PROFIBUS 到 Modbus-RTU 网关

PBMD-K20 使用手册

北京微硬科技有限公司

2007-1-1

目　　录

手册阅读指导

1、如果您已经熟悉 Modbus-RTU 协议以及熟练使用西门子配置软件 Step7，仅仅关心本产品的使用问题，请参看第一章：PBMD-K20 快速使用指南。

2、如果您对西门子配置软件 Step7还不熟悉，请参看第二章：PBMD-K20在 Step7中的配置。或致电西门子技术支持热线：400-810-4288

3、如果您还不熟悉 Modbus-RTU 协议，请参看第三章：Modbus-RTU 协议简介，您只需要了解您正在使用的功能码即可。

4、如果您刚刚了解 Profibus-DP 以及 Modbus-RTU，请通读本手册，或致电北京微硬创新科技有限公司技术支持热线：010-82986935

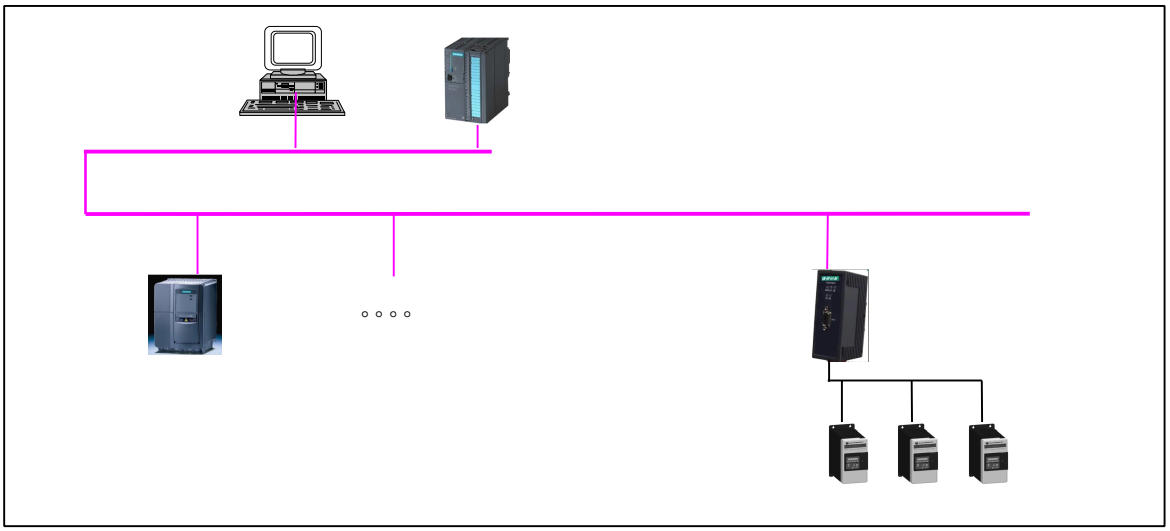
您关心的技术参数

安装方式：导轨安装。

支持的波特率：9.6K-12M

能带 Modbus 站点数：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 37 条；②最大的数据量为输入输出各 224 字节。即使您现场的应用没有超过这个限制，还和你现场的环境有关。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。

典型应用网络图



第一章 PBMD-K20 快速使用指南

1、硬件连线

微硬创新 PBMD-K20 硬件连线如下：

(1) 如图 1-0，顶部为电源接口（直流 24V）、Modbus 主从设置拨码（MS 为 Modbus 做从站，MM 为做 Modbus 主站）、Profibus 地址设置拨码（采用的是 8421 码，如 AD1-AD3 拨到 ON 的位置地址为 7）。

