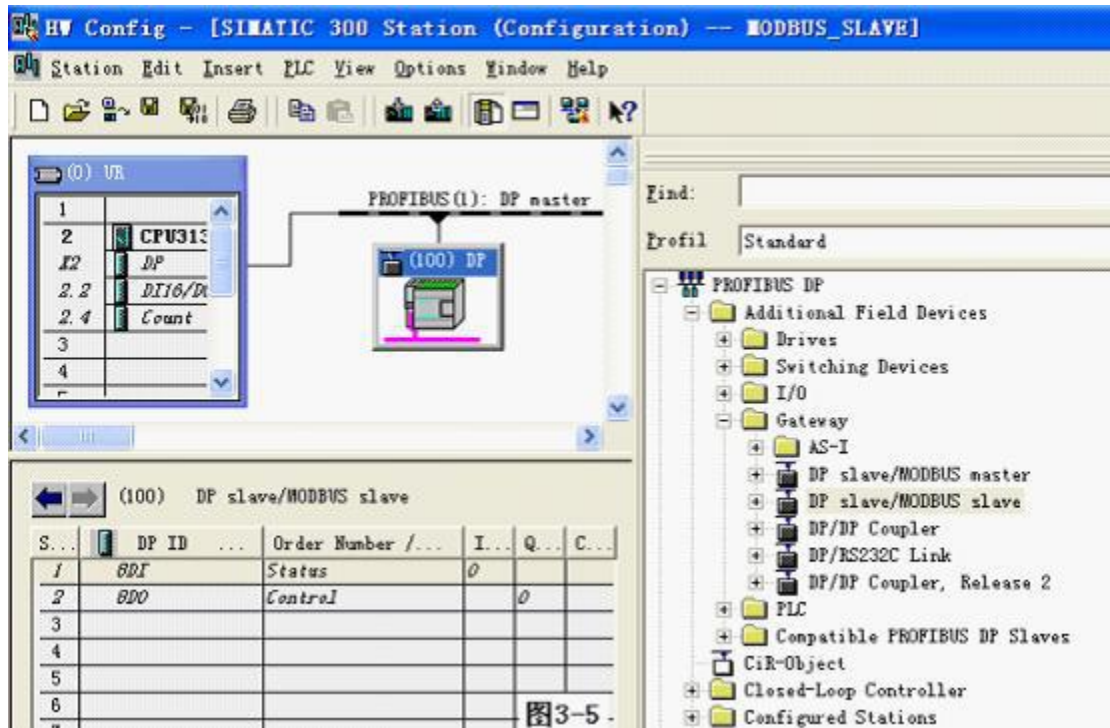
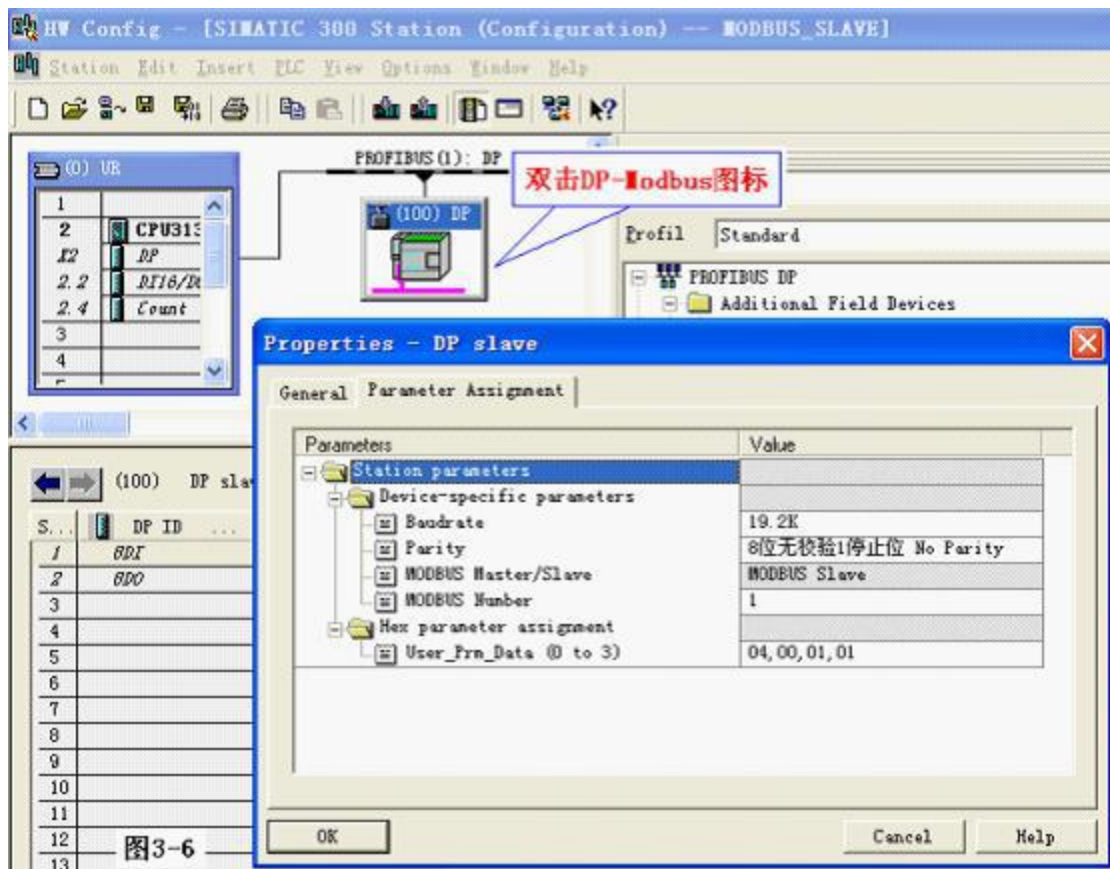


图3-4



- 4) 配置 DP-Modbus 协议转换器的 modbus 侧 RS485 接口，双击 DP-Modbus 图标，出现如图 3-6 的窗口，选择 Parameter Assignment。



“Baudrate” [波特率]和“Parity” [校验]: 必须设置的和您要连接的 Modbus 主站设备的一致, 否则 DP-Modbus 协议转换器和你要连接的设备无法通讯。

“MODBUS Master/Slave” [主/从]: 产品设置成从站, 使用 GSD 文件 D_SLAVE.GSD, 只能选择 MODBUS 从站方式。[用户无法改变]

“Modbus Number” [DP-Modbus 协议转换器 modbus 站号]: 本例为 1。

5) 建立 PROFIBUS 输入/输出与 MODBUS 存储区通讯映射关系

D_SLAVE 有 1#--20#共 20 个槽 (逻辑上, 非物理设备); 1#、2#槽已占用, 剩下 18 个槽提供用户使用, 建立一个 PROFIBUS 输入/输出与 MODBUS 存储区对应关系表。每个槽是关系表的一项; 所以该关系表最多有 18 项。再看 Hardware catalog 中打开 DP slave/MODBUS slave 目录, DP slave/MODBUS slave 下每一个模块可以作为关系表中的一项, 双击可插入在某一个槽中。如图 3-7 所示

