

PROFIBUS 到 MODBUS 协议总线桥

PB-B-MODBUS(232/485)主站产品手册 (简称: PB-B-MM 产品手册)

V 3.x



北京鼎实创新科技有限公司

2014-7

关于本手册（必读部分）

本手册分为上、下两册，上册是关于 MODBUS 主站的手册，目前产品最高版本为 V3.4。下册是关于 MODBUS 从站的手册，目前产品最高版本为 V3.3。用户可根据实际需要有选择阅读。

关于 V3.x 版本

1. V3.x 型 (PB-B-MODBUS/V3.x) 是 V2 型 (PB-B-MODBUS/V2) 的改进型产品；V3.x 与 V2 完全兼容，即原使用 V2 型产品的场合，使用 V3.x 型产品替换，不必作任何改动。
2. PB-B-MODBUS 型产品，在 PROFIBUS 一侧只做 PROFIBUS 从站；在 MODBUS 一侧即可做 MODBUS 主站(见图 0-1)，也可以做 MODBUS 从站(见图 0-2)。

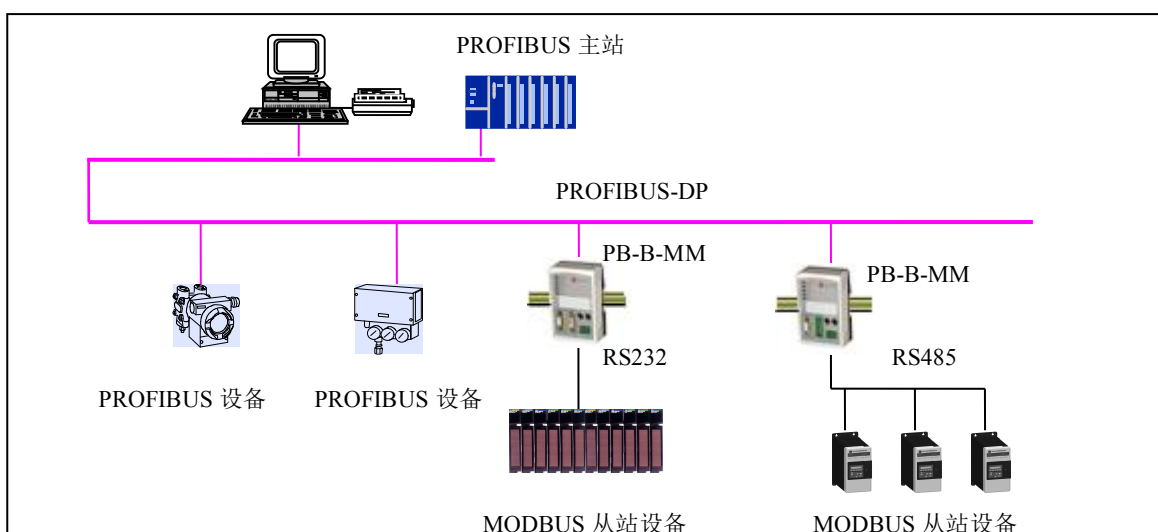


图 0-1 PB-B-MODBUS/232/485/V3x 做主站

上图 0-1 中 PB-B-MODBUS 在 MODBUS 一侧是主站，通过 RS232/485 接口连接到 MODBUS 从站设备上。

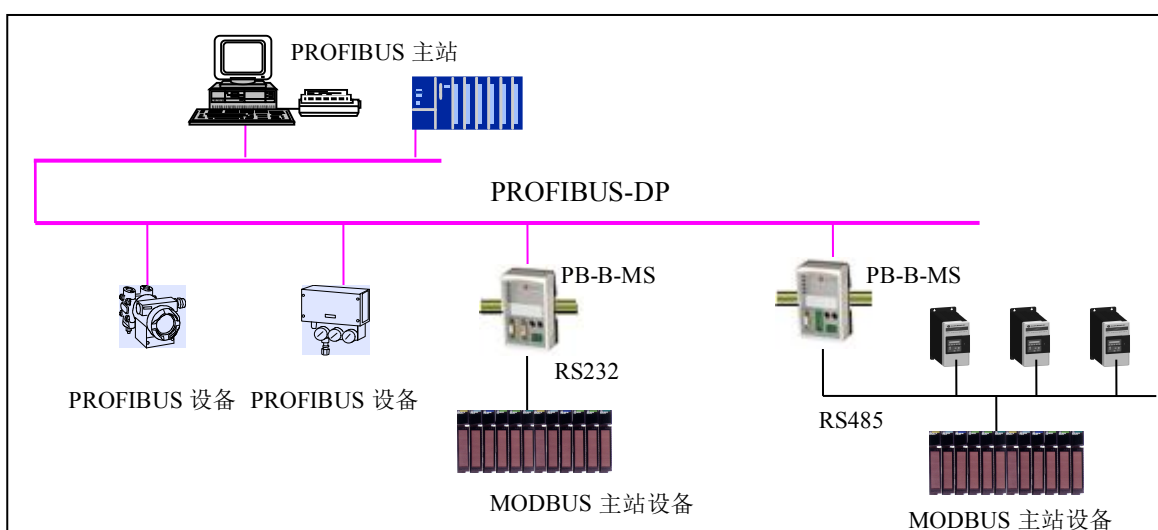


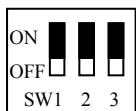
图 0-2 PB-B-MODBUS/232/485/V3x 做从站

上图 0-2 中 PB-B-MODBUS/V32 在 MODBUS 一侧是从站，通过 RS232/485 接口连接到 MODBUS 主站设备上。

3. V3.x 型与 V2 型产品相比增加如下功能：

- (1) 在原 MODBUS 主站功能中，增加了 MODBUS 协议 05H 功能、06H 功能；
- (2) V3.x 可设置成 MODBUS 从站。

4. V3.x 型产品根据产品背面的功能拨码开关数量，分为 3 拨码的桥和 4 拨码的桥（4 拨码桥为升级版）。3 拨码桥中的 SW1 和 4 拨码桥中的 SW2 作用一致，用作设置 MODBUS 主/从功能，如下：



SW1(3 拨码的桥)或者 SW2(4 拨码的桥)=OFF： V3.x 设置成 MODBUS 主站。

SW1(3 拨码的桥)或者 SW2(4 拨码的桥)=ON： V3.x 设置成 MODBUS 从站。

5. 关于 GSD 文件：V3.x 型产品作为 MODBUS 主站或从站所采用的 GSD 文件是两个不相同的文件：

当 V3.x 设置成 MODBUS 主站时,使用 GSD 文件:DS_MMV3x.GSD; 组态中的产品名称:PB-B-MM/V3x;

当 V3.x 设置成 MODBUS 从站时,使用 GSD 文件: DS_MSV3x.GSD; 组态中的产品名称: PB-B-MS/V3x;

注意：

1. 到目前为止，PB-B-MODBUS 做主站总线桥的最高版本是 PB-B-MM/V34。它是在 V3.3 产品的基础上做了改进，除了具有 PB-B-MM/V33 所有的功能外，还增加了周期性发送报文的功能。
2. PB-B-MODBUS 做从站产品的最高版本是 PB-B-MS/V33。在使用时请注意产品背面拨码开关 SW1(3 拨码的桥)或者 SW2(4 拨码的桥)的设置，关于从站的产品介绍可参考 MODBUS 从站手册。

本手册第五章以 PB-B-MM/V33 为例进行配置和通信方法的介绍。PB-B-MM/V34 的使用过程与 V33 相同，后增加功能的具体用法请见本手册第五章 7 节。

目 录(上册)

第一章 产品概述.....	5
一. 系列产品概述.....	5
1. 产品系列.....	5
2. 桥系列产品主要用途.....	5
二. PROFIBUS 到 MODBUS 总线桥 PB-B-MODBUS.....	6
1. 产品特点.....	6
2. 技术指标.....	6
第二章 产品结构、安装、启动.....	8
1. 产品布局.....	8
2. 安装.....	9
3. 外形尺寸.....	9
4. PROFIBUS 接口接插件及安装.....	10
5. RS232 接口及电缆.....	10
6. RS485 接口及安装.....	11
(一) PB-B-MODBUS/485/V3x 的 RS485 接口传输技术的基本特征.....	11
(二) PB-B-MODBUS485/V3x 接口极性.....	12
(三) RS485 终端的接法.....	12
7. 电源.....	13
8. PROFIBUS 从站地址设置.....	14
9. 设置总线桥为 MODBUS 主站或 MODBUS 从站.....	14
10. 指示灯.....	15
11. 上电步骤及故障排除.....	15
第三章 MODBUS 技术简介.....	17
1. MODBUS 通信协议.....	17
2. MODBUS 协议要点.....	17
3. 异常应答.....	18
4. MODBUS 存储区.....	19
5. MODBUS 功能.....	19
(1) 读取输出状态.....	19
(2) 读取输入状态.....	20
(3) 读取保持寄存器.....	21
(4) 读取输入寄存器.....	21
(5) 强置单线圈.....	22
(6) 预置单保持寄存器.....	22
(7) 读取异常状态.....	23
(8) 回送校验.....	23
(9) 读取通信事件计数器.....	23
(10) 读取通信事件计数器.....	23
(11) 强置多线圈.....	23
(12) 预置多寄存器.....	23
第四章 协议转换原理.....	25
1. PB-B-MODBUS 产品硬件结构.....	25
2. 与 PROFIBUS 的连接.....	25
3. PROFIBUS 与 MODBUS 的协议转换原理.....	26
第五章 产品配置与通信方法.....	28
1. 产品配置与通信方法的实例.....	28
2. 系统配置方法.....	28