(2) 底部为 Modbus 通讯接口，B（+），A(-)，本产品内置终端电阻，需要接入终端的时候将 TB 和 B 短接，TA 和 A 短接即可。

(3) 正面为 Profibus 通讯接口和指示灯。

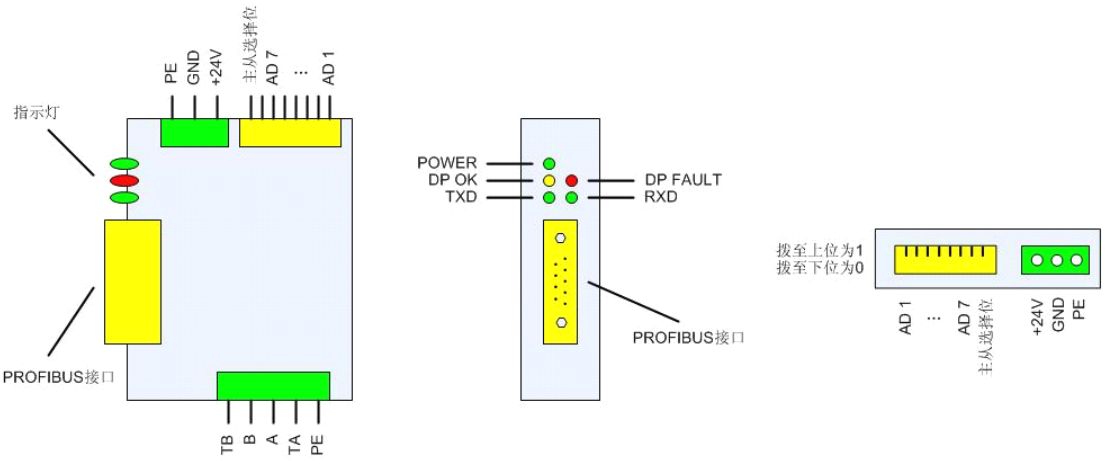


图 1-0：PBMD-K20 接线示意图

2、Step7 中的配置说明

(1) Modbus-RTU 侧接口的配置

在 Step7 硬件配置界面，添加了微硬模块 PBMDP-K20 之后，双击图标，在出现如图 1-1 的窗口，选择 Parameter Assignment。

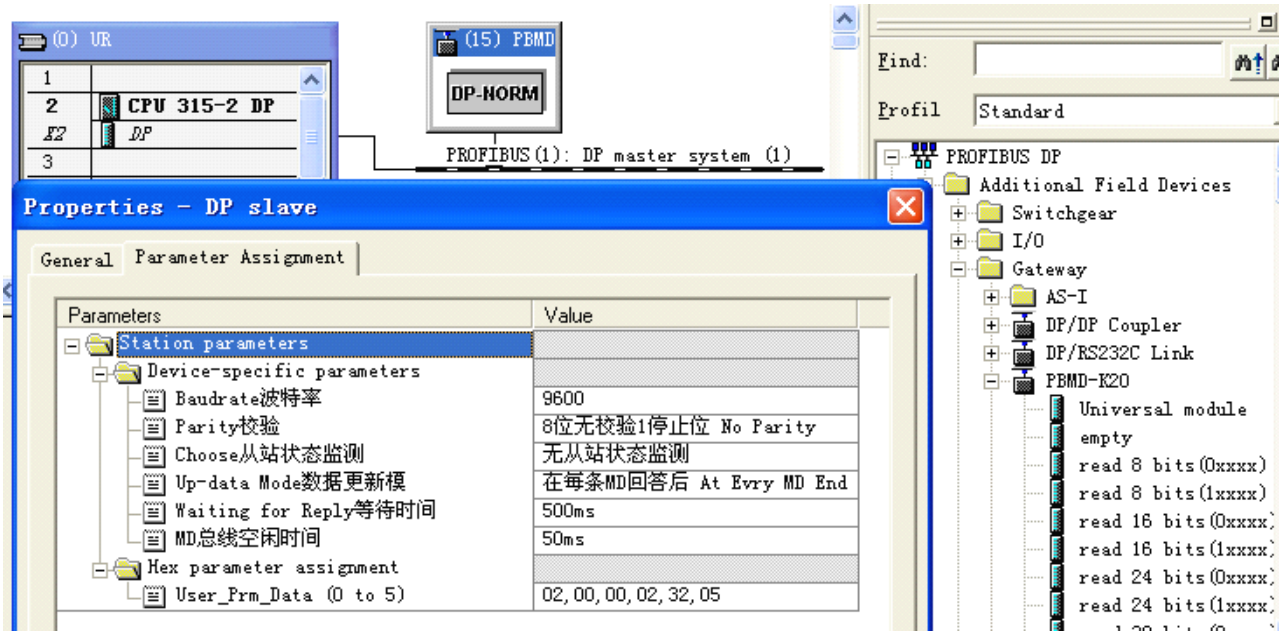


图 1-1：Modbus-RTU 接口的设置

波特率和校验：必须设置的和您要连接的 Modbus 设备的一致，否则微硬模块和你要连接的设备无法通讯，下面设备的通讯接口的设置请参看他们手册的说明或者致电设备厂家询问。

从站状态监测：见附录 A

数据更新模式：可以选择默认。

等待时间：推荐默认的 500mS，他的意思是微硬模块发出一条 Modbus 报文之后等待下面设备回答的时间，如果超出 500mS，不再等待直接发送下一条，如果在 500mS 内回来了，紧接着等待一个空闲时间后发送下一条报文。

总线空闲时间：推荐默认的 50mS，他的意思是指，接到下面设备回答的报文之后等待 50mS 再发送下一条报文。有些设备响应速度比较慢，如果 50mS 太快的话，建议将此时间调长。

(2) Modbus 报文的配置

下面举例说明，如阅读有困难请参看第三章 Modbus-RTU 简介。假如您要读取 Modbus 站号为 1 的设备的 3 区的寄存器地址从 0 开始的连续三个寄存器的值(3 区用户手册上可能是 300XX 或者说支持 04 功能码（Modbus 报文第二个字节))。您可以在右边产品列表里面 PBMD-K20 下面选择“read 3 Words(3XXXX)”模块插入到 Slot3 里面，如图 1-2。

双击你插入的模块，选择 Parameter Assignment,从站站号即为你要访问的 Mobus 设备的站地址，此例为 1；起始地址就是你要访问寄存器的起始地址，此例为 0。那么三个寄存

器回来的数据就存放在这里分配的 IB256-IB261 等 6 个字节里面。

其他您要读写的数据都可根据此例来配置。

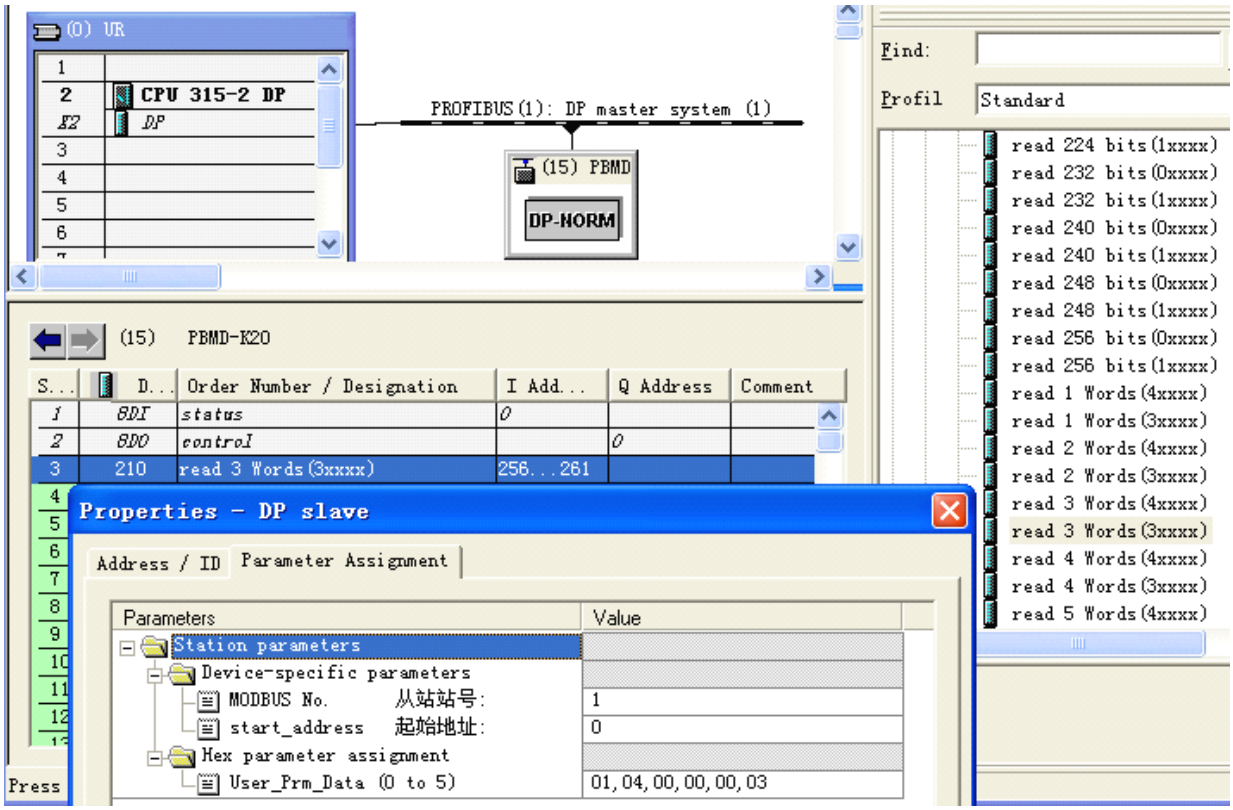


图 1-2：Modbus-RTU 报文的配置

(3) 启动微硬模块开始工作。

以上工作完了，最后一点就是要启动微硬模块开始工作。将控制字最低为置 1。本例控制字为 QB0（在 Slot2 里面，具体地址是多少还要看您的配置），所以您需要在 OB1 模块里面加上如图 1-3 的程序。