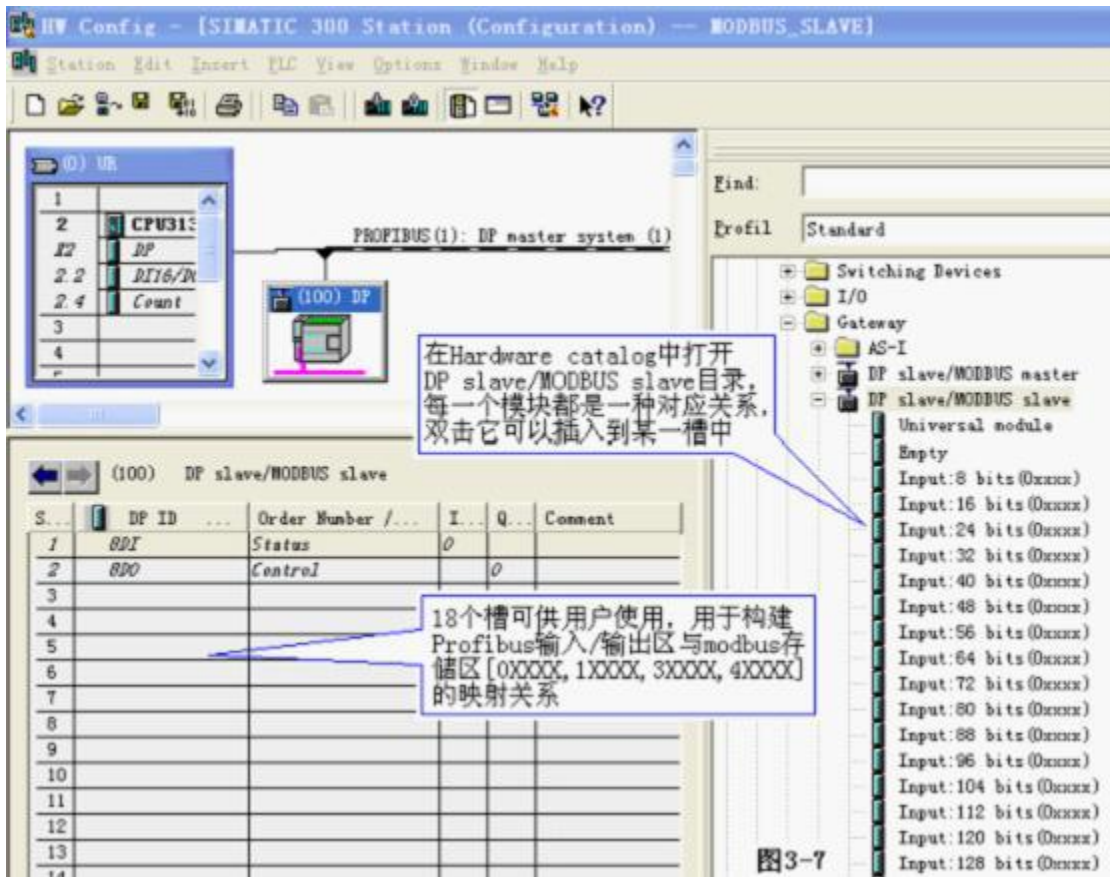


图3-7

- a. 举例说明在 3#槽中插入“Input:32 bits (0xxxx)” — 建立 MODBUS 线圈 0XXXX 与 PROFIBUS 输入的联系。选中 3#槽，然后双击“Input:32 bits (0xxxx)”。3#槽中插入“32DI Input:32 bits (0xxxx) IB1…IB4”，见图 3-8

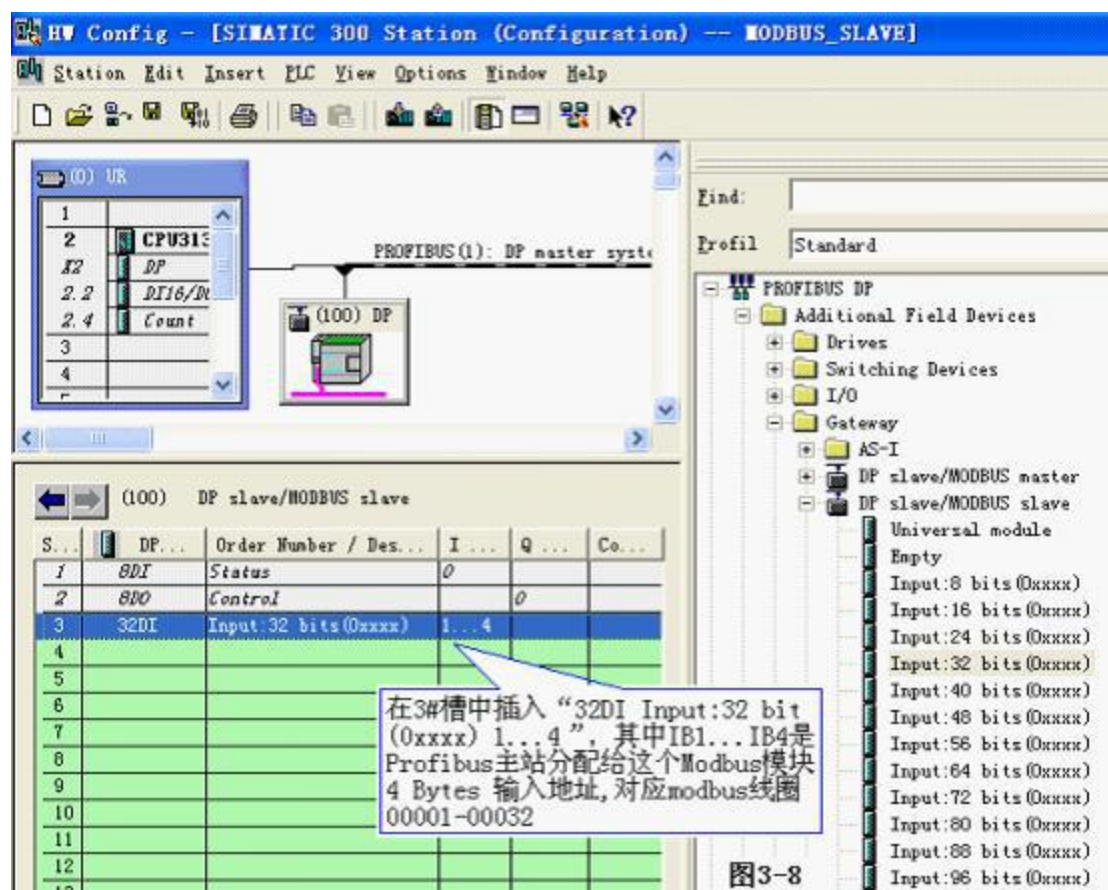


图3-8

本 MODBUS 模块建立了 PROFIBUS I1.0-I4.7(该地址由 PROFIBUS 主站自动分配,共 4×8=32bits)与 MODBUS 线圈 0000100032 的对应关系,即: PROFIBUS 的 I1.0-I4.7 可以读到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 线圈 00001-0032 的状态。见图 3-9。

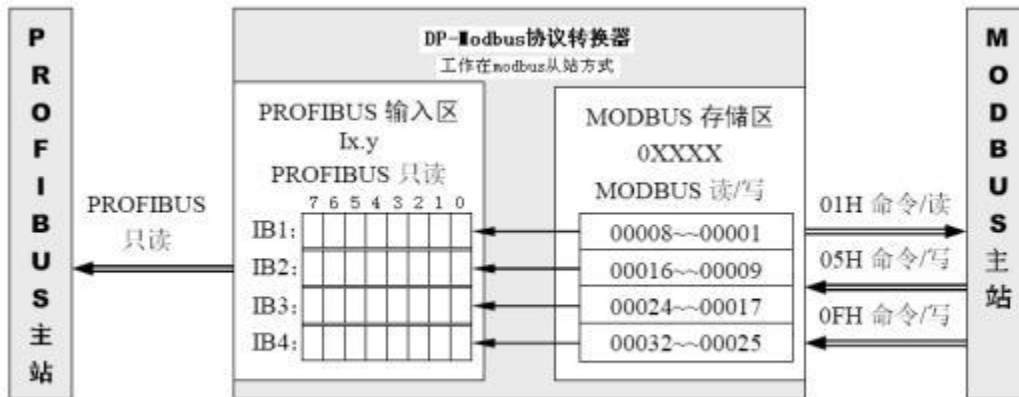


图3-9

注意：MODBUS 一侧线圈地址一定是从 00001 开始的。如果再插入有一项 “Input:32 bits in (0xxxx)”，则 MODBUS 线圈地址顺序连续分配，即从 000033-0064。详见 “E. 说明在 7 槽中插入 “Input:32 bits (0xxxx)” — 再建立一项 MODBUS 线圈 0XXXX 与 PROFIBUS 输入的联系”。

- b. 说明在 4#槽中插入 “Output: 32 bits (1xxxx)” — 建立 MODBUS 离散量输入 1XXXX 与 PROFIBUS 输出的联系选中 4#槽，然后双击 “Output:32 bits (1xxxx)” 。4#槽中插入 “32D0 Output:32 bits (1xxxx) QB1..QB4”。本 MODBUS 模块建立了 PROFIBUS Q1.0-Q4.7(该地址由 PROFIBUS 主站自动分配,共 4× 8=32BITS)与 MODBUS 离散量输入 10001-10032 的对应关系，即：PROFIBUS 的输出数据 Q1.0-Q4.7 可以写到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 离散量输入区 10001-10032，见图 3-10 所示。

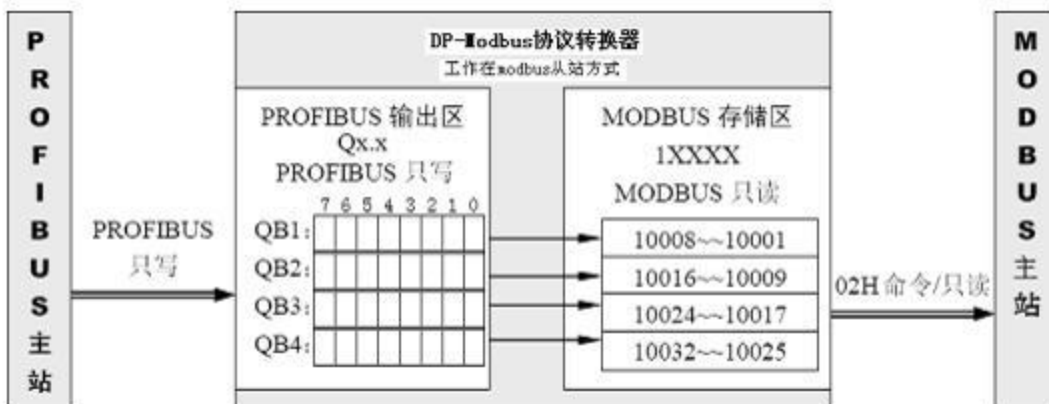


图3-10

注意：MODBUS 一侧离散量输入地址一定是从 10001 开始的。如果再插入一项“Output:32 bits (1xxxx)”，则 MODBUS 离散量输入地址连续顺序分配，即从 10033-10064；详见“F. 举例说明在 8#槽中插入“Output:32 bits (1xxxx)”——再建立一项 MODBUS 离散量输入 1XXXX 与 PROFIBUS 输出的联系”。