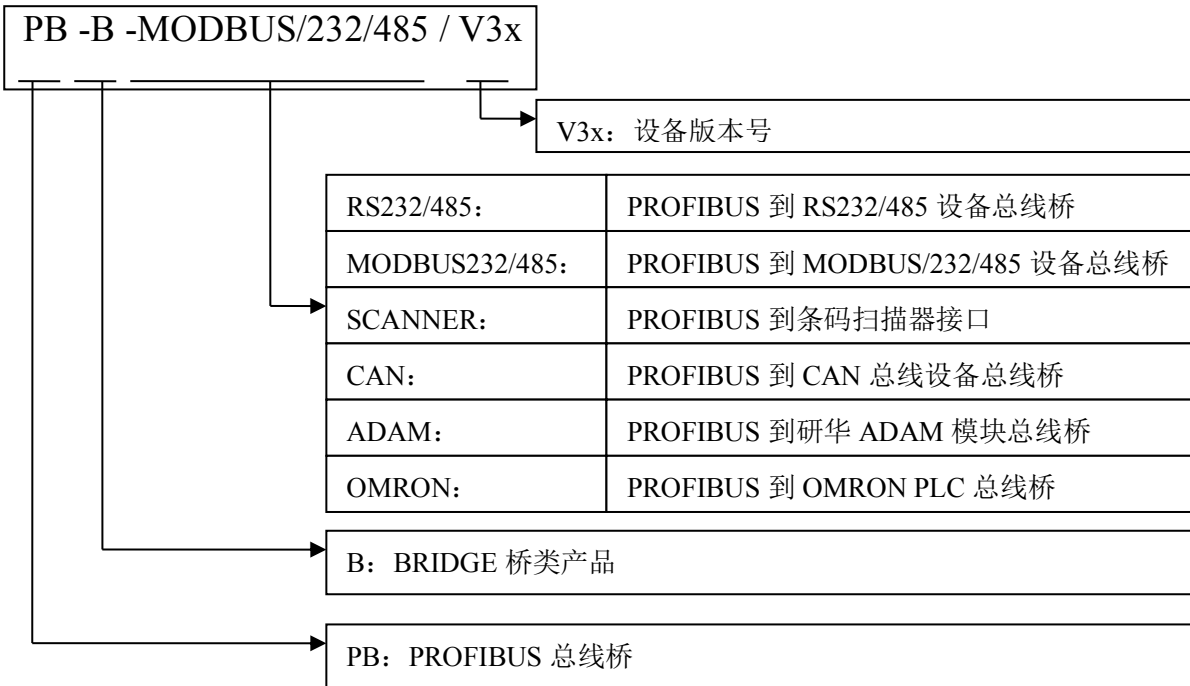
(一) 在 PC1-STEP 7 上建立一个“项目”	28
(二) 硬件配置	29
(三) 配置 PB-B-MODBUS 作为 PROFIBUS 从站	30
(四) 配置 PB-B-MM/V32 的 MODBUS 报文队列	33
(五) “编译存盘”系统配置完毕	43
3. 通信控制字与通信状态字	43
(1) 通信状态字格式	44
(2) 通信控制字格式	45
4. PB-B-MODBUS/V32 工作状态及转换	46
(1) 工作状态流程图	46
(2) 上电后 MODBUS 启动	48
(3) 几种错误和故障状态及解除方法	48
5. 如何在主站中启动读/写 MODBUS 通信数据	50
(1) 设备与地址对应关系	52
(2) 通信状态字及通信控制字 PROFIBUS 对应关系	52
(3) 如何获取通信状态字	52
(4) 如何在主站中实现 MODBUS 启动、复位、停止等待、清除错误标志等	53
(5) 如何在主站中将数据写入 MODBUS 数据区 0XXXX、4XXXX	53
(6) 如何在主站得到 MODBUS 数据区 0XXXX、1XXXX、3XXXX、4XXXX 数据	55
6. 从站状态检测	58
(1) “MODBUS 从站状态监测”功能	58
(2) 举例说明 1: MODBUS 从站通信状态 (位) 监测	58
(3) 举例说明 2: MODBUS 从站通信状态 (字节) 监测	60
(4) 几种特例	63
(5) 注意事项—配置从站最大报文条数	64
7. V34 新功能介绍	64
(1) 周期性发送报文功能	64
(2) 使用方法	65
第六章 有毒有害物质表	67

第一章 产品概述

一. 系列产品概述

1. 产品系列

PB-B-MODBUS 接口（以下有时简称“接口”）是 PROFIBUS 总线桥系列中的产品；本产品手册只适合 PB-B-MODBUS 型产品，物理接口为 RS232 或 RS485，在 MODBUS 一侧总线桥做主站。



2. 桥系列产品主要用途

将具有 MODBUS、RS232/485、CAN 等专用通信协议的接口设备连接到 PROFIBUS 总线上，使设备成为 PROFIBUS 总线上一个从站。见图 1-1 所示，应用总线桥 PB-B-XXXX 将不同的通信协议的设备连接到 PROFIBUS 总线上。

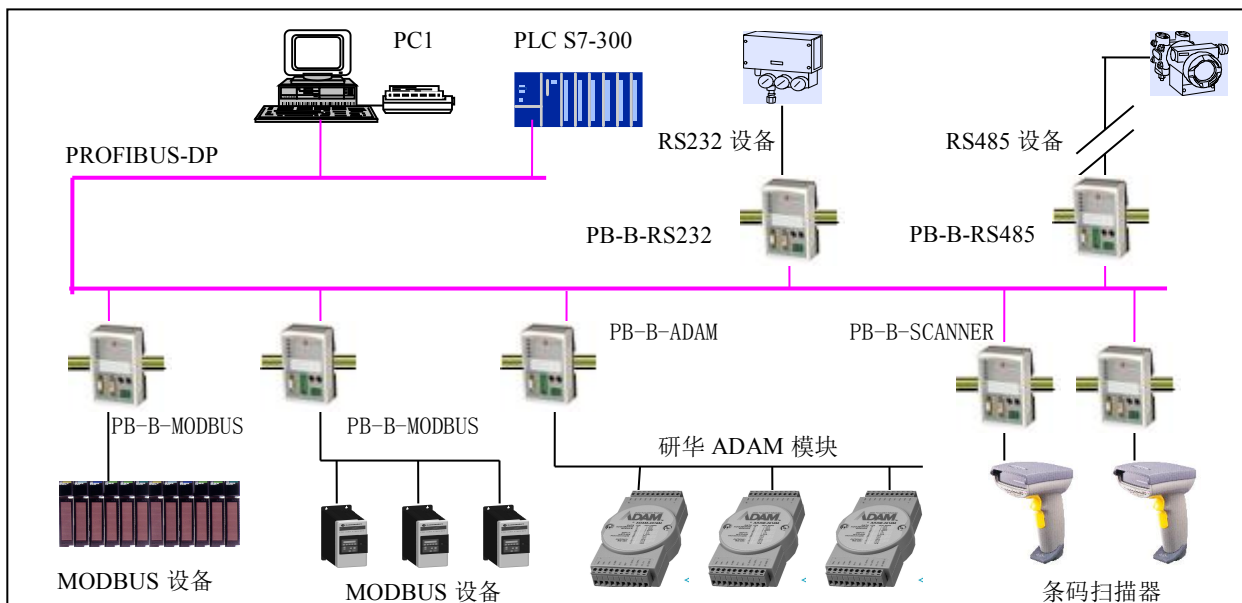


图 1-1 具有不同通信协议的设备与 PROFIBUS 总线桥的连接

二. PROFIBUS 到 MODBUS 总线桥 PB-B-MODBUS

1. 产品特点

▼**应用广泛**：凡具有 RS232/485 接口，标准 MODBUS RTU 协议的设备都可以使用本产品实现与现场总线 PROFIBUS 的互连。如：具有 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。

▼**应用简单**：用户不用了解 PROFIBUS 和 MODBUS 技术细节，用户只需参考本手册及提供的应用实例，根据要求完成配置，不需要复杂编程，即可在短时间内实现连接通信。

▼**透明通信**：用户可以依照 PROFIBUS 通信数据区和 MODBUS 通信数据区的映射关系，实现 PROFIBUS 到 MODBUS 之间的数据透明通信。

▼**技术资料**：《总线桥产品选型手册》、《PB-B-MM 产品手册》、《PB-B-MS 产品手册》，全部资料可在网上下载。网址：www.c-profibus.com.cn

2. 技术指标

(1) PB-B-MODBUS 接口在 PROFIBUS 侧是一个 PROFIBUS-DP 从站，在 MODBUS 一侧是 MODBUS 主站；接口通过 PROFIBUS 通信数据区和 MODBUS 数据区的数据映射实现 PROFIBUS 和 MODBUS 的数据透明通信。如图 1-2：

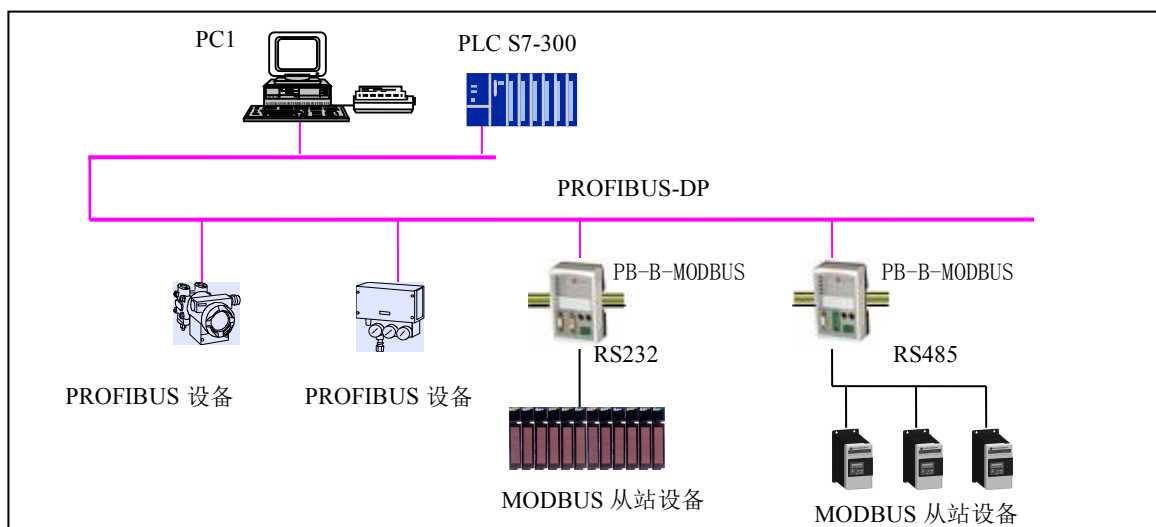


图 1-2 PB-B-MODBUS/V3x 做主站

上图 1-2 中，接口 PB-B-MODBUS 在 PROFIBUS 一侧是 DP 从站，在 MODBUS 设备一侧是主站，通过 RS232/485 接口连接到 MODBUS 从站设备上。

(2) PB-B-MODBUS 作为 MODBUS 主站，支持 01H、02H、03H、04H、05H、06H、0FH、10H 号功能；

(3) PROFIBUS-DP/V0 协议符合 GB/T 20540-2006： 测量和控制数字数据通信工业控制系统用现场总线 第 3 部分： PROFIBUS 规范；

(4) PROFIBUS-DP 从站，波特率自适应，最大波特率 12M；

- (5) PROFIBUS 输入/输出数量可自由设定, 最大 PROFIBUS 输入/输出:
- ① Input Bytes + Output Bytes \leq 232 Bytes
 - ② Max Input Bytes \leq 224 Bytes
 - ③ Max Output Bytes \leq 224 Bytes
- (6) MODBUS 协议接口是标准 RS232 或 RS485 接口, 半双工; 波特率: 2400、4800、9600、19.2K、38.4K、57.6K 可选; 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。
- (7) 电源电压: 24 VDC(\pm 20%);
- (8) 额定电流: 110 mA (24 VDC 时)
- (9) 环境温度:
- 运输和存储: $-40^{\circ}\text{C} \sim +70^{\circ}\text{C}$
- 工作温度: $-20^{\circ}\text{C} \sim +55^{\circ}\text{C}$
- (10) 工作相对湿度: 5~95%
- (11) 外形尺寸: (宽) 70mm \times (长) 112.5mm \times (厚) 39.5mm;
- (12) 安装方式: 35mm 导轨;
- (13) 防护等级: IP20;
- (14) 重量: 约 230g。