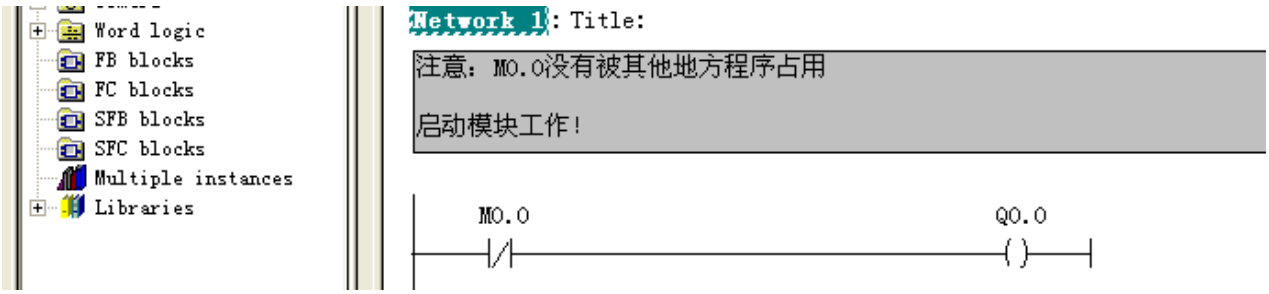


图 1-3：启动设备

在这里，有需要更进一步了解我们产品使用的用户，可以看看下面通讯状态字和通讯控制字的说明。

通信状态字 **Status**

D7：奇偶校验	D6：CRC 校验	D5：等待超时	D4~D1：异常应答	D0：接收/发送
0：没有错误 1：奇偶校验错	0：没有错误 1：CRC 校验错	0：没有错误 1：等待超时	0：没有错误 1：Modbus 访问异常	0：准备接收 1：准备发送

注意：正常情况下我们会看到状态字是 0 和 1 交替变化，其他位如果出现 1，证明 Modbus 通讯有问题，下面讲解一下出现错误后解决方法：

D4~D1：异常应答如果不为 0，说明你发出去的 Modbus 报文对于被访问设备来说是无效的，有可能是地址超限，或者写给设备的值是非法的。解决此问题的方法就是一定要弄清楚你要访问的数据是什么，寄存器地址是多少？被设置的值有没有范围限制等等

D5：等待超时，可以将此手册图 1-1 中总线空闲时间调大！

D6：CRC 校验错，可能用户编写的 CRC 高低字节反了，或者在没有完整收到一帧报文也会出现 CRC 错，这时候我们可以通过串口调试助手或者 Modsim32 之类监控一下报文。

D7：奇偶校验错，接口没有设置的一致！图 1-1 中的波特率和奇偶校验没有和设备的相一致。

需要提醒的是，往往一个错误有可能使得几个地方报错，这就需要现场调试人员判断错误出现在那里，最简单的自助办法就是学会使用串口调试助手和 Modsim32 以及 Modscan 等软件，一般情况下只要和这三个软件能通讯的上的话，肯定能和我们产品进行通讯。

通信控制字 **Control**

D7	D6	D5	D4-D3	D2	D1	**D0**
强制复位	停止等待	清除错误	保留	写允许	读允许	**启动工作**

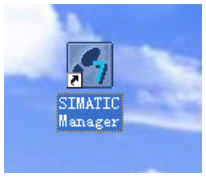
注意：这里不推荐用户使用其他功能，仅仅需要你将 D0 置 1，启动 PBMD-K20 发送 Modbus 报文即可，如果遇到比较特殊的用法，请致电我公司技术人员进行咨询！