- c. 举例说明在 5#槽中插入“Input:8 Words (4xxxx)”——建立 MODBUS 保持寄存器 4XXXX 与 PROFIBUS 输入的联系。选中 5#槽，然后双击“Input:8 Words (4xxxx)”，5#槽中插入“215 Input:8 Words (4xxxx) IB256..IB271”。本 MODBUS 模块建立了 PROFIBUS 输入 IW256-IW270(该地址由 PROFIBUS 主站自动分配，8 Words)与 MODBUS 保持寄存器 40001-40008 的对应关系；即：PROFIBUS 的 IW256-IW270(8 Words)可以读到(DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 保持寄存器 40001-40008 中的数据，见图 3-11

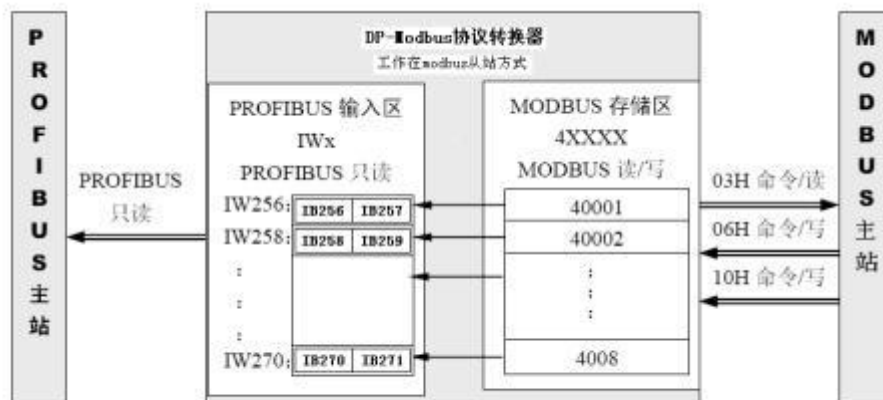


图3-11

注意：MODBUS 一侧保持寄存器地址一定是从 40001 开始的。如果再插入有一项“Input:6 Words (4xxxx)”，则 MODBUS 保持寄存器地址顺序连续分配，即从 40009 开始；详见“G. 举例说明在 9#槽中插入“Input:6 Words (4xxxx)”——再建立一项 MODBUS 保持寄存器 4XXXX 与 PROFIBUS 输入的联系”。

在 STEP7 中对应的程序：

```
Network 4 : Title:
使用SFC14读IW256-IW270 送到MW20-MW34. 这 8 WORDS 与MODBUS 40001-40008对应:
(注:LADDER=100H=256.)
```

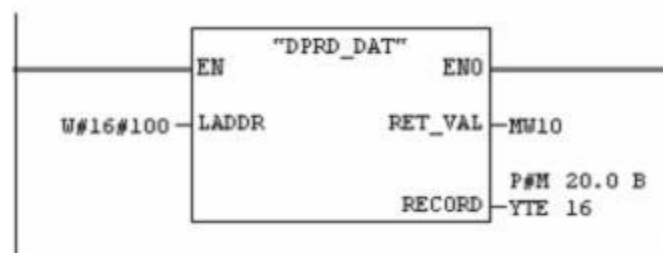


图3-11b

- d. 举例说明在 6#槽中插入“Output:4 Words (3xxxx)”——建立 MODBUS 输入寄存器 3XXXX 与 PROFIBUS 输出的联系选中 6#槽,再双击“Output:4 Words (3xxxx)”,6#槽中插入“227 Output:4 Words (3xxxx) QB256..QB263”。本 MODBUS 模块建立了 PROFIBUS QW256-QW262(该地址由 PROFIBUS 主站自动分配,共 4 Words)与 MODBUS 输入寄存器 30001-30004 的对应关系,即: PROFIBUS 的输出数据 QW256-QW262 可以写到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 输入寄存器区 30001-30004,见图 3-12 所示。

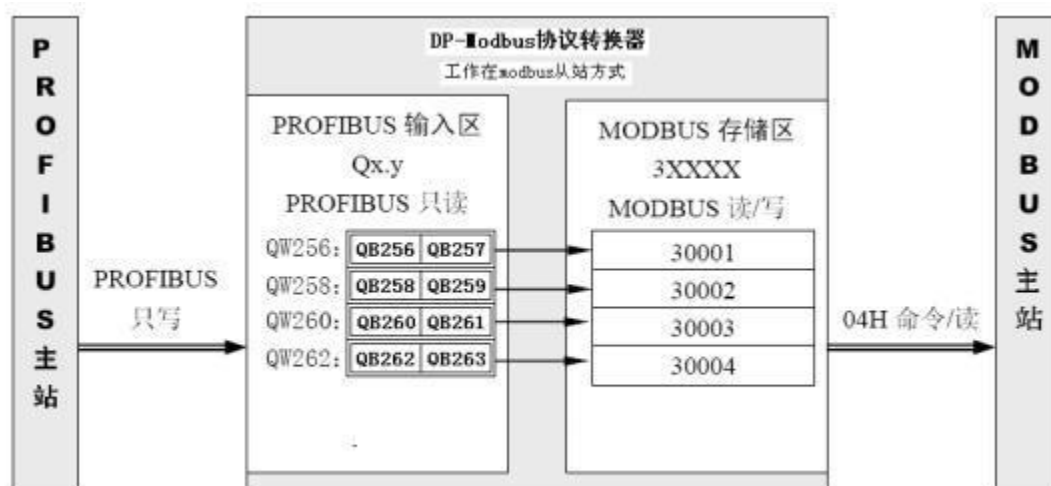


图3-12

注意: MODBUS 一侧输入寄存器地址一定是从 30001 开始的。如果再插入一项“Output:4 Words (3xxxx)”,则 MODBUS 输入寄存器地址顺序连续分配,即从 30005 开始。详见“H. 举例说明在 10#槽中插入“Output:8 Words (3xxxx)”——再建立一项 MODBUS 输入寄存器 3XXXX 与 PROFIBUS 输出的联系”。

在 STEP7 中对应的程序:

Network 7: Title:

使用SFC15将MW60~MW66共4 WORDS写入QW256~QW262, 这4 WORDS 与MODBUS 30001~30004对应;
(注: LADDER=100H=256)

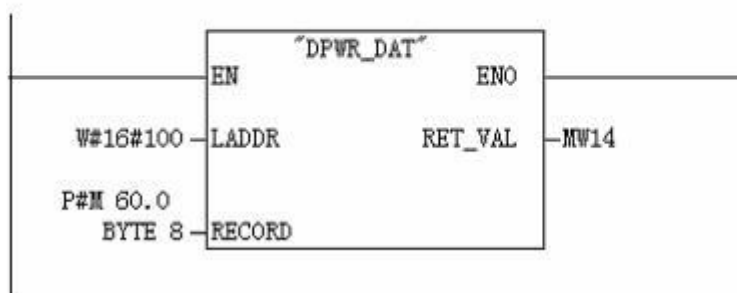


图3-12b

- e. 举例说明在 7#槽中插入“Input:32 bits (0xxxx)” — 再建立一项 MODBUS 线圈 0XXXX 与 PROFIBUS 输入的联系选中 7#槽,然后双击“Input:32 bits (0xxxx)”,7#槽中插入“32DI Input:32 bits (0xxxx) IB5..IB8”。本 MODBUS 模块又建立了一项 PROFIBUS 输入 I5.0-I8.7(该地址由 PROFIBUS 主站自动分配,共 4×8=32bits)与 MODBUS 线圈 0XXXX 的联系。

注意: MODBUS 一侧的地址是连续顺序分配的, 3#槽设定的 MODBUS 线圈地址是 00001-00032, 因此, 本模块对应的 MODBUS 线圈地址是 00033-00064。即: PROFIBUS 的 I5.0-I8.7 可以读到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 线圈 00033-00064 的状态, 见图 3-13 所示:

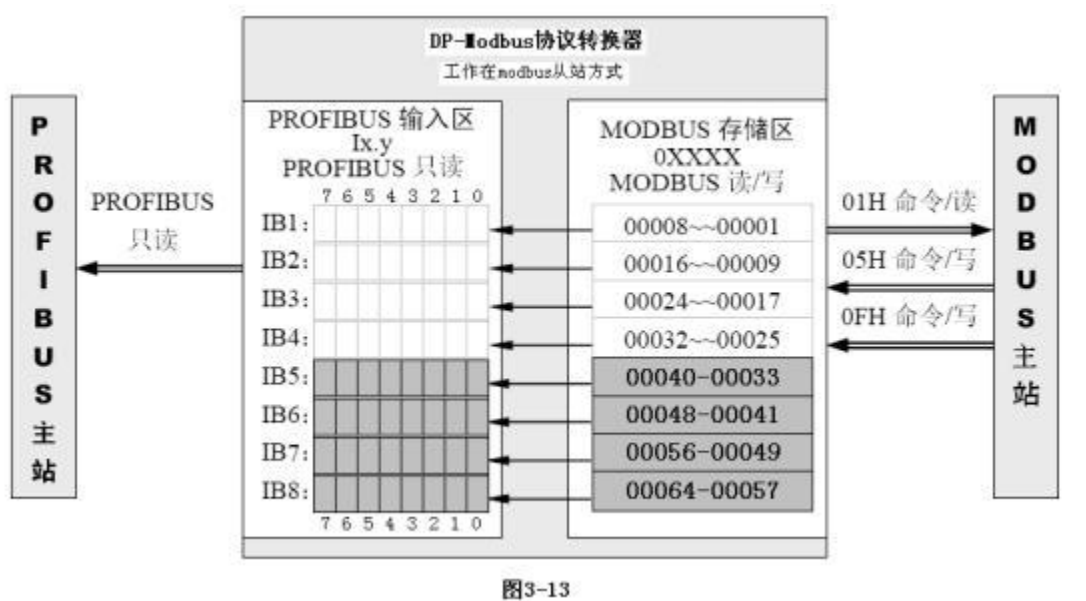


图3-13

- f. 举例说明在 8#槽中插入“Output:32 bits (1xxxx)” — 再建立一项 MODBUS 离散量输入 1XXXX 与 PROFIBUS 输出的联系选中 8#槽, 然后双击“Output:32 bits (1xxxx)”。8#槽中插入“32DO Output:32 bits (1xxxx) QB5..QB8”本 MODBUS 模块又建立了一项 PROFIBUS 输出 Q5.0-Q8.7(该地址由 PROFIBUS 主站自动分配,共 4×8=32 bits)与 MODBUS 离散量输入 1XXXX 的联系。

注意: MODBUS 一侧地址是连续顺序分配的, 3#槽设定的 MODBUS 离散量输入地址是 10001-10032, 因此, 本模块对应的 MODBUS 离散量输入地址是 10033-10064。即: PROFIBUS 的输出数据 Q5.0-Q8.7 可以写到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 离散量输入区 10033-10064, 见图 3-14。

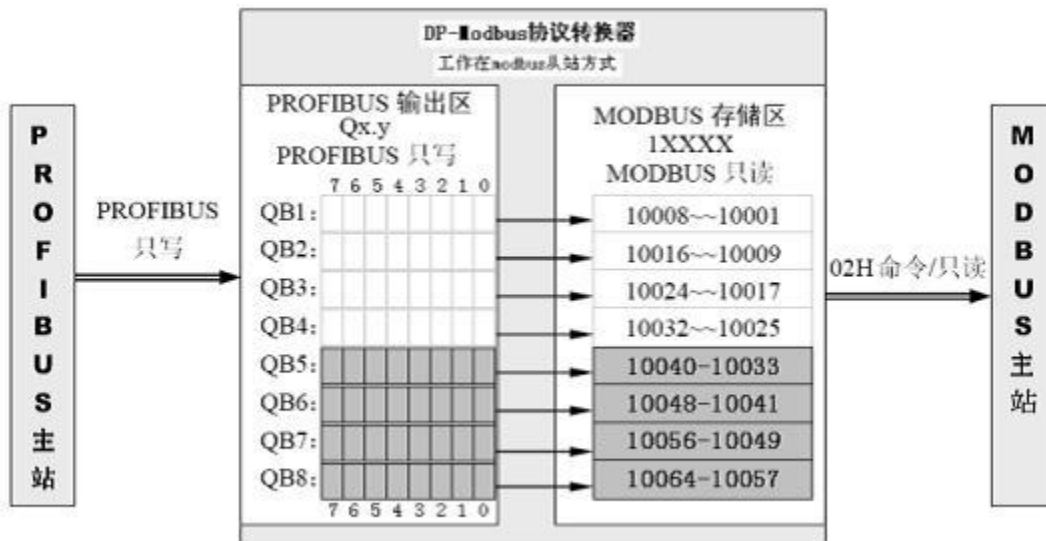


图3-14

- g. 举例说明在 9#槽中插入 “Input:6 Words (4xxxx)” — 再建立一项 MODBUS 保持寄存器 4XXXX 与 PROFIBUS 输入的联系选中 9#槽, 然后双击 “Input:6 Words (4xxxx)” 。9#槽中插入 “213 Input:6 Words (4xxxx) IB272..IB283” 。本 MODBUS 模块又建立了一项 PROFIBUS 输入 IW272-IW282 (该地址由 PROFIBUS 主站自动分配, 共 6 Words) 与 MODBUS 保持寄存器 4XXXX 的联系。

注意: MODBUS 一侧地址的顺序是连续分配的, 5#槽设定的 MODBUS 保持寄存器地址是 40001-40008, 因此, 本模块对应的 MODBUS 保持寄存器地址是 40009-40014。即: PROFIBUS 的 IW272-IW282 可以读到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 保持寄存器 40009-40014 的数据, 见图 3-15 所示

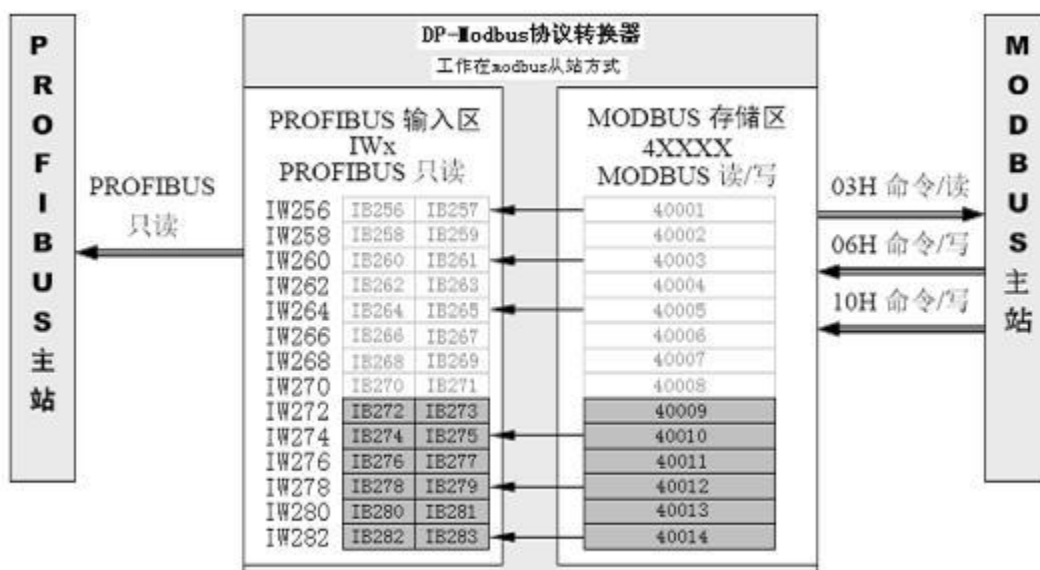


图3-15

在 STEP7 中对应的程序:

Network 5: Title:

使用SFC14读IW272~IW282送到MW36~MW46。这6 WORDS与MODBUS 40009~40014对应; (注: LADDR=110H=272)

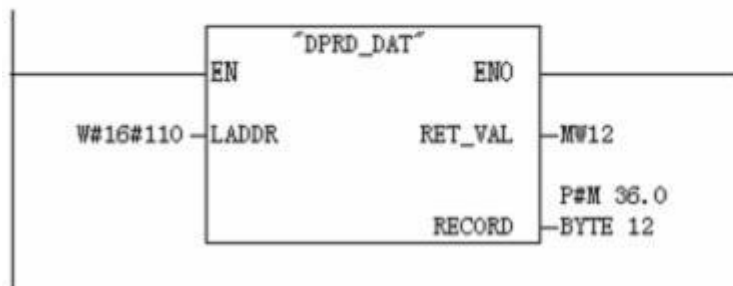


图3-15b

- h. 举例说明在 10#槽中插入 “Output:8 Words (3xxxx)” — 再建立一项 MODBUS 保持寄存器 3XXXX 与 PROFIBUS 输入的联系选中 10#槽, 然后双击 “Output:8 Words (3xxxx)”, 10#槽中插入 “231 Output:8 Words (3xxxx) QB264..QB279”。本 MODBUS 模块又建立了一项 PROFIBUS 输出 QB264-QB279 (该地址由 PROFIBUS 主站自动分配, 共 8 words) 与 MODBUS 输入寄存器 3XXXX 的联系。

注意: MODBUS 一侧地址顺序是连续分配的; 6#槽设定的 MODBUS 输入寄存器地址是 30001-30004, 因此本模块对应的 MODBUS 输入寄存器地址是 30005-30012。即: PROFIBUS 的输出数据 QW264-QW278 可以写到 (DP-Modbus 协议转换器作为 modbus 从站时内部的) MODBUS 输入寄存器区 30005-30012, 见图 3-16。