第二章 产品结构、安装、启动

1. 产品布局

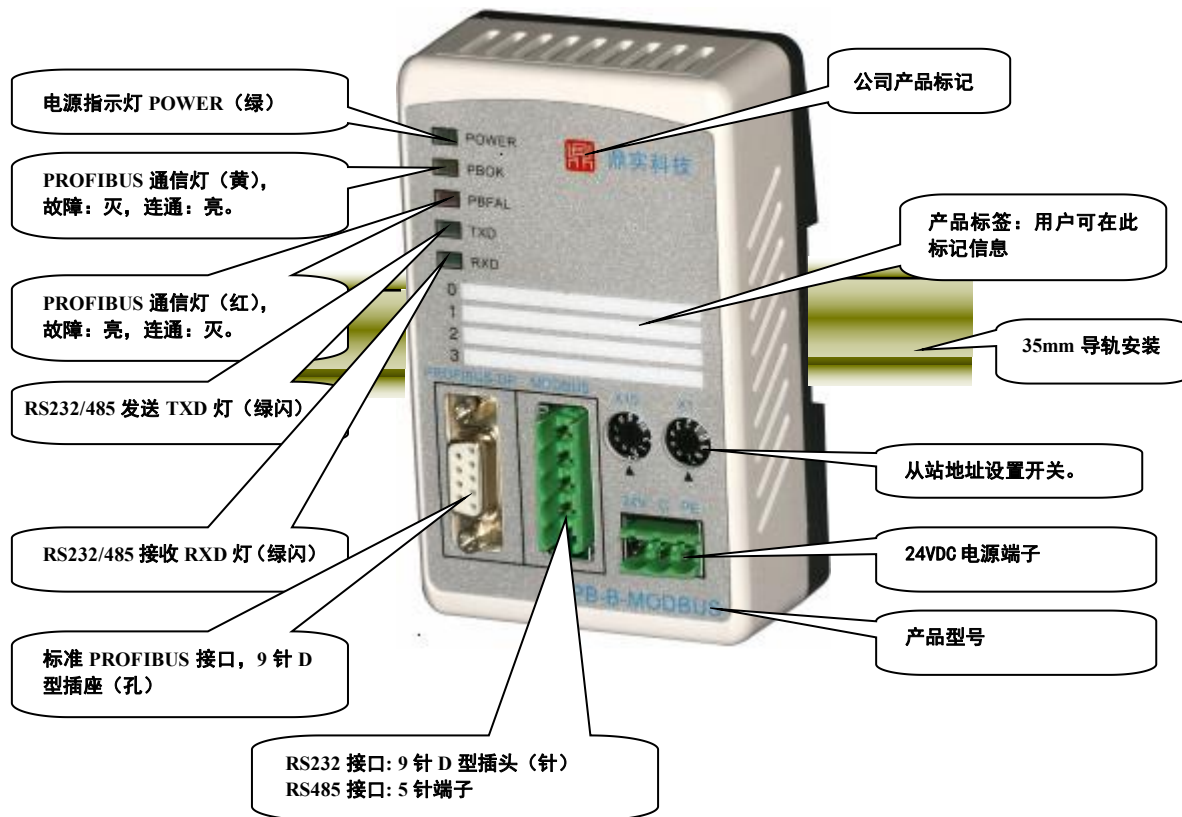


图 2-1 产品正面

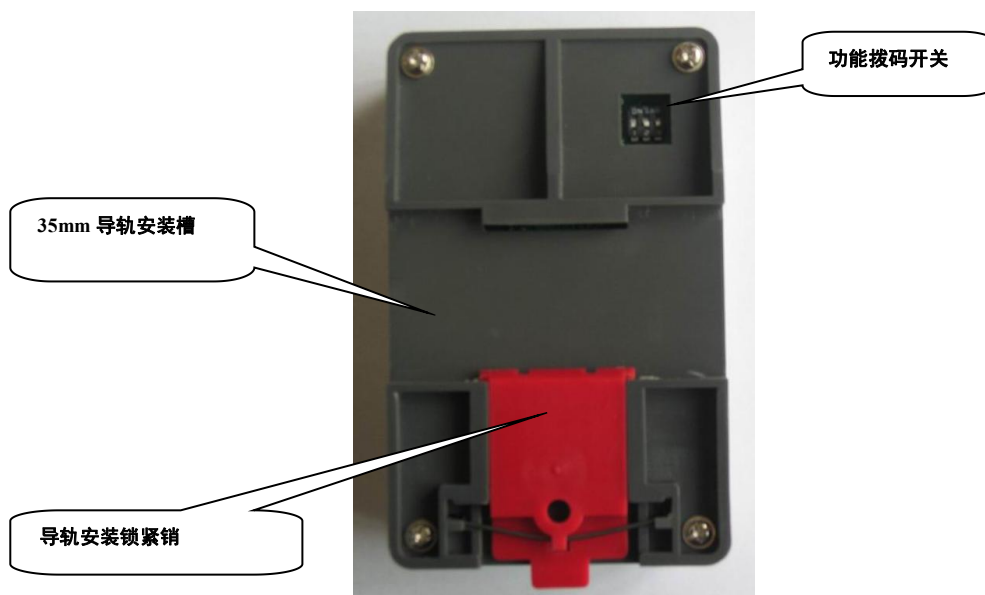


图 2-2 产品背面

2. 安装

产品使用 35mm 导轨安装，见图 2-3:



图 2-3 产品使用 35mm 导轨安装

3. 外形尺寸

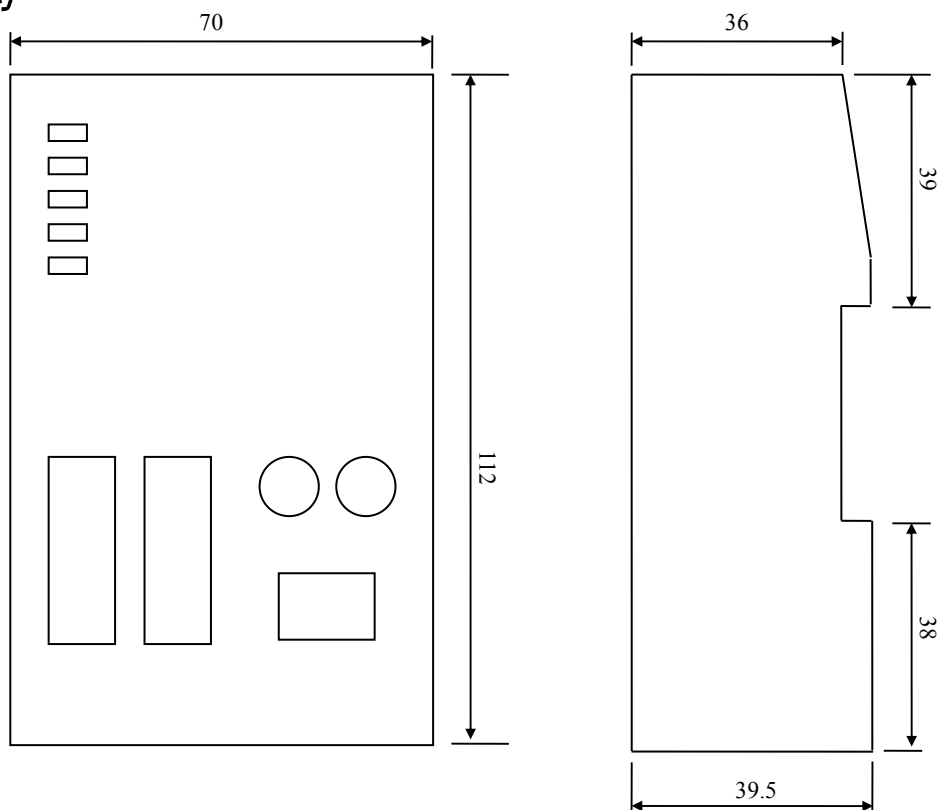


图 2-4 产品外形尺寸图

4. PROFIBUS 接口接插件及安装

PB-B-MODBUS 总线桥的接口，采用标准 9 针 D 形 PROFIBUS 插座（孔）。建议用户使用标准 PROFIBUS 插头及标准 PROFIBUS 电缆。有关 PROFIBUS 安装规范请用户参照有关 PROFIBUS 技术标准。如下图 2-5 所示：

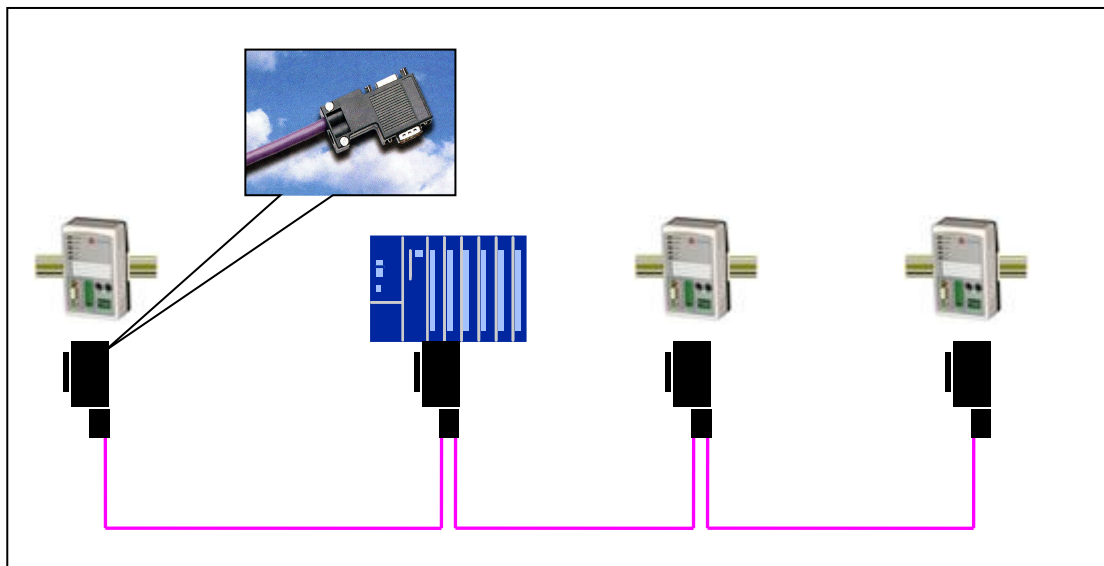


图 2-5 PROFIBUS 接口采用标准 9 针 D 形 PROFIBUS 插头及电缆

5. RS232 接口及电缆

PB-B-MODBUS/232/V3x 的 RS232 接口，采用 9 针 D 形插座（孔），是标准的三线制 RS232 接口。可以按照下图 2-6 自制 RS232 电缆。

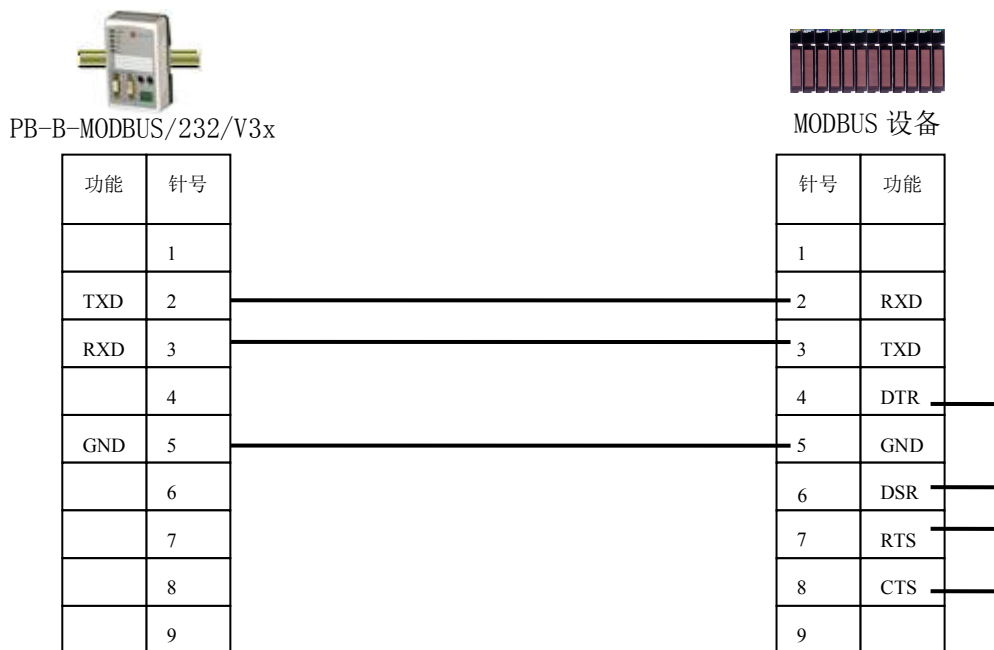


图 2-6 根据设备 232 接口管脚自制 RS232 电缆

注意:MODBUS 设备一端的 9 针插头定义如上图,参考了 MODICON PLC 140 CPU 534 14; 对其它 MODBUS 设备, 请注意它的 RS232 接口的管脚定义, 制作电缆, 使 TXD(2)→RXD, RXD(3)→TXD。