第二章 PBMD-K20 在 Step7 中的配置

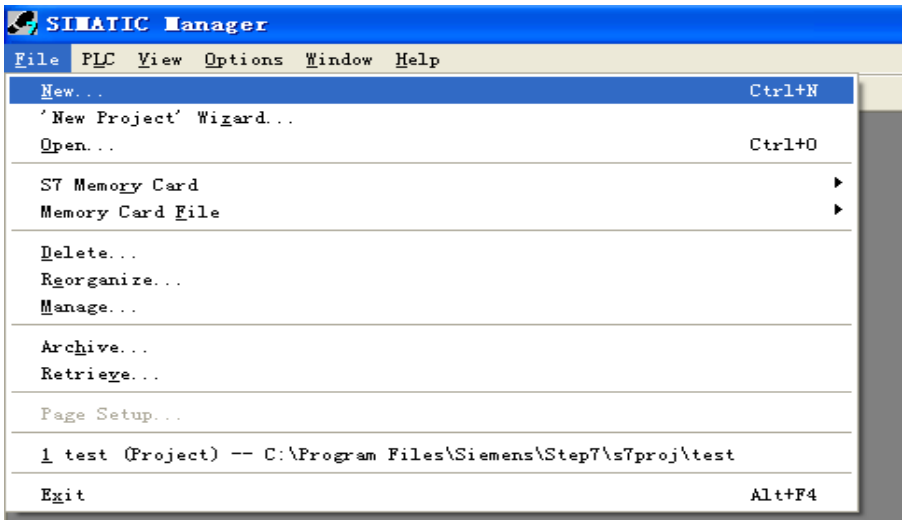
注意：请完整阅读完本章内容，如还有问题请致电微硬科技或者西门子公司

1、请将 GSD 文件拷贝到 Step7 安装目录 :\Program Files\Siemens\Step7\S7DATA\GSD 里面。

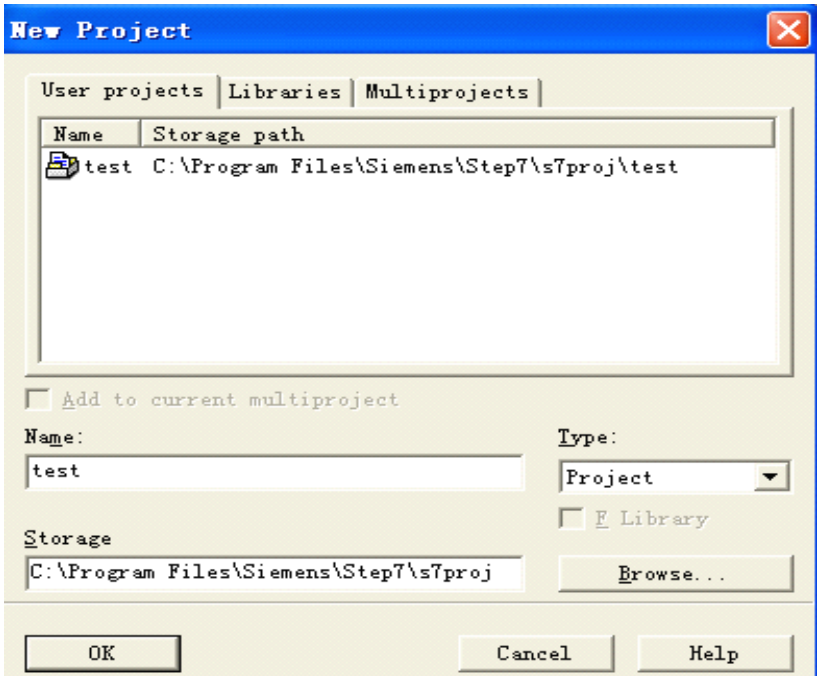
2、打开桌面上的图标



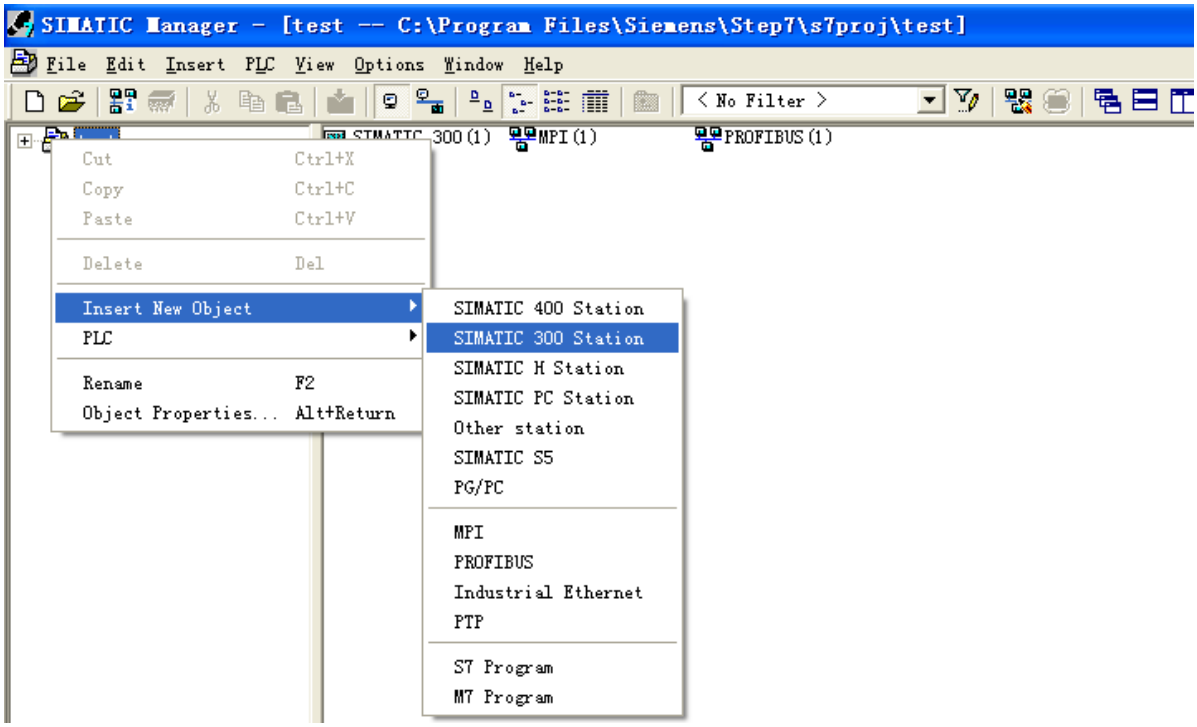
3、新建项目



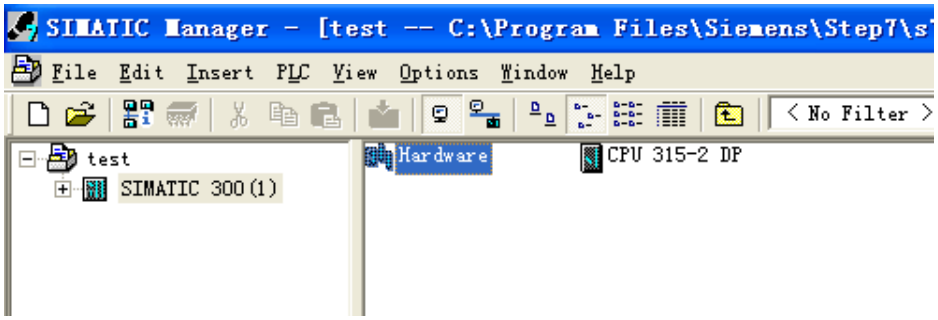
4、输入项目名称，您还可以选择项目存储目录。



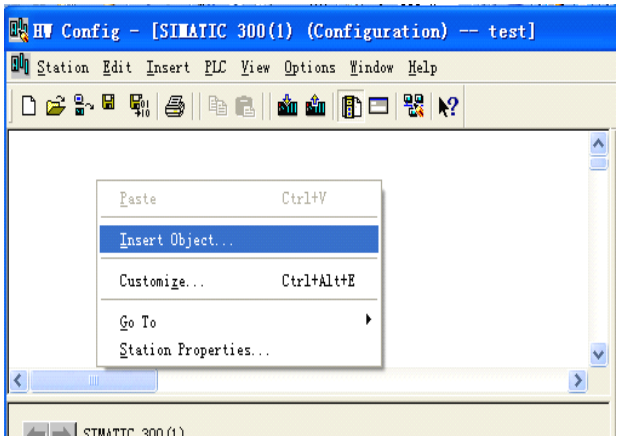
5、选择主站类型，此例用的是 300PLC

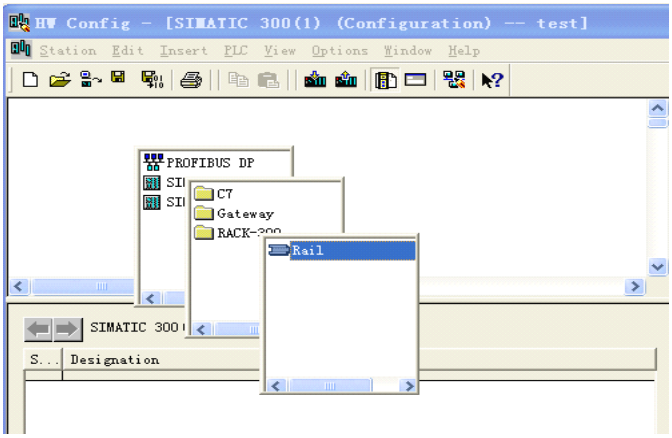


6、点击 SIMATIC 300(1)，继续点击 Hardware 进入硬件配置界面

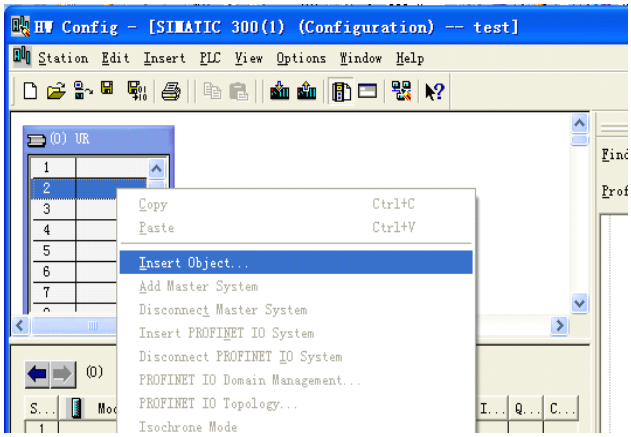


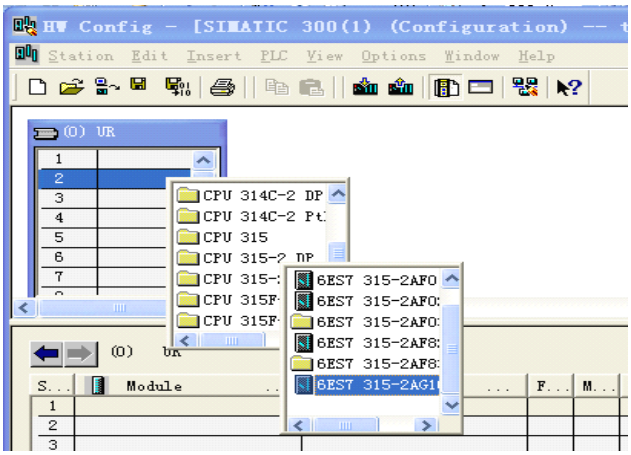