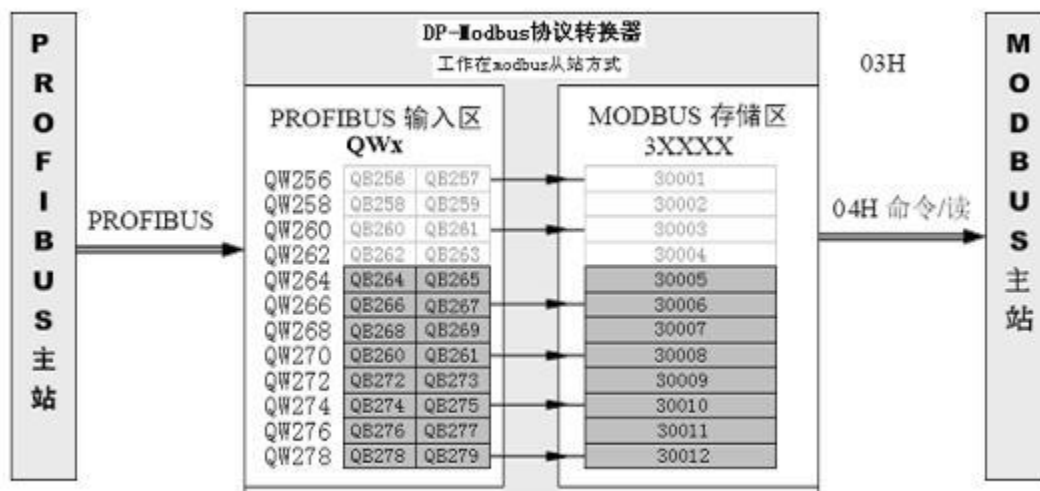


图3-16

在 STEP7 中对应的程序:

Network 8: Title:

使用SFC15将MW68~MW82共8 WORDS写入QW264~QW278, 这8 WORDS 与MODBUS 30005~300012对应; (注: LADDER=108H=264)

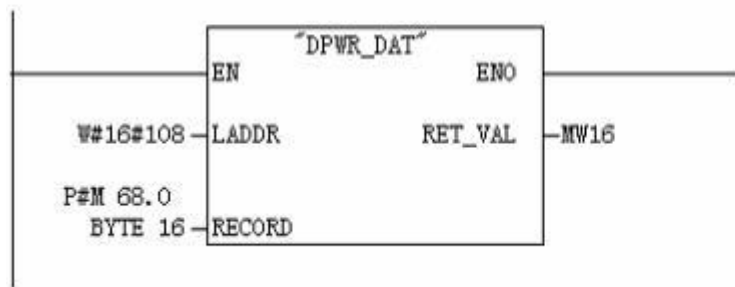


图3-16b

i. “编译存盘”系统配置完毕

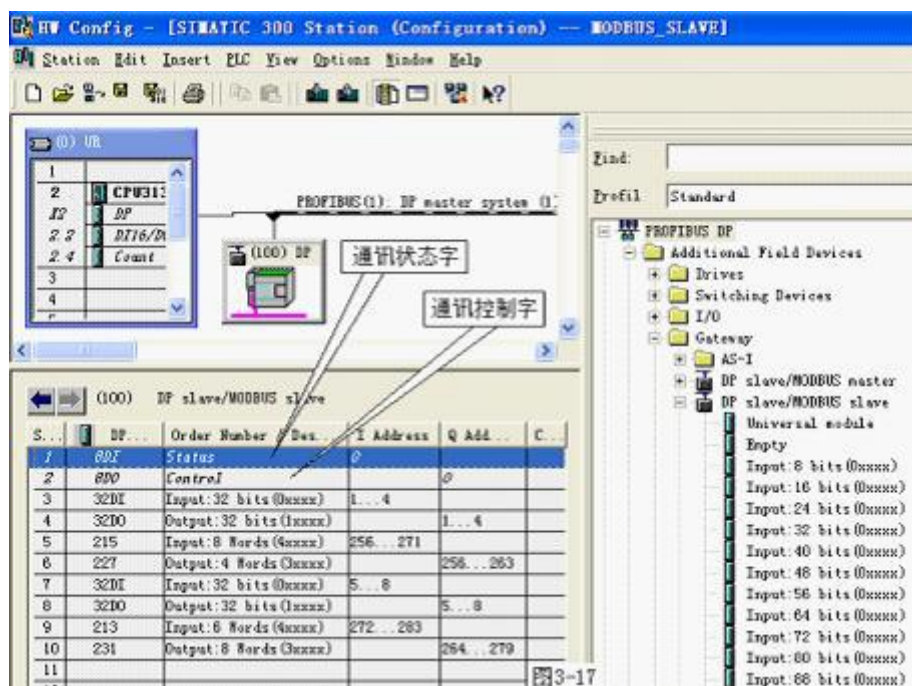


图3-17

至此，系统配置完毕。可以编译存盘“Save and Compile” → 退出。

4. 通信状态字与通信控制字

见图 3-17，在 DP slave/MODBUS master 的硬件配置中可以看到，1#、2#槽被接口占用；1#槽是一个字节输入，用作通信状态字 status，

本例中占用 PROFIBUS 输入地址 IB0；

D7:预留 D6:预留 D5:预留 D4:RUN D3:预留 D2:预留 D1:预留 D0:预留

注：在 modbus 从站工作模式下，通信状态字 status 中只有 D4 位有效，它在不工作时 (STOP)，保持不变；当他“1”与“0”交替变化时，代表处于运行状态 (RUN)，只要在变量表中监视 I0.4 就可查看 DP-MODBUS 协议转换器的运行状态。

2#槽是一个字节输出，用作通信控制字 control，本例中占用 PROFIBUS 输出地址 QB0；在 modbus 从站工作模式下，该控制字已无实际用途（为客户定制预留的），大连德嘉国际电子已将其改为由拨码开关的 1 号拨码进行启停控制。

5. 调试

在 modbus 从站工作模式下，

- 1) 首先查看下排左侧第一个 LED 灯是否是绿色闪动，如果闪动说明转换器进入 modbus 从站工作方式，且与 PLC 的通讯已经建立；如果不闪，请查看 profibus 总线或转换器地址拨码是否正确或 RUN/STOP 拨码处于停止位置
- 2) 查看下排右边第一个 LED 灯是否红色闪动，如果闪动说明接收到的 modbus 报文 CRC 校验出错——A：通讯波特率主从站是否一致；B：检查通讯线路；C：两侧终端电阻是否连接
- 3) Modbus 主站未收到数据，或置数失败，请查看主站接收到的转换器发送的 Modbus 异常码。最常见的问题可能是主站要读写的 DP-Modbus 转换器的 modbus 寄存器地址范围有误，请查看 step 中的有关 DP-Modbus 转换器的 DP slave/MODBUS slave 硬件组态的各个插槽的定义或检测 modbus 主站通讯寄存器地址的设置。

5 Modbus-RTU 协议简介

对于您来讲，您只需要了解 Modbus 有 4 个区对应的 8 条重要的功能码，4 条读，2 条写单个位或寄存器，2 条写多个位或者多个寄存器。

MODBUS 协议要点

- 1) MODBUS 是主/从通信协议。主站主动发送报文，只有与主站发送报文中呼叫地址相同的从站才向主站发送回答报文。
- 2) 报文以 0 地址发送时为广播模式，无需从站应答，可作为广播报文发送，包括：
 - 修改线圈状态；
 - 修改寄存器内容；
 - 强置多线圈；
 - 预置多寄存器；
 - 询问诊断；
- 3) MODBUS 规定了 2 种字符传输模式：ASCII 模式、RTU（二进制）模式；两种传输模式不能混用；本产品 DP-MODBUS 转换器只使用 RTU 模式。
- 4) MODBUS 报文 RTU 格式

至少 3.5 个字符的 报文间隔时间	地址 1*byte	功能码 1*byte	数据 N*byte	CRC 校验 2*byte	至少 3.5 个字符的 报文间隔时间
-----------------------	--------------	---------------	--------------	------------------	-----------------------

- 5) 异常应答
 - a. 从机接受到的主机报文，没有传输错误，但从机无法正确执行主机命令或无法作出正确应答；从机将以“异常应答”回答之。
 - b. 异常应答报文格式

例：主机发请求报文，功能码 01：读 1 个 04A1 线圈值

从机地址	功能码	高位起始地	低位起始地	线圈数高位	线圈数低位	CRC
0A	01	04	A1	00	01	XXXX

由于从机最高线圈地址为 0400，则 04A1 超地址上限，从机作出异常应答如下（注意：功能码最高位置 1）：

从机地址	功能码	异常码	CRC
0A	81	02	xxxx

异常应答码

异常码	名称	说明
01	非法功能	所收到的报文功能对于被编址从机是不允许执行的。若有询问命令发出，则本码表示在此之前无编程功能。
02	非法数据地址	数据字段中的地址对于被编址的从机是禁止的。
03	非法数据	数据字段中的值对于被编址的从机是禁止的。
04	相关设备故障	从机PC 不能对报文或异常终止错误作出应答。
05	确认	从机PC 已接受并正在处理长程序任务。应发出“探询”报文。查询该程序何时完成。若尚未完成，PC 会对“探询”报文发出否定应答。
06	忙碌、拒绝执行	收到报文无误，但PC 已受约执行长程序命令。要求以后等PC 有空时在传送。