6. RS485 接口及安装

(一) PB-B-MODBUS/485/V3x 的 RS485 接口传输技术的基本特征

PB-B-MODBUS/485/V3x 产品的 485 接口性能与 PROFIBUS 接口端完全一致,是标准的 RS485 接口,以下简述本产品 RS485 特性:

(1) RS485 传输技术基本特征

- ① 网络拓扑: 线性总线, 两端有有源的总线终端电阻;
- ② 传输速率: 2400 bit/s~57.6Kbit/s;
- ③ 介质: 屏蔽双绞电缆, 也可取消屏蔽, 取决于电磁环境的条件 (EMC);
- ④ 站点数: 每分段 32 个站 (不带中继), 最多可达到 127 个站 (带中继);
- ⑤ 插头连接: 5 端子

(2) RS485 传输设备安装要点

- ① 全部设备均与 RS485 总线连接;
- ② 每个分段上最多可接 32 个站;
- ③ 每段的头和尾各有一个总线终端电阻, 确保操作运行不发生误差。两个总线终端电阻应该有电源。

见图 2-7 所示。

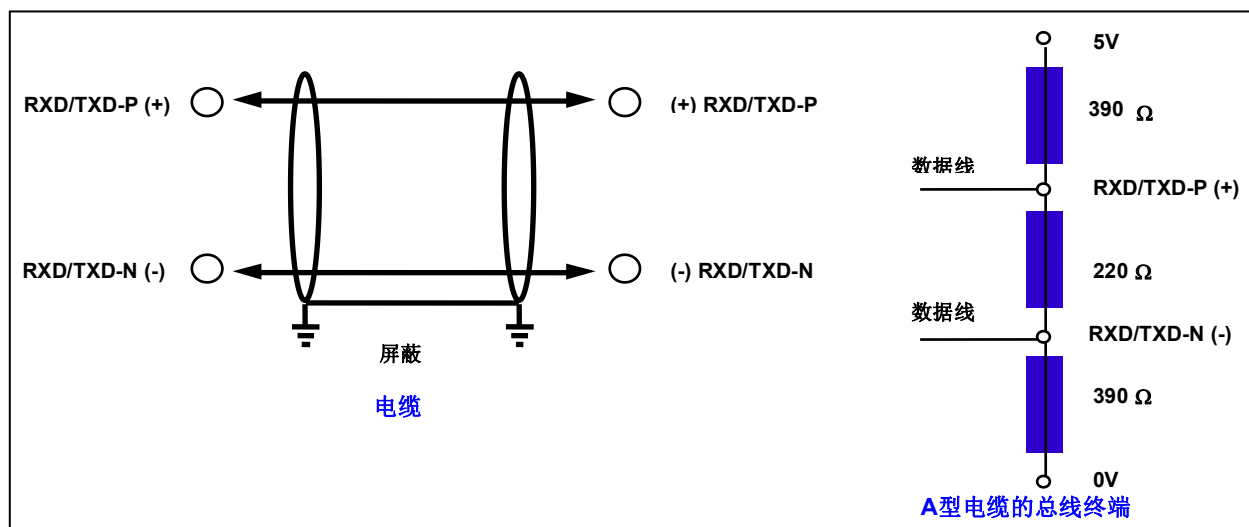


图 2-7 RS485 的电缆接线和总线终端电阻

- ④ 电缆最大长度取决于传输速率。如使用 A 型电缆, 传输速率 $<187.5K$ 时与电缆最大长度为 1200M。
- ⑤ A 型电缆参数:

阻抗: 135-165 Ω	电容: $<30\text{pf/m}$	回路电阻: 110 Ω
线规: 0.64mm	导线面积: $>0.34\text{mm}^2$	
- ⑥ 如用屏蔽编织线和屏蔽箔, 应在两端与保护接地连接, 并通过尽可能的大面积屏蔽接线来复盖, 以保持良好的传导性, 另外建议数据线与高压线隔离。

(二) PB-B-MODBUS485/V3x 接口极性

PB-B-MODBUS485/V3x 产品 485 接口端子的极性如图 2-8 所示：

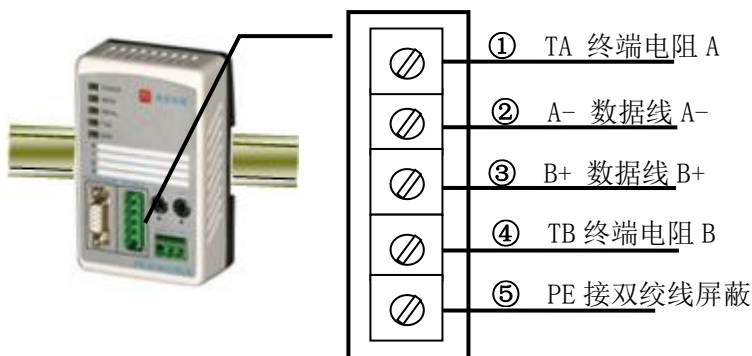


图 2-8 PB-B-MODBUS/RS485/V3x 产品 RS485 接口端子的极性

(三) RS485 终端的接法

PB-B-MODBUS/485/V3x 产品 485 接口性能与 PROFIBUS 接口端完全一致，RS485 总线两端应有终端电阻，见图 2-9 所示：

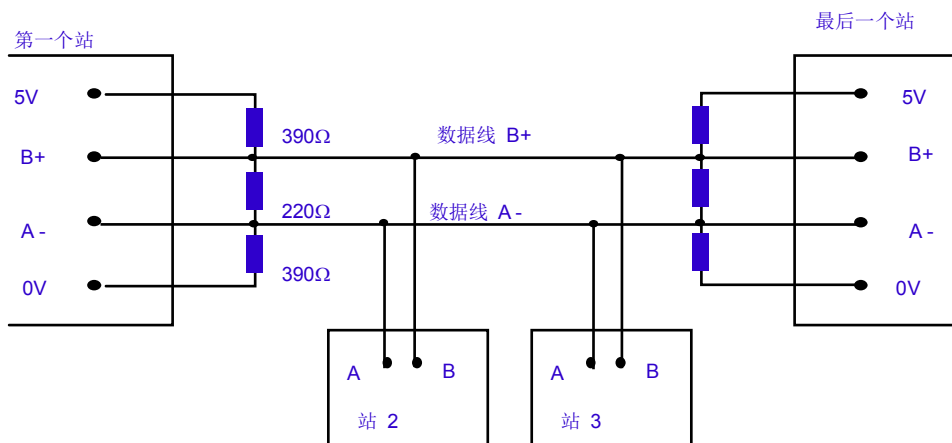


图 2-9 RS485 总线两端应有终端电阻

PB-B-MODBUS/485/V3x 产品已将终端电阻集成到产品中，见图 2-10：

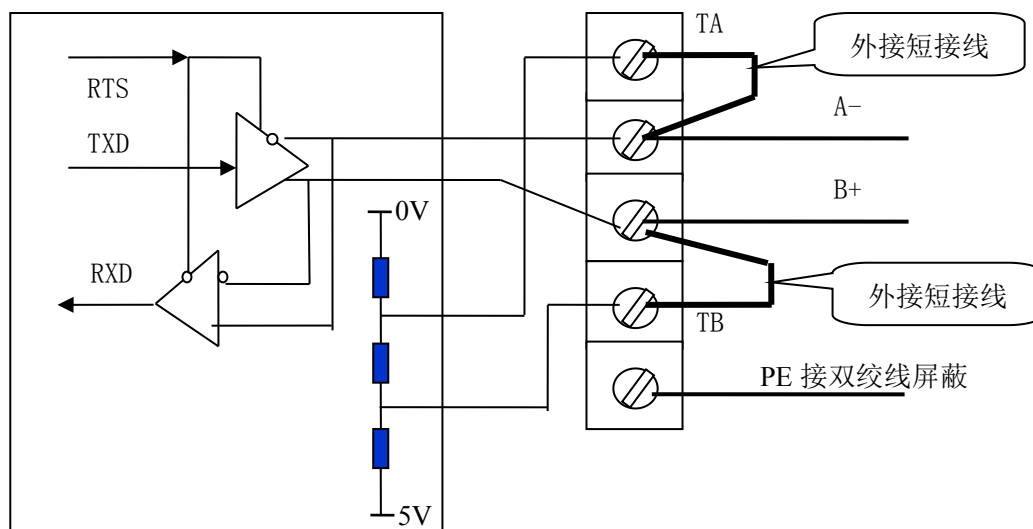


图 2-10 PB-B-MODBUS/485/V3x 产品内部集成了总线终端电阻

因此，当 PB-B-MODBUS/485/V3x 位于 RS485 总线终端时，应在 A-和 TA 间及 B+、TB 间各外接短接线，以便将内置的终端电阻接入总线。见图 2-10、图 2-11 中 RS485 端子外接短接线的连接。