7、添加导轨



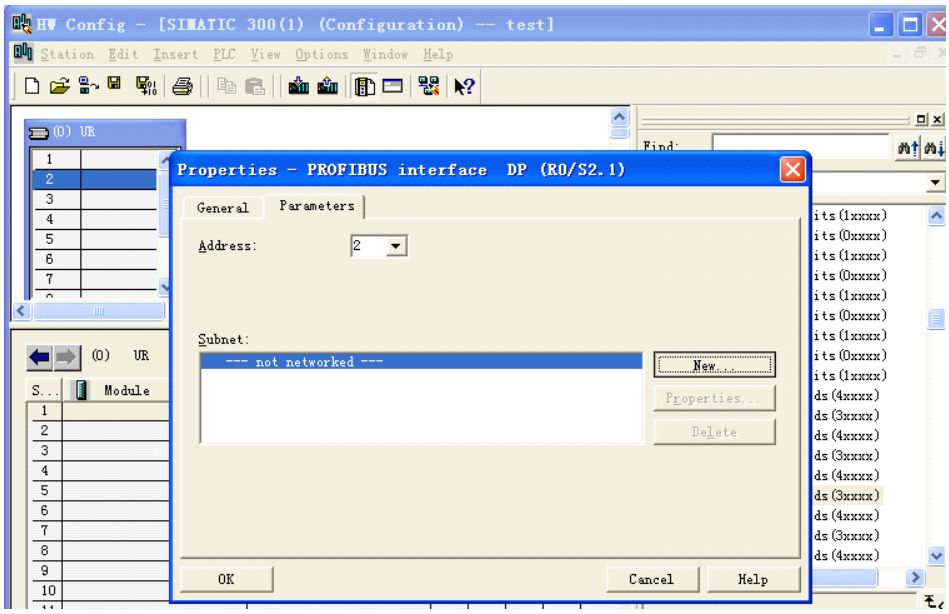


8、添加 PLC，选择正确的 PLC 型号，可参看 PLC 侧面的条码,一般为 6ES7 开头

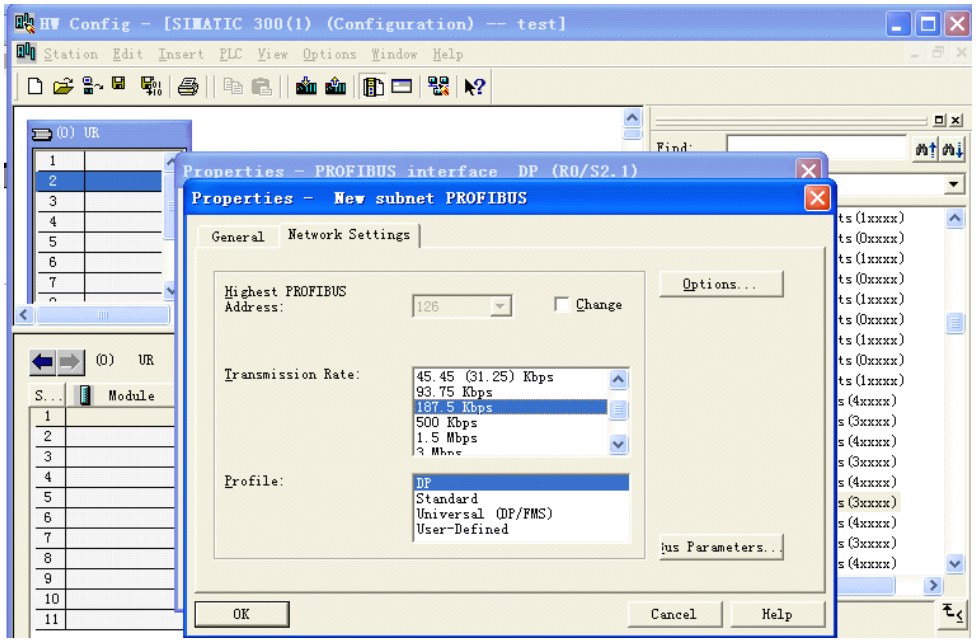




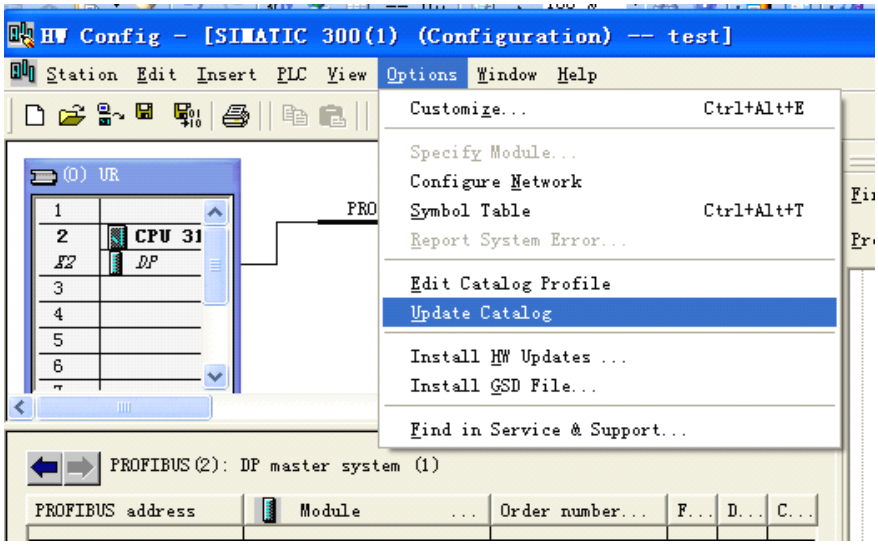
9、新建网络



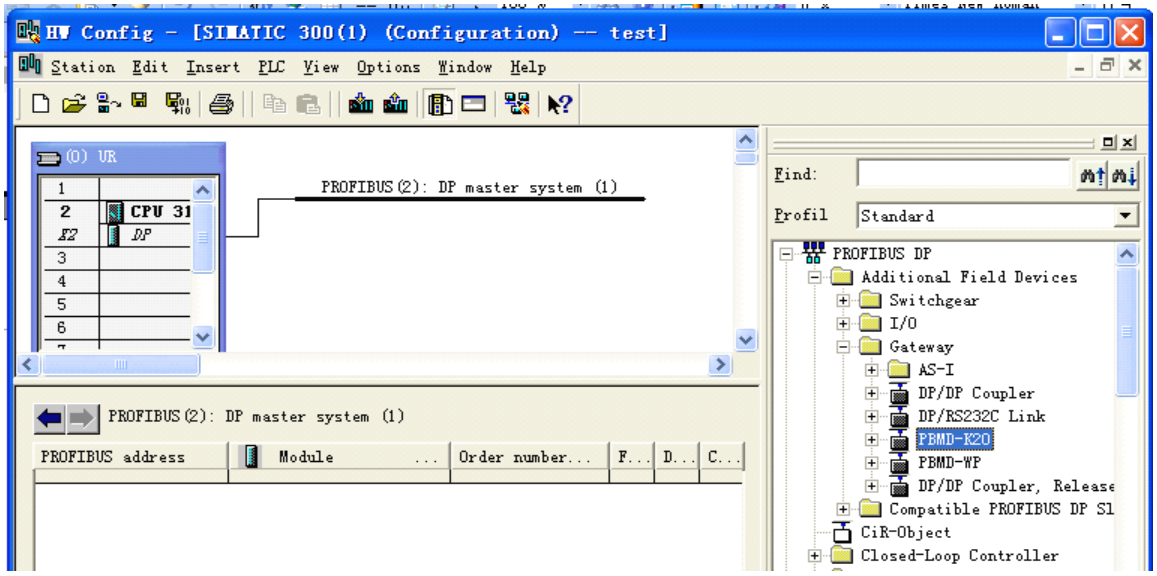
10、设置 Profibus-DP 波特率



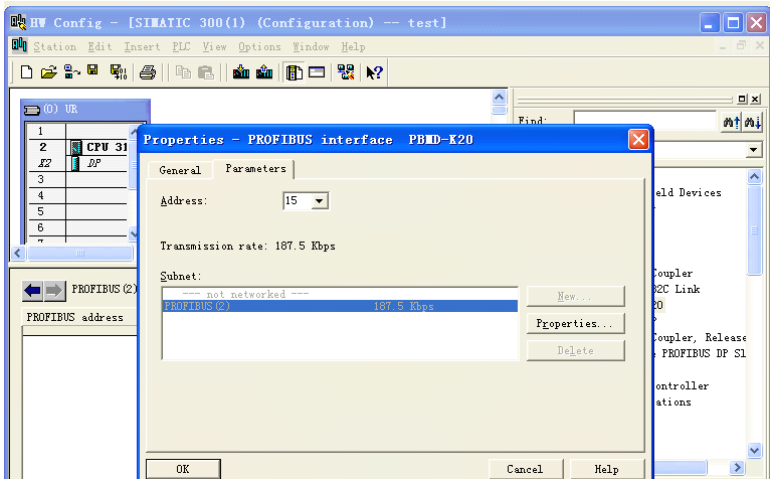
11、更新产品列表，目的是使 Step7 发现第一步拷贝的 GSD 文件



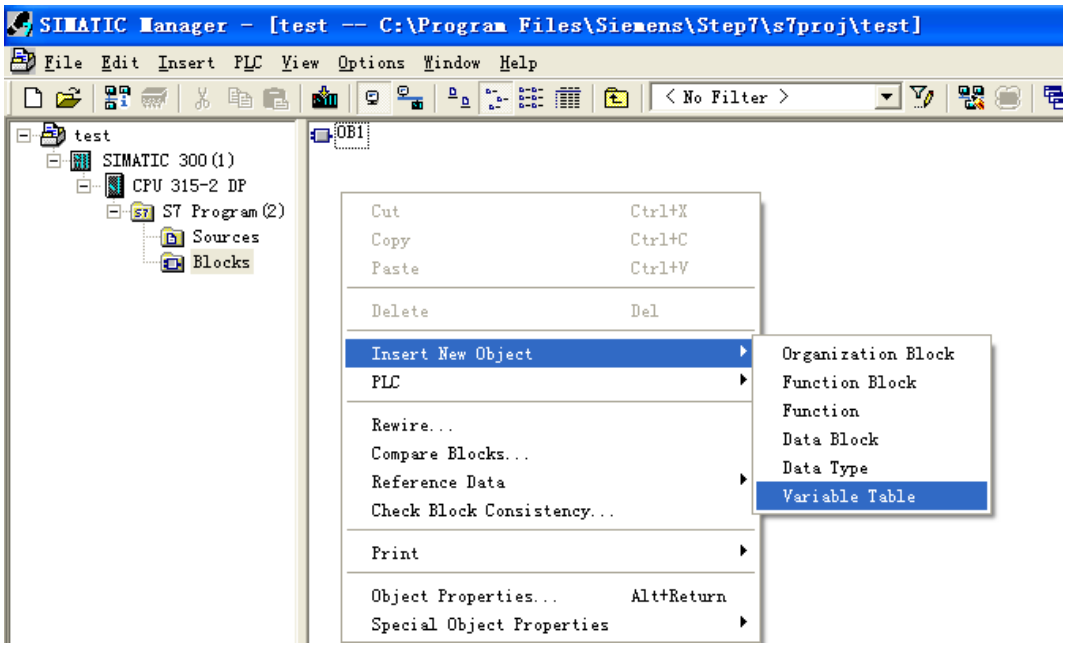
12、更新后即可在右边产品列表里面发现微硬科技产品 PBMD-K20



13、点击选中 DP master system (1) 下面的线使其变全黑。双击右侧列表里面 PBMD-K20, 设置站地址，这个地方的 15 必须和微硬设备上的旋转拨码开关一致



14、经过上面的配置后，接下来的设置可以参看第一章。要注意的是 OB1 模块和变量表在主界面去寻找和建立。