1、MODBUS 存储区

MODBUS 涉及到的控制器（或 MODBUS 设备）存储区以 0XXXX、1XXXX、3XXXX、4XXXX 标识：

存储区标识	名称	类型	读/写	存储单元地址
0XXXX	线圈	位	读/写	00001-0XXXX， XXXX：与设备有关
1XXXX	输入线圈	位	只读	10001-1XXXX， XXXX：与设备有关
3XXXX	输入寄存器	字	只读	30001-3XXXX， XXXX：与设备有关
4XXXX	保持/输出寄存器	字	读/写	40001-4XXXX， XXXX：与设备有关

2、MODBUS 功能码

Modbus 报文相对比较固定，所以您只需要稍作了解，看几条报文之后就知道了它的结构，在需要的时候再来具体查询。

(1)、读取输出状态

功能码：01H

主站询问报文格式：

地址	功能码	起始地址	起始地址	线圈数	线圈数	CRC
		高位	低位	高位	低位	
11	01	00	13(19)	00	25	XXXX

功能：读从站输出线圈 0XXXX 状态。

注意：有些设备线圈起始地址为 00000，对应设备中 00001 地址，依次顺延。要看具体设备

本例：读 11H 号从站输出线圈，寄存器起始地址=0013H=19，线圈数=0025H=37；因此，本询问报文功能是：读 17（11H）号从站输出线圈 00019—00055，共 37 个线圈状态；

从站应答格式：

地址	功能码	字节计数	线圈状态 19-26	线圈状态 27-34	线圈状态 35-42	线圈状态 43-50	线圈状态 51-55	CRC
11	01	05	CD	6B	B2	0E	1B	XXXX

功能：从机返回输出线圈 0 XXXX 状态

本例：CD=11001101，对应 00019-00026；

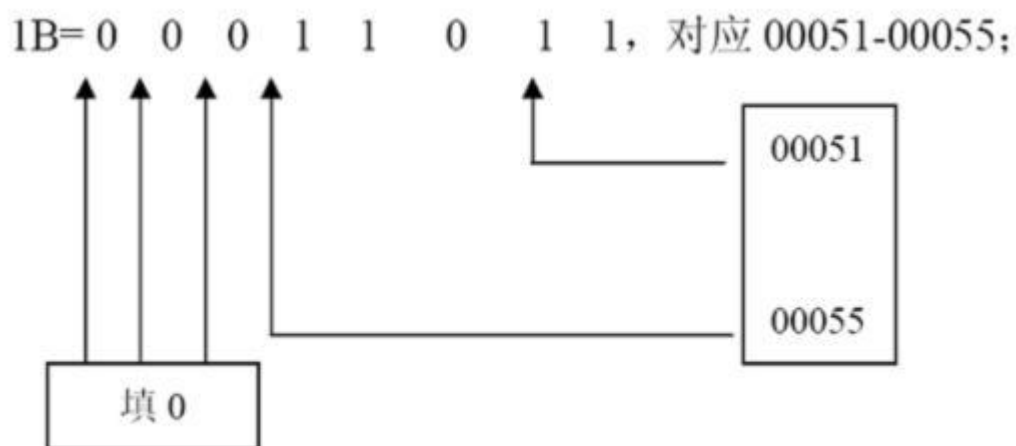


图4-1

(2)、读取输入状态

功能码：02H

主站询问报文格式：

地址	功能码	起始地址 高位	起始地址 低位	线圈数 高位	线圈数 低位	CRC
11	02	00	C4	00	16	XXXX

功能：读从站输入线圈 1XXXX 状态。

注意：有些设备线圈起始地址 10000 对应设备中 10001 地址，依次顺延。

本例：读 11H 号从站输入线圈，起始地址=00C4H=196，线圈数=0016H=22。

因此，本询问报文功能是：读 17（11H）号从站输入线圈 10196—10217，共 22 个输入线圈状态；

从站应答格式：

地址	功能码	字节 计数	DI 10196-10203	DI 10204-10211	DI 10212-10217	CRC
11	02	03	AC	DB	35	XXXX

功能：从机返回 DI=1XXXX 状态

(3)、读取保存寄存器

功能码：03H

主站询问报文格式：

地址	功能码	寄存器起始地 址高位	寄存器起始 地址低位	寄存器数 高位	寄存器数 低位	CRC
11	03	00	6B(107)	00	03	XXXX

功能：读从站保持寄存器 4XXXX 值

注意：有些设备寄存器起始地址 40000 对应设备中 40001 地址, 依次顺延。

本例：读 11H 号从站保持寄存器值，起始地址=006BH=107，寄存器数=0003；

因此，本询问报文功能是：读 17（11H）号从站 3 个保持寄存器 40107—40109 的值；

从站应答格式：

地址	功能码	字节计数	寄存器 40107 高位	寄存器 40107 低位	寄存器 40108 高位	寄存器 40108 低位	寄存器 40109 高位	寄存器 40109 低位	CRC
11	03	06	02	2B	01	06	2A	64	XXXX

功能：从站返回保持寄存器的值：(40107)=022BH，(40108)=0106H，(40109)=2A64H

(4)、读取输入寄存器

功能码：04H

主站询问报文格式：

地址	功能码	寄存器起始地址 高位	寄存器起始 地址低位	寄存器数 高位	寄存器数 低位	CRC
11	04	00	08	00	01	XXXX

功能：读从站输入寄存器 3XXXX 值。

注意：有些设备中寄存器起始地址 30000 对应设备中 30001 地址, 依次顺延。

本例：读 11H 号从站输入寄存器值，起始地=0008H=0008，寄存器数=0001；

因此，本询问报文功能：读 17（11H）号从站 1 个保持寄存器 30008 的值；

从站应答格式

地址	功能码	字节计数	输入寄存器高位	输入寄存器低位	CRC
			30008	30008	
11	04	02	01	01	XXXX

功能：从站返回输入寄存器 30008 的值；（30008）=0101H

(5)、强置单线圈

功能码：05H

主站报文格式：

地址	功能码	线圈地址	线圈地址	断通标志	断通标志	CRC
		高位	低位			
11	05	00	AC (172)	FF	00	XXXX

功能：强置 17 号从站线圈 0XXXX 值。有些设备中线圈起始地址 00000 对应设备中 00001 地址，依次顺延。

断通标志=FF00，置线圈 ON。

断通标志=0000，置线圈 OFF。

例：起始地址=00AC(H)=172。强置 17 号从站线圈 0172 为 ON 状态。

应答格式：原文返回

地址	功能码	线圈地址	线圈地址	断通标志	断通标志	CRC
		高位	低位			
11	05	00	AC (172)	FF	00	XXXX

功能：强置 17 号从机线圈 0172 ON 后原文返回

(6)、预置单保持寄存器

功能码：06H

主站报文格式：

地址	功能码	寄存器地址		数据值		CRC
		高位	低位	高位	低位	
11	06	00	87 (135)	03	9E	XXXX

功能：预置单保持寄存器 4XXXX 值。有些设备中线圈起始地址 40000 对应设备中 40001 地址，依次顺延。

例：预置 17 号从机单保持寄存器 40135 值=0x039E；

应答格式：原文返回

地址	功能码	寄存器地址		数据值		CRC
		高位	低位	高位	低位	
11	06	00	87 (135)	03	9E	XXXX

功能：预置 17 号从机单保持寄存器 40135 值=0x039E 后原文返回。

(7)、强置多线圈

功能码：0FH

主站报文格式：

地址	功能码	线圈起始	线圈起始	线圈数	线圈数	字节 计数	线圈状态	线圈状态	CRC
		地址高位	地址低位	高位	低位		20-27	28-29	
11	0F	00	13	00	0A	02	CD	00	XXXX

功能：将多个连续线圈 0XXXX 强置为 ON/OFF 状态。

注意：有些设备中线圈起始地址 00000 对应设备中 00001 地址，依次顺延。

本例：强置 11H 号从站多个连续线圈，线圈起始地址=0013H=19，线圈数=000AH=10；

因此，本询问报文功能是：强置 17（11H）号从站 10 个线圈 00019—00028 的值； CDH→00019-00026； 00H→00027-00028；

从站应答格式：

地址	功能码	线圈起始 地址高位	线圈起始 地址低位	线圈数 高位	线圈数 低位	CRC
11	0F	00	13	00	0A	XXXX

(8)、预置多寄存器

功能码：10H

主站报文格式：

地址	功能码	起始 寄存器地址 高位	起始 寄存器地址 低位	寄存器数 高位	寄存器数 低位	字节 计数	数据 高位	数据 低位	数据 高位	数据 低位	CRC
11	10	00	87	00	02	04	01	05	0A	10	XXXX