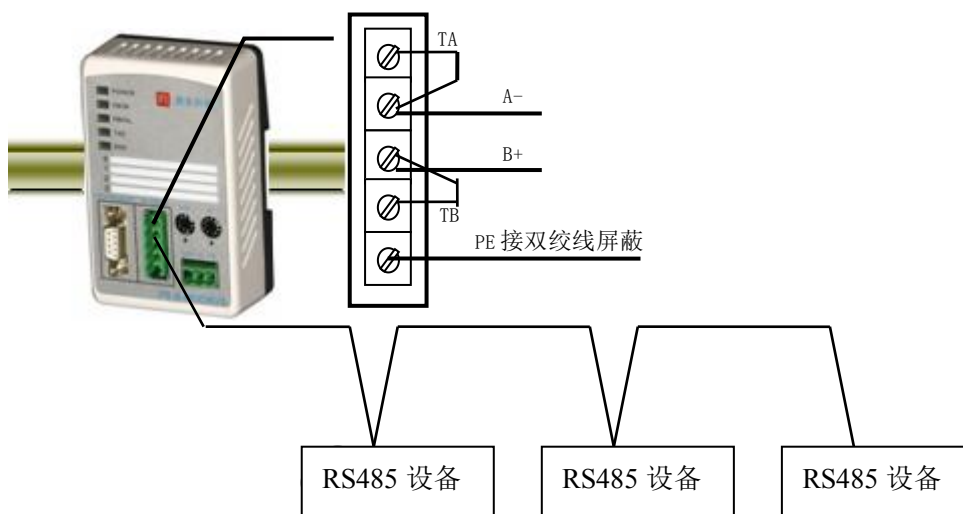


图 2-11 PB-B-MODBUS/485/V3x 位于 RS485 总线终端时端子接线方法

当 PB-B-MODBUS/485/V3x 不作 RS485 总线终端时应按下图 2-12 连接 RS485 端子。

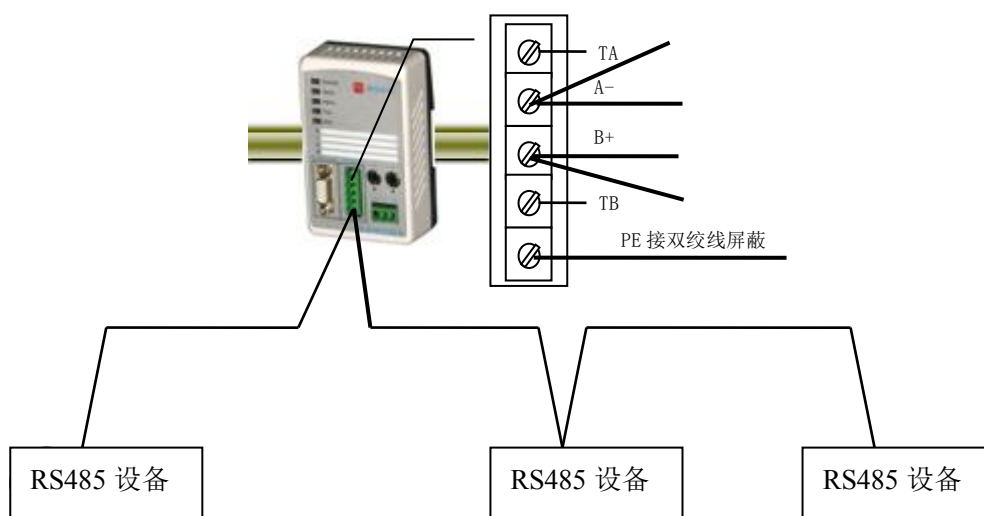


图 2-12 PB-B-MODBUS/485/V3x 不作 RS485 总线终端时端子接线方法

7. 电源

供电： 24VDC(±20%)，额定电流 110mA



8. PROFIBUS 从站地址设置

总线桥在 PROFIBUS 一侧是 PROFIBUS 从站，因此需要设置 PROFIBUS 从站地址。地址设置由产品正面的两个十进制旋转开关 SA 来设置，见下图 2-13，图中将从站的地址设置为 19。



图 2-13 PROFIBUS 从站地址设置开关 SA，地址设为 19

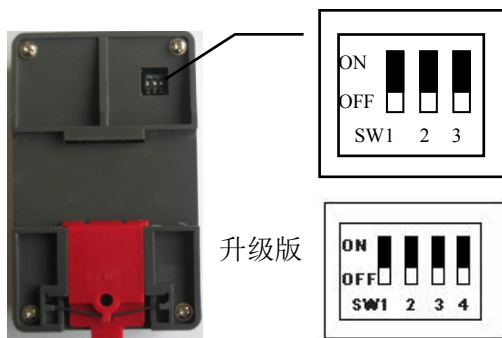


图 2-14 产品背面的功能选择开关

如果需要设置大于 99 的 PROFIBUS 地址，需要使用产品背面的功能选择开关 SW3(3 拨码的桥)或者 SW4(4 拨码的桥)来配合设置地址，见图 2-14 所示。

如果 SW3(3 拨码的桥)或者 SW4(4 拨码的桥) = OFF (向下)，这个从站的地址就是 SA (19)；

如果 SW3(3 拨码的桥)或者 SW4(4 拨码的桥) = ON (向上)，这个从站的地址就是 100+SA (19)=119；

如果 SA >= 27，即使 SW3(3 拨码的桥)或者 SW4(4 拨码的桥) = ON (向上)，本产品 PROFIBUS 仍然是 SA，因为 PROFIBUS 规定从站地址范围是 0~126。

9. 设置总线桥为 MODBUS 主站或 MODBUS 从站

总线桥功能拨码开关 SW1(3 拨码的桥)或者 SW2(4 拨码的桥)，用来设置 PB-B-MODBUS 做主/从站的功能，见下图 2-15：

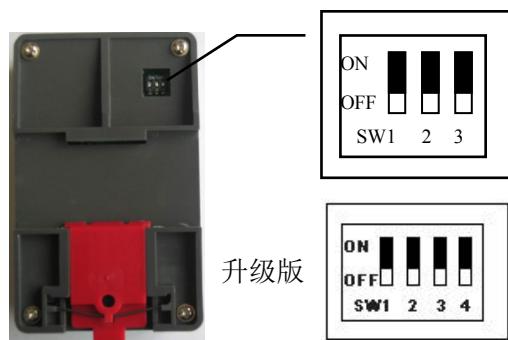


图 2-15 SW1(3 拨码的桥)或者 SW2(4 拨码的桥)设置 MODBUS 主/从站功能

SW1(3 拨码的桥)或者 SW2(4 拨码的桥)=OFF (下位)：产品设定为 PB-B-MM/RS232/485/V3x，即产品为 MODBUS 主站，使用 GSD 文件名为：DS_MMV3x.GSD；

SW1(3 拨码的桥)或者 SW2(4 拨码的桥)=ON (上位)：产品设定为 PB-B-MS/RS232/485/V3x，即产品为 MODBUS 从站，使用 GSD 文件名为：DS_MS3x.GSD。

10. 指示灯

- (1) 电源指示灯 POWER (绿色)。亮: 有电源; 灭: 无电源。
- (2) PROFIBUS 通信状态灯 PBOK (黄色), 亮: PROFIBUS 主站与本总线桥已连通, 进入数据交换状态; 灭: PROFIBUS 主站没有和本总线桥连通。
- (3) PROFIBUS 通信故障灯 PBFAL (红色), 亮: PROFIBUS 通信故障, 灭: PROFIBUS 主站与本总线桥已连通, 进入数据交换状态。
- (4) MODBUS232/485 数据发送 TXD 灯 (绿色)。闪亮: PB-B-MODBUS 向现场设备发送数据。灭: 没有数据发送。
- (5) MODBUS232/485 接收 RXD 灯 (绿色)。闪亮: PB-B-MODBUS 接收现场设备发送的数据。灭: 没有数据接收。

11. 上电步骤及故障排除

(1) PROFIBUS 主站与 PB-B-MODBUS 连通

- ① 确认 24V 电源及极性的连接。
- ② 检查 PROFIBUS 从站地址拨码开关。注意: 只有上电时 PB-B-MODBUS 接口才读一次开关设置的地址。因此, 改变地址必须从新上电。
- ③ 如果 PROFIBUS 主站已配置好本接口从站, 应连接 PROFIBUS 插头。注意: 如果本接口位于 PROFIBUS 站点的两端, 应使用带终端电阻的 PROFIBUS 插头, 并将插头上的终端电阻选择开关打到 “ON” 位置。
- ④ 接通 24V 电源, 电源指示灯 POWER 灯 (绿色) 亮。
- ⑤ PROFIBUS 通信故障灯 PBFAL (红色) 亮, 表明 PROFIBUS 主站与本接口连接失败, 请检查 PROFIBUS 电缆及插头和 PROFIBUS 主站中对本接口的配置 (见本手册第五章)。如果 PROFIBUS 通信故障灯 PBFAL (红色) 灭, 并且 PROFIBUS 通信状态灯 PBOK (黄色) 亮, 说明 PROFIBUS 主站已经和本接口从站建立数据通信, PROFIBUS 一侧已连通。
- ⑥ 常见问题: PROFIBUS 故障灯 PBFAL (红色) 亮, 即 PROFIBUS 没有连通:
 - 检查 PROFIBUS 的连接 (电缆、插头、终端电阻);
 - 检查 PROFIBUS 从站地址拨码开关及配置中对从站地址的设置;

(2) PB-B-MODBUS 主站与 MODBUS 设备的连通

- ① 如果现场设备已经准备好, 可以用 RS232 电缆或 RS485 双绞线电缆连接到 MODBUS 设备上。注意: 尽量避免 RS232 插头的带电插拔。
- ② MODBUS 一侧的通信, 可以观察 MODBUS 发送灯 TXD 和接收灯 RXD。

MODBUS/232/485 通信正常取决于：

- (A) PROFIBUS 主站控制器是否已和 PB-B-MODBUS 连通？可参考(1)。
- (B) PROFIBUS 主站中 PB-B-MODBUS 接口配置正确（如：使用 STEP 7 完成的 HARDWARE 配置，特别是串口波特率等的设置），并将配置下载到 PROFIBUS 主站控制器中；
- (C) PROFIBUS 主站是否将 MODBUS 通信控制字的启动位 start_M=1，启动了 MODBUS 通信？参考“第五章——3 通信控制字与通信状态字——（2）通信控制字格式”。
- (D) 其他问题：参考“第五章——4.PB-B-MODBUS 工作状态及转换——（3）几种错误和故障状态及解除”。

第三章 MODBUS 技术简介

声明：使用 PB-B-MODBUS 产品不必了解 MODBUS 的技术细节，如果读者仅从使用产品角度出发，

可以只阅读本章正体部分（忽略斜体小字部分）。

1. MODBUS 通信协议

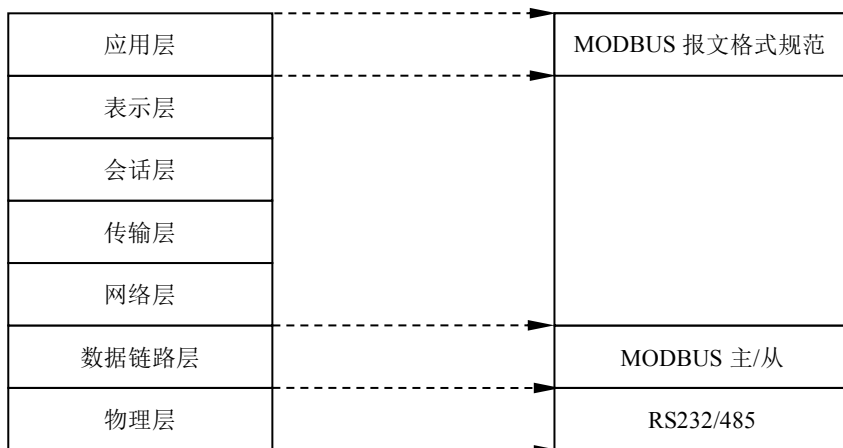
(1) Modbus 协议主要用于控制器之间的通信。通过此协议，两个控制器相互之间或控制器通过网络（例如以太网）和其它设备之间可以进行通信。目前有很多设备采用 MODBUS 的通信协议标准。

(2) 如果按照国际 ISO/OSI 的 7 层网络模型来说，标准 MODBUS 协议定义了通信物理层、链路层及应用层；

物理层：定义了基于 RS232 和 RS485 的异步串行通信规范；

链路层：规定了基于站号识别、主/从方式的介质访问控制；

应用层：规定了信息规范（或报文格式）及通信服务功能；



OSI 参考模型

MODBUS 协议

(3) 目前很多 MODBUS 设备应用都是基于 RS232/485，也有变化的 MODBUS 网络通信，只使用 MODBUS 的应用层（信息规范），而底层使用其它通信协议，如：底层使用以太网+TCP/IP 的 MODBUS 网络通信、底层使用无线扩频通信 MODBUS 网络等等。

2. 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 PB-B-MODBUS 只能用于 RTU 模式。

特性	RTU 模式	ASCII 模式
编码	二进制	ASCII (打印字符: 0-9, a-z, A-Z)
每个字符位数	起始位:1 BIT	起始位:1 BIT
	数据位:8 BITS	数据位:7 BITS
	奇偶校验位(可选):1 位	奇偶校验位(可选):1 位
	停止位:1 或 2	停止位:1 或 2
报文校验	CRC(循环冗余校验)	LRC(纵向冗余校验)

(4) 传输错误校验

- 传输错误校验由奇偶校验、冗余校验检验。
- 当校验出错时，报文处理停止，从机不再继续通信，不对此报文产生应答；
- 通信错误一旦发生，报文便被视为不可靠；MODBUS 主机在一定时间过后仍未收到从站应答，即作出“通信错误已发生”的判断。