第三章 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。

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 高位	起始地址 低位	线圈数 高位	线圈数 低位	CRC
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；

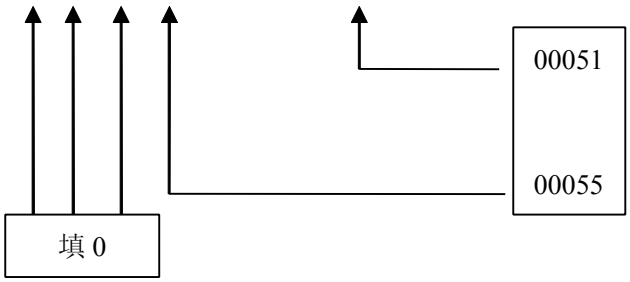
从站应答格式：

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；

1B= 0 0 0 1 1 0 1 1，对应 00051-00055；



(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 30008	输入寄存器低位 30008	CRC
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

询问格式：

地址	功能码	线圈地址 高位	线圈地址 低位	断通标志	断通标志	CRC
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 高位	线圈地址 低位	断通标志	断通标志	CRC
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

询问格式：

地址	功能码	寄存器地址 高位	寄存器地址 低位	数据值 高位	数据值 低位	CRC
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 高位	寄存器地址 低位	数据值 高位	数据值 低位	CRC
11	06	00	87	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

主站询问报文格式：

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	字节计数	线圈状态 20-27	线圈状态 28-29	CRC
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

主站询问报文格式：

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

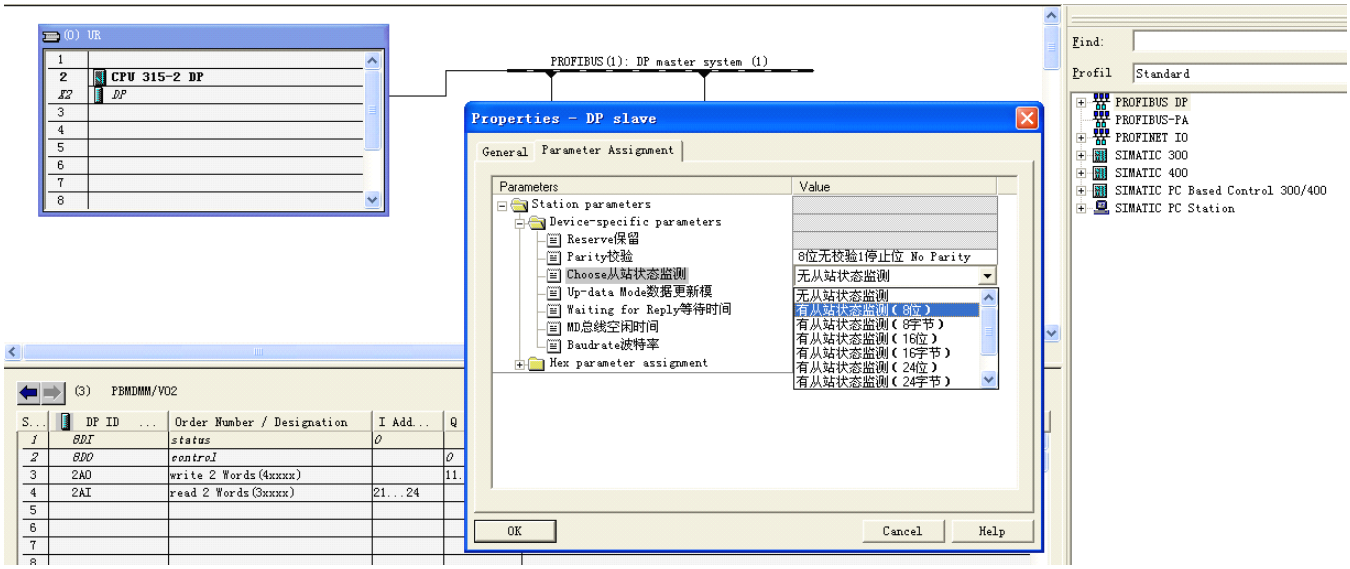
→40136.