功能：预置从站多个保持寄存器值 4XXXX。

注意：有些设备中保持寄存器起始地址 40000 对应设备中 40001 地址，依次顺延。

本例：预置 11H 号从站多个保持寄存器值，寄存器起始地址=0087H=135，线圈数=0002H=2。

因此，本询问报文功能是：预置 17（11H）号从站 2 个保持寄存器值； 0105H→40135； 0A10H→40136。

应答格式

地址	功能码	起始 寄存器 地址高位	起始 寄存器 地址低位	寄存器数 高位	寄存器数 低位	CRC
11	10	00	87	00	02	XXXX

6 与 Giant525 称重模块通讯 (点击: [实例下载](#))

1. 首先将 Giant525 称重模块的 modbus 通讯波特率设置为 19200; 串行通讯协议为 modbus RTU ;无校验, 1 个停止位, 8 个数据位 Modbus 从站地址设为 “1”

2. 在 STEP7 中建立一个新的项目 “DP_MODBUS_Giant525”

1) 将大连德嘉国际电子提供的 GSD 文件 D_MASTER.GSD 拷贝到 Step7\S7data\gsd\目录下; 产品图标 DS007_N.BMP 和 DS007_S.BMP

文件拷贝到 Step7\S7data\nsbmp\ 目录下

注: 以上的详细目录在 XP 系统中分别是:

C:\Program Files\Siemens\Step7\S7DATA\GSD

C:\Program Files\Siemens\Step7\S7DATA\nsbmp

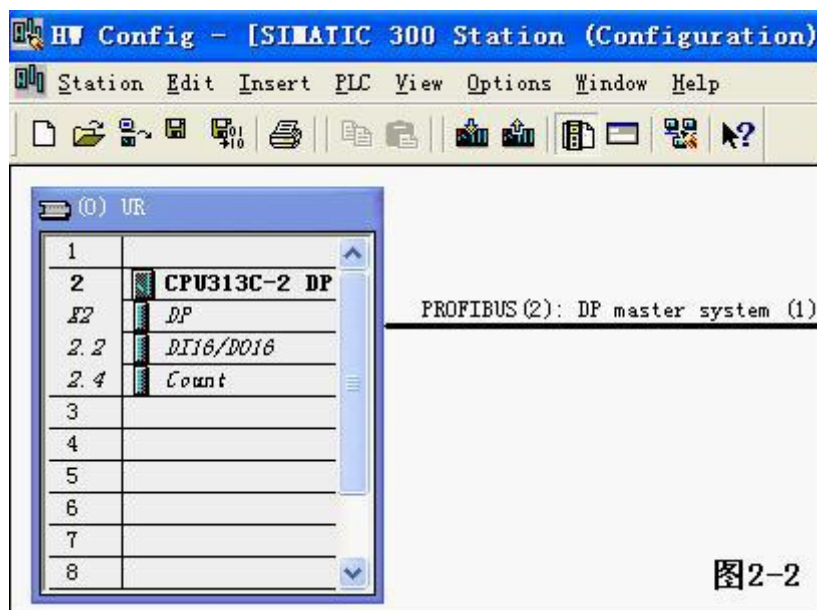
2) 在 STEP 7 上通过向导 ‘New Project’ Wizard 建立一个“项目”, CPU 类型选择 CPU313C-2DP, 项目名字叫 “DP_MODBUS_Giant525”

3. 在 STEP7 的硬件组态中的设置:

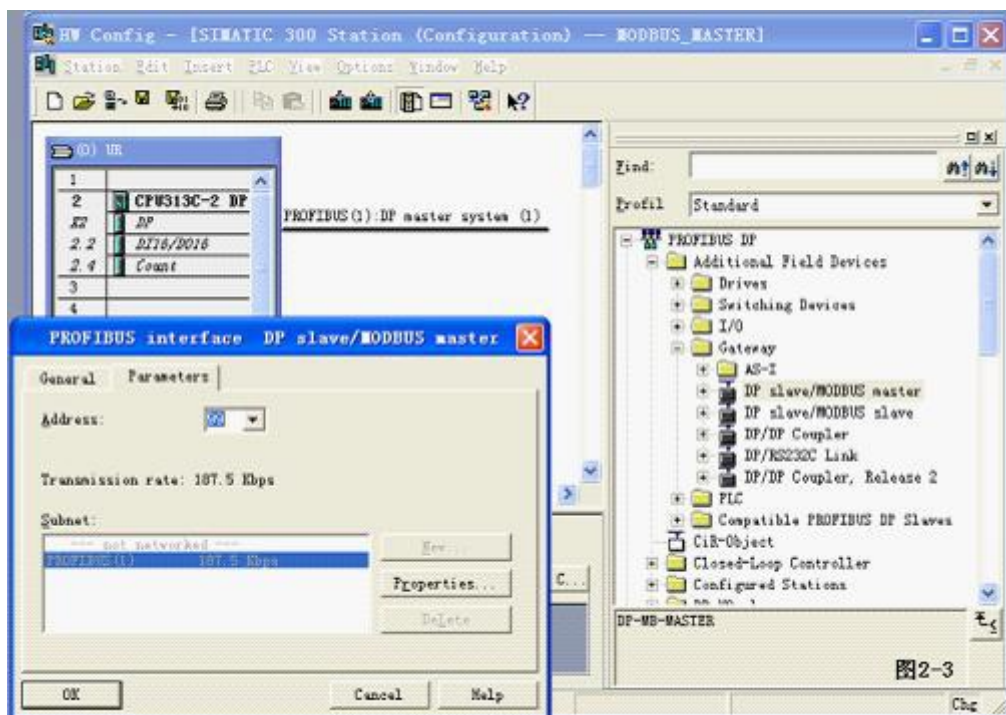
a. SIMATIC 300 Station→Hardware 双击, 并在 HW Config 的菜单中选择 Option→Update Catalog 点击, 将设备 GSD 文件加入设备 Catalog 中



- b. 配置 PROFIBUS: 双击 CPU 槽位中的 DP, →属性→new→Network Settings→187.5K→OK。



- c. 配置 DP-Modbus 协议转换器作为 PROFIBUS 从站点中 PROFIBUS(1) DP master system(1), 使其选中横线变黑, 打开 Hardware Catalog → PROFIBUS DP → Additional Field Devices → Gateway → DP slave/MODBUS master 双击; 然后选择 DP 从站站号, 本例选择从站站号为: 99→“OK”



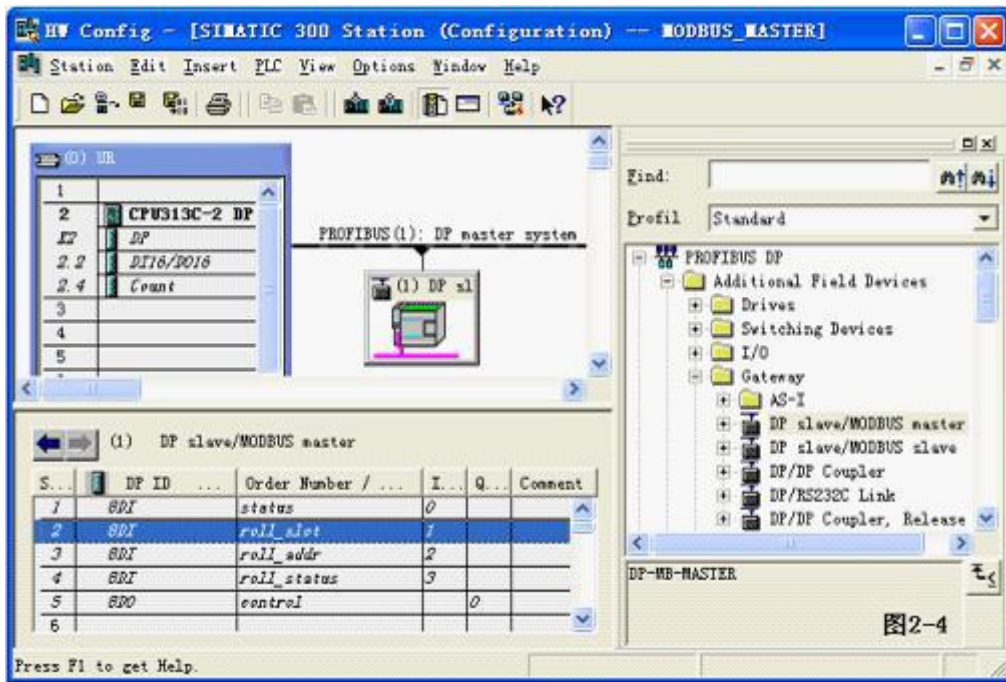


图2-4

- d. 配置DP-Modbus 协议转换器的modbus 侧RS485 接口双击DP-Modbus 图标, 出现如图2-5 的窗口, 选择 Parameter Assignment.