(5) 报文级（字符级）采用CRC-16（循环冗余错误校验）

(6) MODBUS 报文RTU 格式

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

3. 异常应答

(1) 从机接收到的主机报文，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。

(2) 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	高位起始地址	低位起始地址	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

(3) 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（见注 1）。
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（见注 2）。
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 有空时再传送。

07	否定	刚发送的编程功能无法执行，应发布“探询”报文以取得详细的设备错误信息。本码只对功能13/14有效（见注2）。
08	存储器奇偶校验错误	扩展存储器的读数对正被访问的存储器数位进行检查。应在错误不会重复发生时进行复验。若所有复验均失败，应维修。
注1：对功能码1—19，异常码04可表示：在应答设备发生不可校正的错误之前，只执行了有关询问报文的一部分。异常功能码04要求立即发布管理通告。		
注2：只是在功能码18发生设备错误信息时，884才支持异常功能码05和06。至于异常码05、06和07之后发生的应答，可参阅具体设备手册的附录A		

4. 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

5. MODBUS 功能

即 MODBUS 应用层，规定了 MODBUS 报文格式和服务功能。

(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：报文中线圈起始地址 00000 对应设备中 00001 地址，其他顺延。

本例：读 11H 号从站输出线圈，起始地址=0013H=19，对应地址 00020；线圈数=0025H=37；末地址=00020+37-1=00056；

因此，本询问报文功能是：读 17（11H）号从站输出线圈 00020—00056，共 37 个线圈状态；

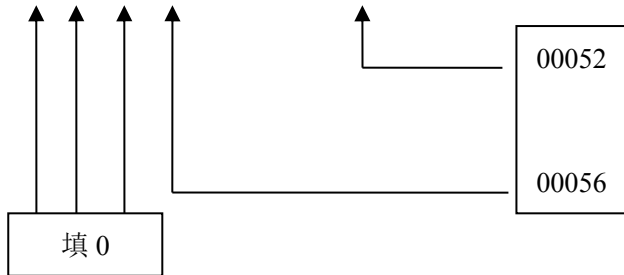
从站应答格式：

地址	功能码	字节计数	线圈状态 20-27	线圈状态 28-35	线圈状态 36-43	线圈状态 44-51	线圈状态 52-56	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 00020-00027；

1B=0 0 0 1 1 0 1 1，对应 00052-00056；



(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：报文中线圈起始地址 00000 对应设备中 10001 地址，其他顺延。

本例：读 11H 号从站输入线圈，起始地址=00C4H=196，对应地址 10197；线圈数=0016H=22，末地址=10197+22-1=10218；

因此，本询问报文功能是：读 17（11H）号从站输入线圈 10197—10218，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 10197-10204	DI 10205-10212	DI 10213-10218	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：报文中寄存器起始地址 00000 对应设备中 40001 地址,其他顺延。

本例：读 11H 号从站保持寄存器值，起始地址=006BH=107，对应地址 40108；寄存器数=0003；末地址=40108+3-1=40110；

因此，本询问报文功能是：读 17（11H）号从站 3 个保持寄存器 40108—40110 的值；

从站应答格式：

地址	功能码	字节计数	寄存器 40108 高位	寄存器 40108 低位	寄存器 40109 高位	寄存器 40109 低位	寄存器 40110 高位	寄存器 40110 低位	CRC
11	03	06	02	2B	01	06	2A	64	XXXX

功能：从站返回保持寄存器 40108—40110 的值；(40108)=022BH，(40109)=0106H，(40110)=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：报文中寄存器起始地址 00000 对应设备中 30001 地址，其他顺延。

本例：读 11H 号从站输入寄存器值，起始地=0008H=0008，对应地址 30009；寄存器数=0001；末地址=30009；因此，本询问报文功能：读 17（11H）号从站 1 个保持寄存器 30009 的值；

从站应答格式：

地址	功能码	字节计数	输入寄存器高位 30009	输入寄存器低位 30009	CRC
11	04	02	01	01	XXXX

功能：从站返回输入寄存器 30009 的值；(30009) =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。报文中线圈起始地址 00000 对应设备中 00001 地址，其它顺延。

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，对应设备中的地址为 00173。强置 17 号从站线圈 0173 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 0173 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。报文中线圈起始地址 00000 对应设备中 40001 地址，其它顺延。

例：预置 17 号从机单保持寄存器 40136 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 40136 值=0x039E 后原文返回。

(7) 读取异常状态

功能码: 07H

本产品 PB-B-MODBUS 暂不支持这一功能。

(8) 回送校验

功能码: 08H

本产品 PB-B-MODBUS 暂不支持这一功能。

(9) 读取通信事件计数器

功能码: 0BH

本产品 PB-B-MODBUS 暂不支持这一功能。

(10) 读取通信事件计数器

功能码: 0CH

本产品 PB-B-MODBUS 暂不支持这一功能。

(11) 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: 报文中线圈起始地址 00000 对应设备中 00001 地址, 其他顺延。

本例: 强置 11H 号从站多个连续线圈, 线圈起始地址=0013H=19, 对应地址 00020; 线圈数=000AH=10; 末地址=00020+10-1=00029;

因此, 本询问报文功能是: 强置 17 (11H) 号从站 10 个线圈 00020—00029 的值; CDH→00020-00027; 00H→00028-00029;

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

(12) 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：报文中保持寄存器起始地址 40000 对应设备中 40001 地址，其他顺延。

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，对应地址 40136，线圈数=0002H=2，末地址=40135+2-1=40137；

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→40136; 0A10H→40137.

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

第四章 协议转换原理

1. PB-B-MODBUS 产品硬件结构

PB-B-MODBUS 是智能型 PROFIBUS 到 MODBUS/232/485 的协议转换接口。在接口 RAM 中建立了 PROFIBUS 到 MODBUS 映射数据区，由软件实现 PROFIBUS 和 MODBUS 协议转换及数据交换。见图 4-1：PB-B-MODBUS232 硬件结构及图 4-2：PB-B-MODBUS485 硬件结构。

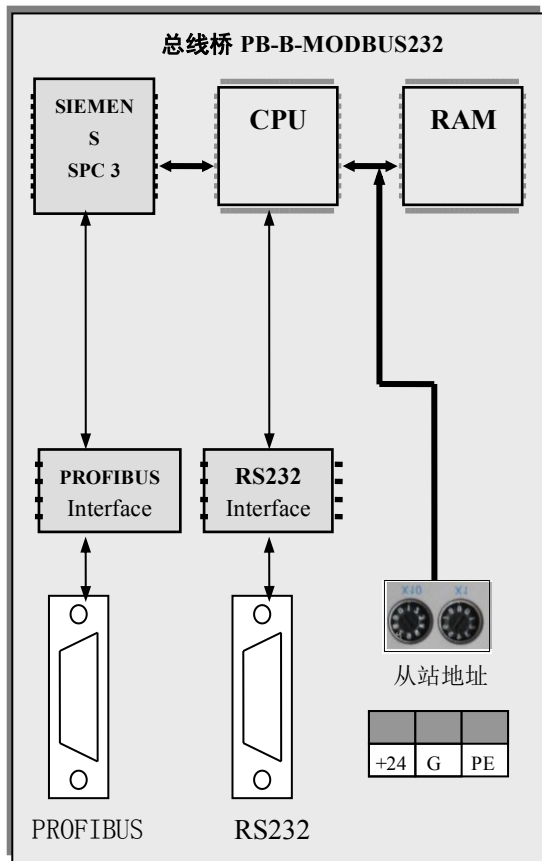


图 4-1 PB-B-MODBUS232 硬件结构

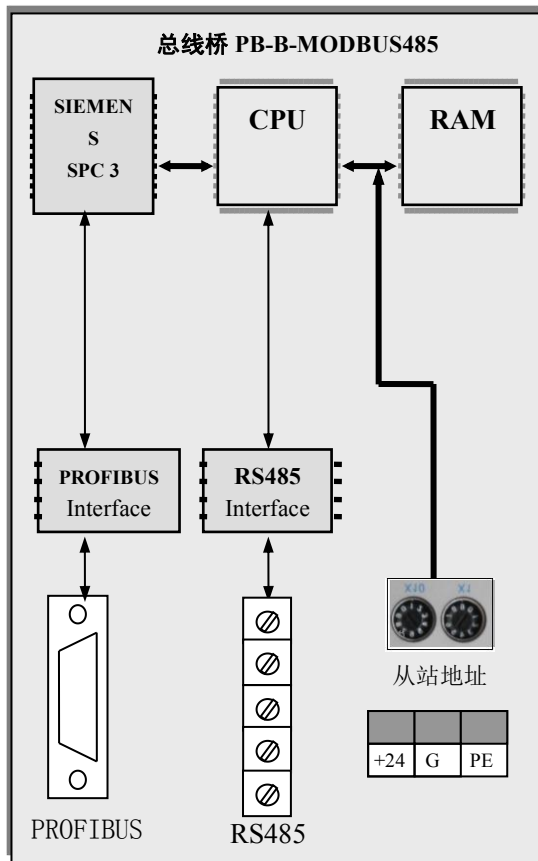


图 4-2 PB-B-MODBUS485 硬件结构

图 4-1、图 4-2 中 SPC3 是西门子公司 PROFIBUS 通信协议芯片。PROFIBUS Interface 是 PROFIBUS 标准驱动电路，由光隔及 RS485 驱动组成。RS232 Interface 是标准的 RS232 驱动电路，由光隔及 RS232 驱动芯片组成。CPU 通过对 SPC3 控制实现 PROFIBUS 的通信，并在 RAM 中建立 PROFIBUS 通信数据缓冲区。另一方面，通过 RS232 Interface 实现和外部 MODBUS 现场设备的通信，同样在 RAM 中建立 MODBUS 通信缓冲区。CPU 通过两个通信缓冲区的数据交换，实现 PROFIBUS 到 MODBUS 的通信。

2. 与 PROFIBUS 的连接

在 PLC 为主站的 PROFIBUS 系统中，PB-B-MM 是一个 PROFIBUS 从站，另一侧 PB-B-MM 通过 RS232/485 与 MODBUS 设备连接，是一个 MODBUS 设备的主站，即主动向 MODBUS 设备发送通信信息、等待设备回答，见图 4-3。PLC 为主站的 PROFIBUS 系统中使用 PB-B-MM 将一个或多个 MODBUS 设备连接到 PROFIBUS 上。图中 PC 机是用于监控的，即二类主站，它在系统中不是必须的。