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

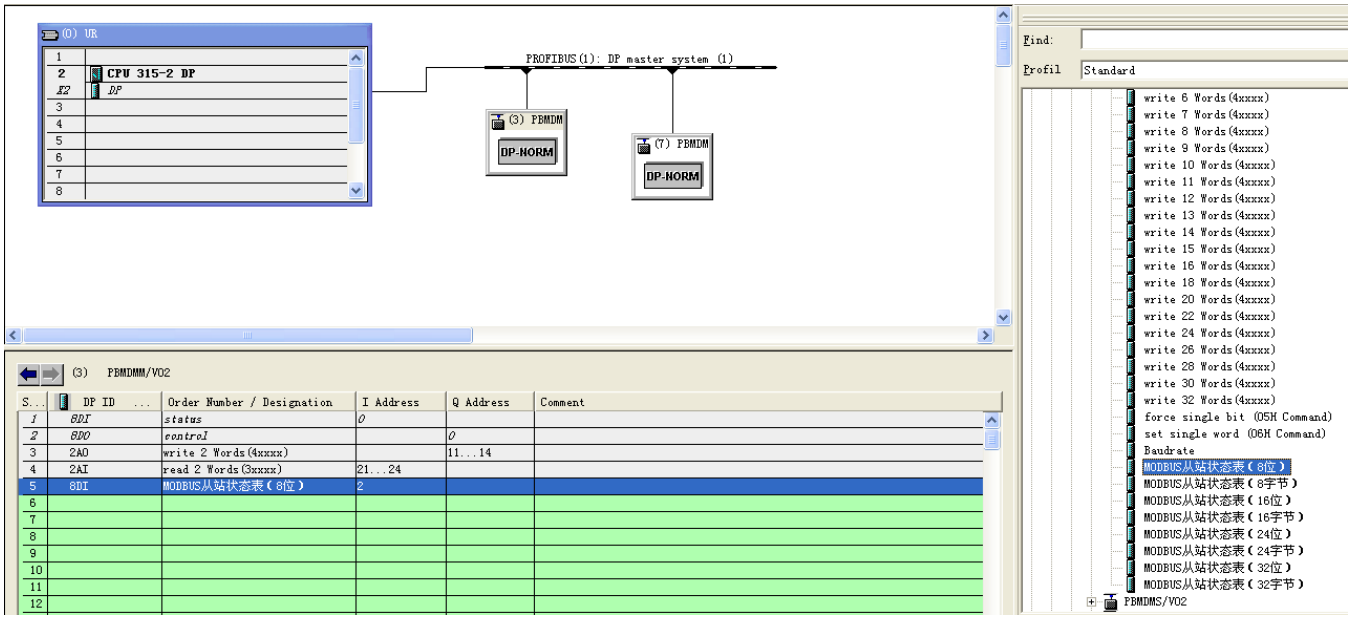
附录 A：从站状态检测功能说明

1. 在 PBMD 模块中配置“Choose 从站状态监测”，如图：如果需要监测的从站数量小于 8 个，则选择“有从站状态监测（8 位）”；如果需要监测的从站数量大于 8 个并小于 16 个，则选择“有从站状态监测（16 位）”；以此类推，最大可监测 32 个从站状态。本例中选择“有从站状态监测（8 位）”。



2. 在 STEP7 右侧模块目录中选择“MODBUS 从站状态表（8 位）”，添加至输入输出地址列表，如图。

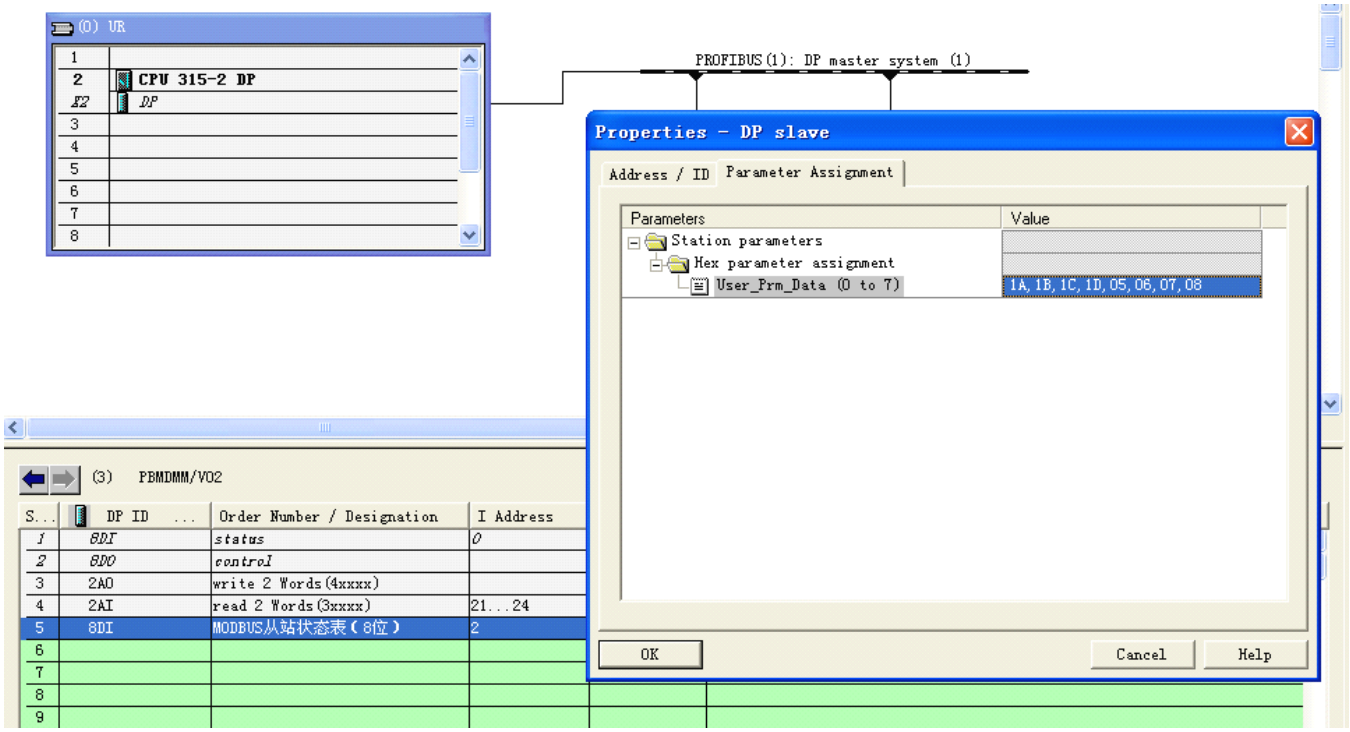
   注意：“MODBUS 从站状态表（8 位）”必须插在所有 MODBUS 报文最后。



3. 双击该条命令，在弹出的对话框中进行设置，如图。

   图中的设置表示：DP 地址 IB2 中，第 0 位代表 MODBUS 第 26 号从站（1AH）的状态，第 1 位代表 MODBUS 第 27 号从站（1BH）的状态，以此类推，第 7 位代表 MODBUS

第 8 号从站（08H）的状态。本例中，我们只关心地址 26、27、28、29 的状态，所以后四位的设置不起作用。



IB2：

D7（忽略）	D6（忽略）	D5（忽略）	D4（忽略）	D3	D2	D1	D0
8 号 从站状态	7 号 从站状态	6 号 从站状态	5 号 从站状态	29 号 从站状态	28 号 从站状态	27 号 从站状态	26 号 从站状态

以 26 号从站为例，D0 位的状态有如下含义：

D0=0 时，PBMD 模块向 26 号从站发送报文后，可能发生了等待应答超时、奇偶校验错、CRC 校验错、从站应答异常的情况，表示通讯异常。

D0=1 时，PBMD 模块与 26 号从站通讯正常。

4. 注：由于监测表也要占用 PROFIBUS 中一定量的用户参数字节，这就减少了插入从站的报文条数。