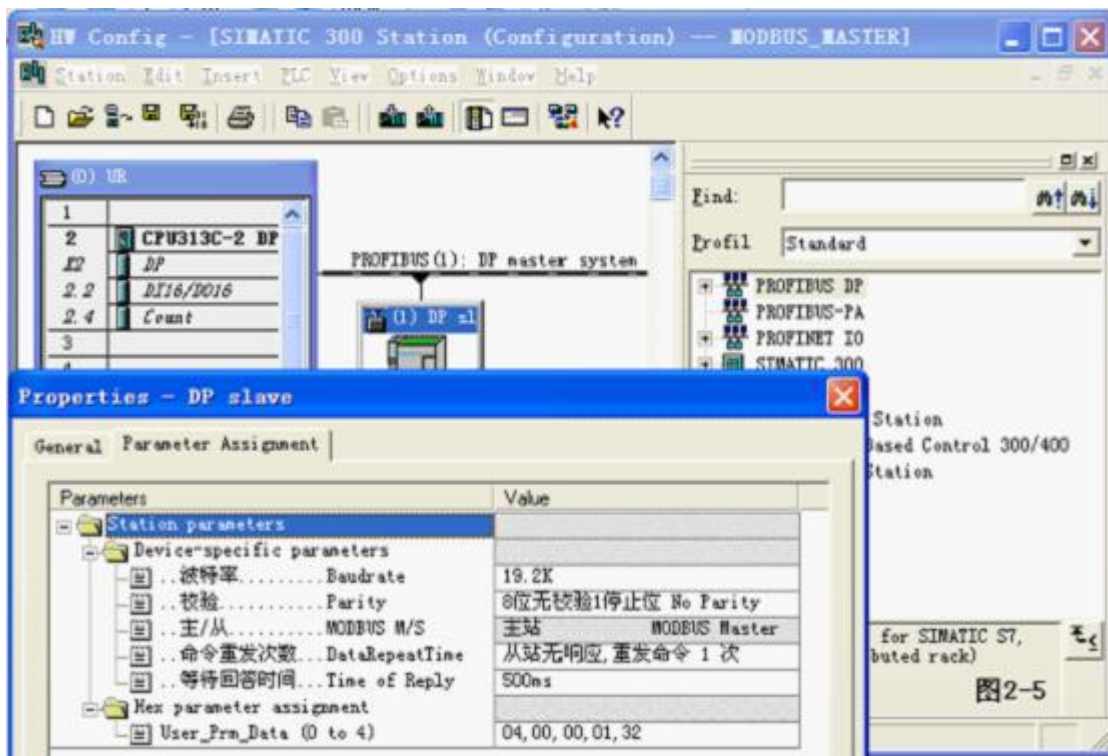


图2-5

e. Modbus 报文队列的配置

选中 6#槽，然后双击“write 1 Words (4xxxx)” 双击 6# 槽中的“1AO write 1 Words (4xxxx) 256..257”；

选择 ParameterAssignment”，完成“从站地址”=1 和“起始地址”=0x0027=39 的参数设定，

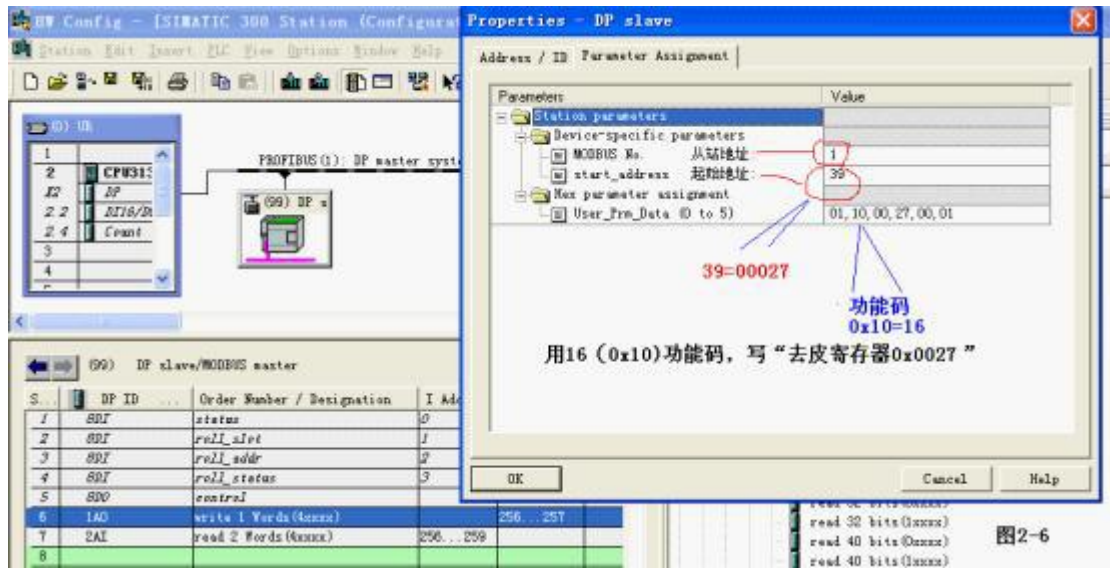


图2-6

选中 7#槽，然后双击“read 2 Words (4xxxx)”。7#槽中插入“read 2 Words (4xxxx) IB256.. IB259”进一步设定 MODBUS 参数: 双击 7#槽中的“read 2 Words (4xxxx)”，选择“Parameter Assignment”，完成“从站地址”=1 和“起始地址”=0x0028=40 的参数设定。

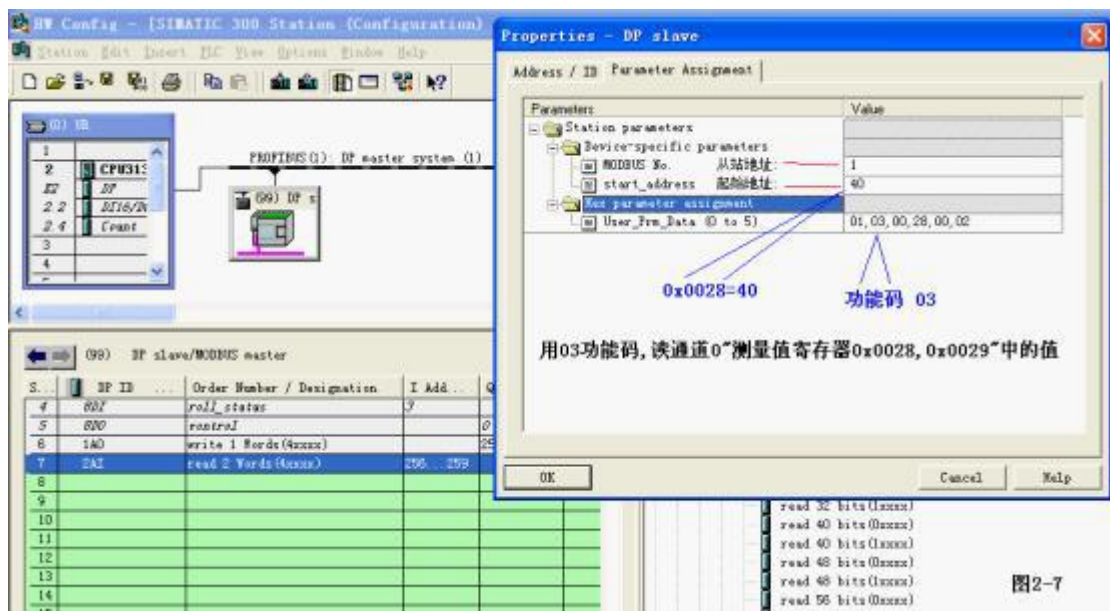
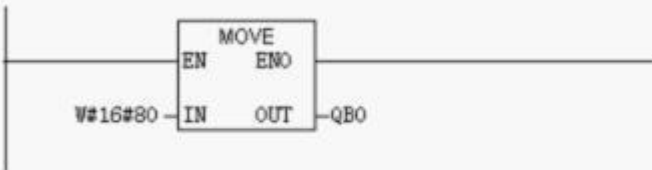


图2-7

4. 在STEP7 的OB1 中编程:

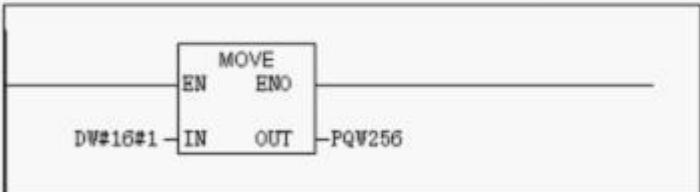
Network 1: Title:

===== 设置:通信控制字control =====
Q0.7如果置“1”,它将根据数据的变化进行寄存器的写操作,如果数据未发生任何变化则对modbus从站不进行寄存器写操作(仅对0x06 0x10功能码有效),这针对于一些仪表的系统参数设置是有次数限制的FLASH类型而专门设计的.而对于频繁变化的数据写操作请一定不要使用该控制位,即D7应为“0”.下边的功能是:将通信控制字control,即 Q0.7置“1”



Network 2: Title:

写Giant525称重模块通道0的“去皮 (TAR) 寄存器 0x0027=39”
在硬件组态中对应的是PQW256 (QB256, QB257)
下边的功能是:将数值1写入去皮 (TAR) 寄存器



Network 3: Title:

读Giant525称重模块通道0的“测量值 (MSV) 寄存器 0x0028 0x0029”
在硬件组态中对应的是PID256 (IB256, IB257, IB258, IB259)
下边的功能是:将测量值传给MDO (MB0, MB1, MB2, MB3)