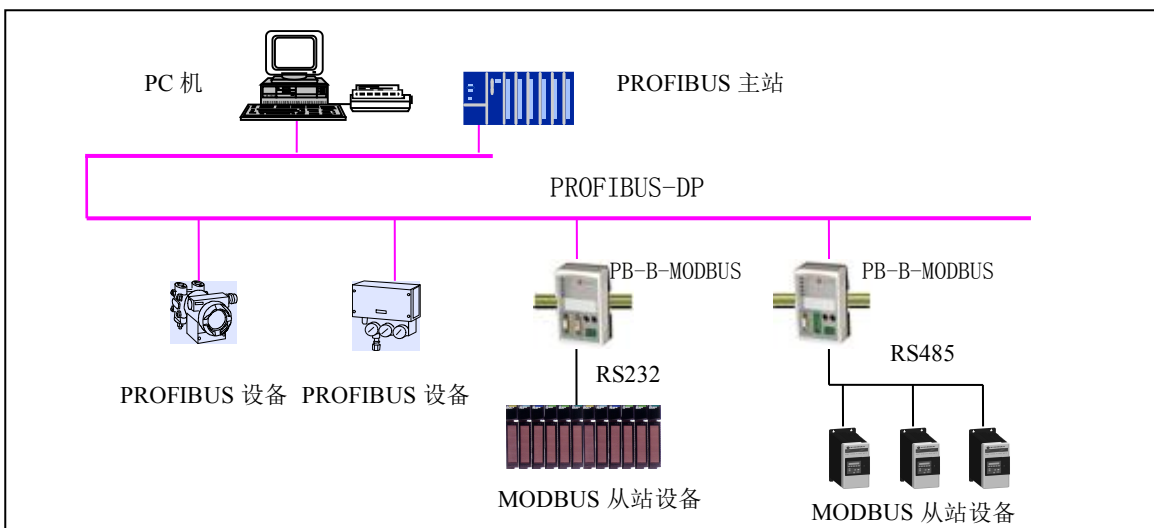


图 4-3 PLC 为主站的 PROFIBUS 系统中使用 PB-B-MM 将设备连接到 PROFIBUS 上

3. PROFIBUS 与 MODBUS 的协议转换原理

本产品依据的 PROFIBUS 与 MODBUS 的协议转换原理见图 4-4，并说明如下：

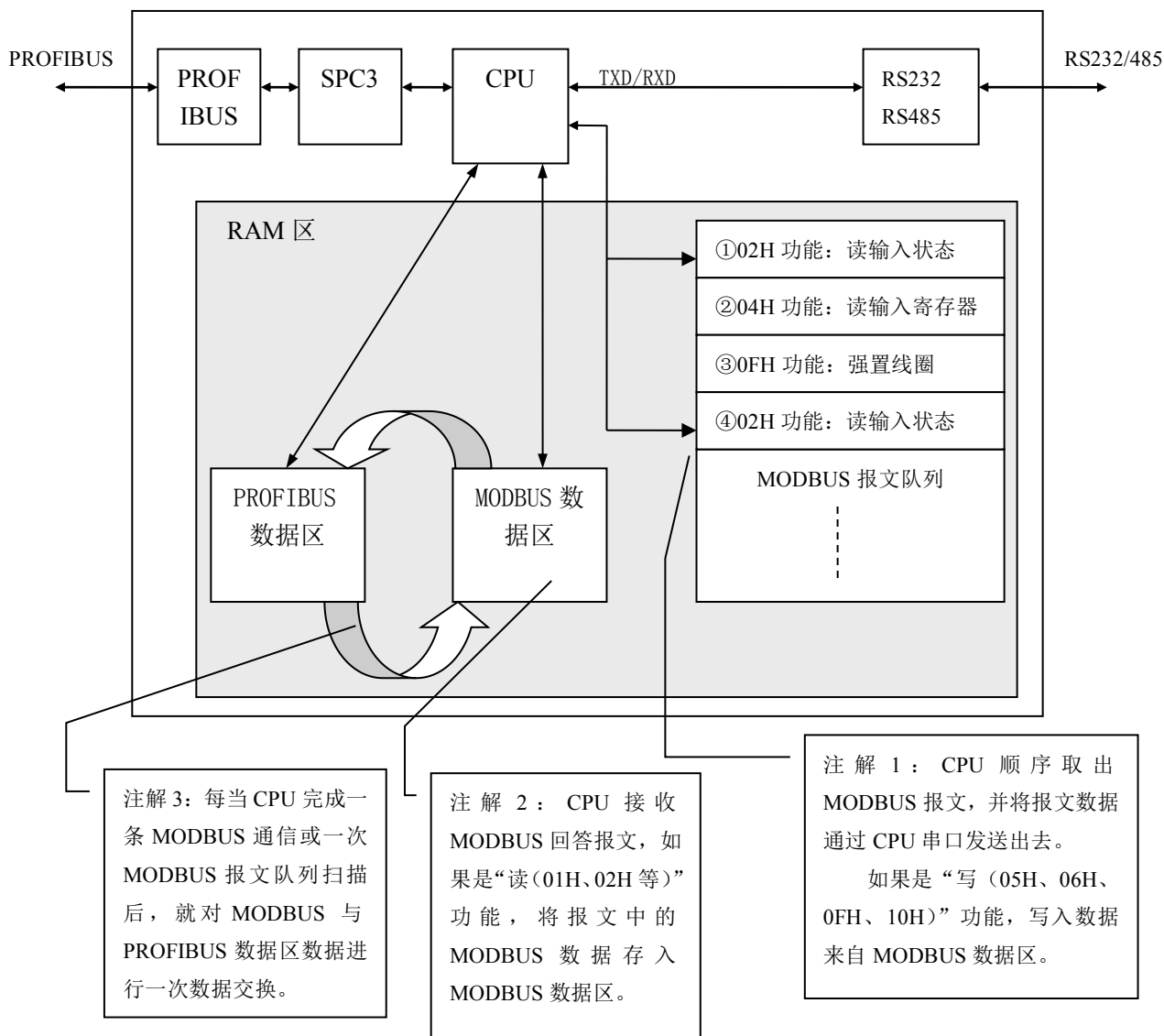


图 4-4 PROFIBUS 与 MODBUS 的协议转换原理

(1) 产品的 RAM 中建立“MODBUS 报文队列”，即 MODBUS 报文序列。它是用户依据应用的要求，

在 PROFIBUS 主站配置本接口产品时，由菜单选择后自动形成，并在主站与本接口连接时传送到本产品的 RAM 中。关于如何依据应用要求，在配置菜单中选择 MODBUS 通信功能，在第五章中将有详细叙述。

(2) 产品的 RAM 中建立 PROFIBUS 数据区，PROFIBUS 主站与本从站的通信数据都存储在这个数据区中。PROFIBUS 通信数据分为输入和输出数据，都是以 PROFIBUS 主站为基点的。

(3) 产品的 RAM 中建立 MODBUS 数据区，本接口是 MODBUS 主站，与 MODBUS 从站的通信数据都存储在这个数据区中。

MODBUS 通信数据分为输入和输出数据，写入（置入，如 05H、06H、0FH、10H 功能）MODBUS 从站的数据为输出数据，与 PROFIBUS 的输出数据对应；从 MODBUS 从站读回（读，如 01H、02H、03H、04H 功能）的数据为 MODBUS 输入数据，与 PROFIBUS 的输入数据对应。如图 4-5：PROFIBUS 与 MODBUS 数据区。

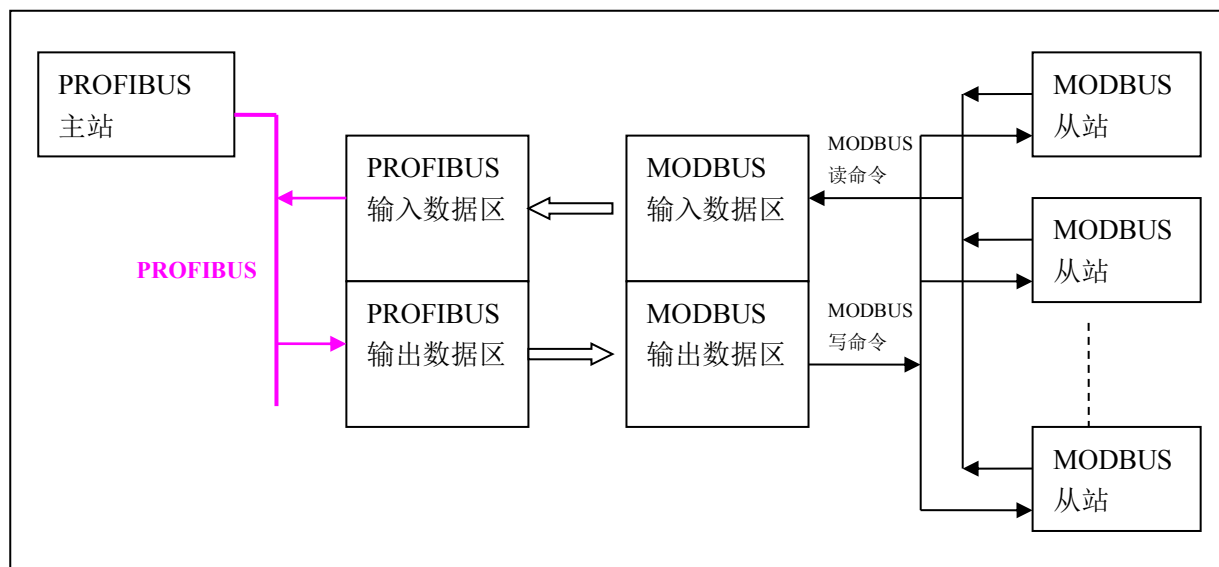


图 4-5 PROFIBUS 与 MODBUS 数据区

(4) CPU 顺序取出 MODBUS 报文，并将报文数据通过 CPU 串口发送出去。如果是“写（05H、06H、0FH、10H）”功能，MODBUS 报文中“写”数据来自 MODBUS 数据区。

(5) CPU 接收 MODBUS 回答报文，如果是“读（01H、02H、03H、04H 等）”功能，将报文中 MODBUS 数据存入 MODBUS 数据区。

(6) 每当 CPU 完成一条 MODBUS 通信或一次 MODBUS 报文队列扫描后，就对 MODBUS 与 PROFIBUS 数据区数据进行一次数据交换。

(7) PROFIBUS 主站通过 PROFIBUS 通信，完成与本接口从站 PROFIBUS 数据区的数据交换。

第五章 产品配置与通信方法

1. 产品配置与通信方法的实例

本章的讲解将以一个实例为背景，本手册以 PB-B-MM 为例介绍产品的配置及通信方法。如下图 5-1 是产品配置与通信方法一个实例：

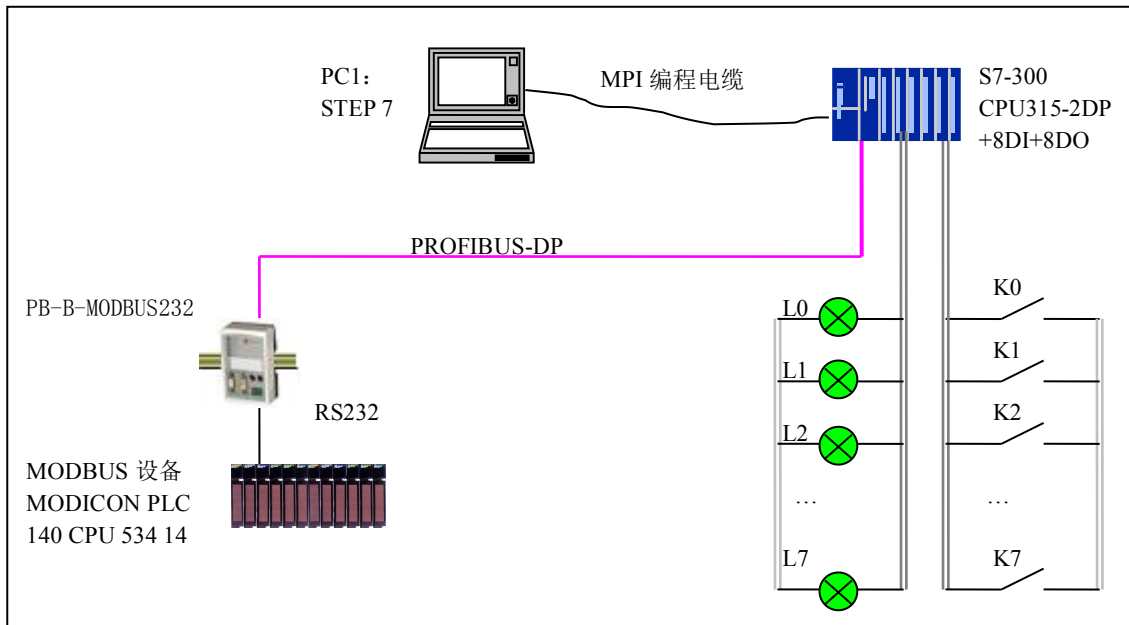


图 5-1 产品配置与通信方法的实例

实例系统配置				
序号	设备名称	型号及技术指标	数量	说明
1	PROFIBUS 主站 PLC/S7-300	CPU315-2DP	1	带 8DI、8DO
2	PROFIBUS/MODBUS 总 线桥	PB-B-MODBUS232	1	GSD 文件： DS_MMV3x.GSD
3	MODBUS 设备	MODICON PLC 140 CPU 534 14	1	2 个 MODBUS 口,9 孔 D 型插头 RS232
4	自锁按钮 K0~K7; 指示灯 L0~L7	接到 S7-300 的 8DI、8DO 模块	1	
5	主站配置及编程软件	STEP 7 V5.2	1	
6	计算机 PC1 及 MPI 编程 电缆		1	

2. 系统配置方法

提示：（一）~（二）是一个 STEP 7 建立一个新项目的一般方法，对于熟悉的读者，可快速浏览，并从（三）开始仔细阅读。

（一）在 PC1-STEP 7 上建立一个“项目”

使用 PC1：

(1) 将 PB-B-MODBUS/V32 的 GSD 文件 DS_MMV32.GSD， COPY 至 PC1： Step7\S7data\gsd\目录下，

产品图标 DS232.bmp 文件 COPY 至 PC1: Step7\S7data\nsbmp\目录下;

(2) 打开  “SIMATIC Manager”，见图 5-2:



图 5-2

(3) File→New, 键入项目文件名: T_MODBUS, →OK, 见下图 5-3:

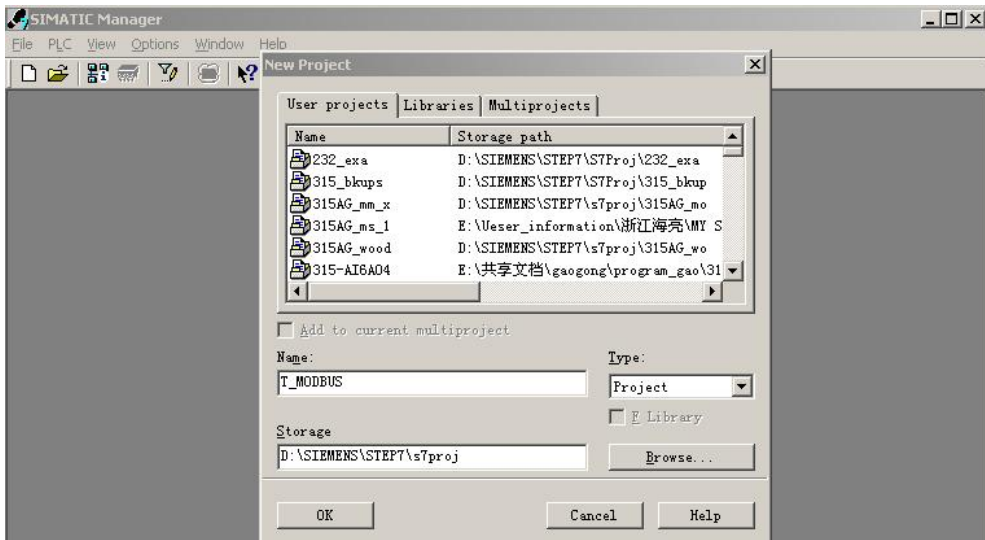


图 5-3

(4) Insert→Station→SIMATIC 300 Station 点击, 见图 5-4。

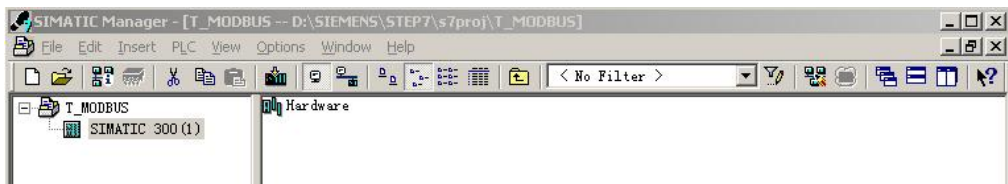


图 5-4

(二) 硬件配置

(1) SIMATIC 300(1)→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 5-5。

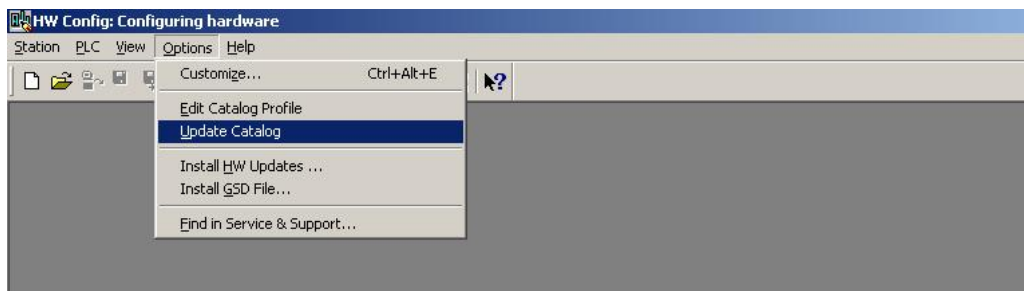


图 5-5

(2) 配置机架: Hardware Catalog\SIMATIC 300\RACK-300\Rail 双击;

(3) 配置 CPU：点中机架 UR 2 槽 → Hardware Catalog\SIMATIC 300\CPU-300\CPU 315-2 DP\6ES7 315-2AF03-0AB0(本例) 双击，见图 5-6 所示，并选择 PROFIBUS 主站站号。

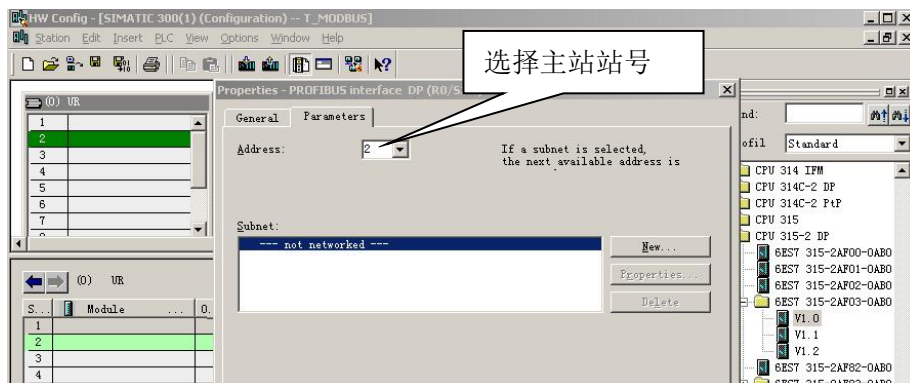


图 5-6

(4) 配置 PROFIBUS：New → Network Settings，选择：DP、187.5kbit/s（仅是举例）→ “OK”，见图 5-7。

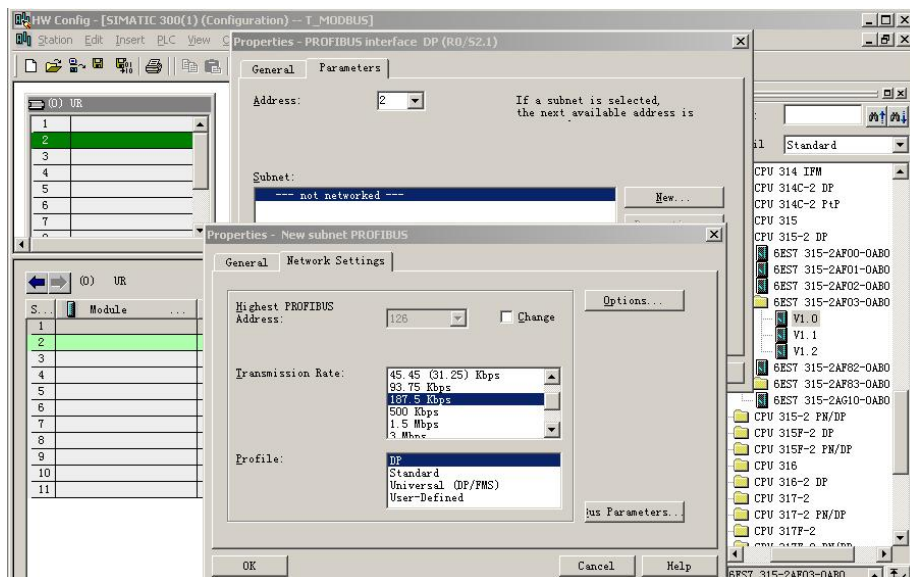


图 5-7

(三) 配置 PB-B-MODBUS 作为 PROFIBUS 从站

(1) 配置 PROFIBUS 从站 PB-B-MM/V32

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\PB-B-MM/V32 双击；

(由于我们已将 GSD 文件 DS MMV32.GSD COPY 至 PC1: Step7\S7data\gsd\目录下，在“(2) Option → Update Catalog 点击。将设备 GSD 文件加入设备 Catalog 中”做了更新，所以现在能够在 Hardware Catalog 中找到我们的产品配置，其他第三方产品的配置办法相同)

选择从站站号，本例选择从站站号为：19 → “OK”，见图 5-8、图 5-9。

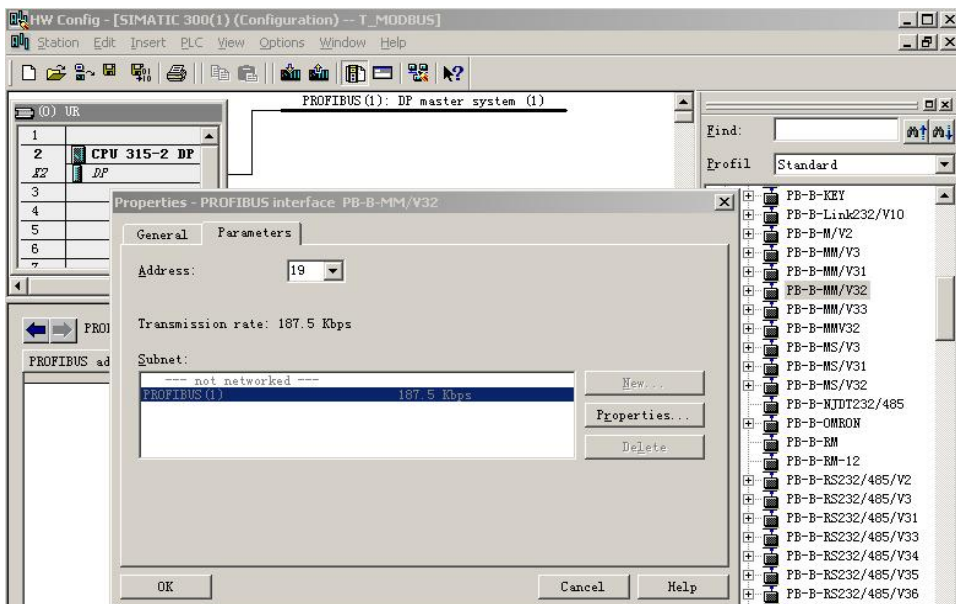


图 5-8

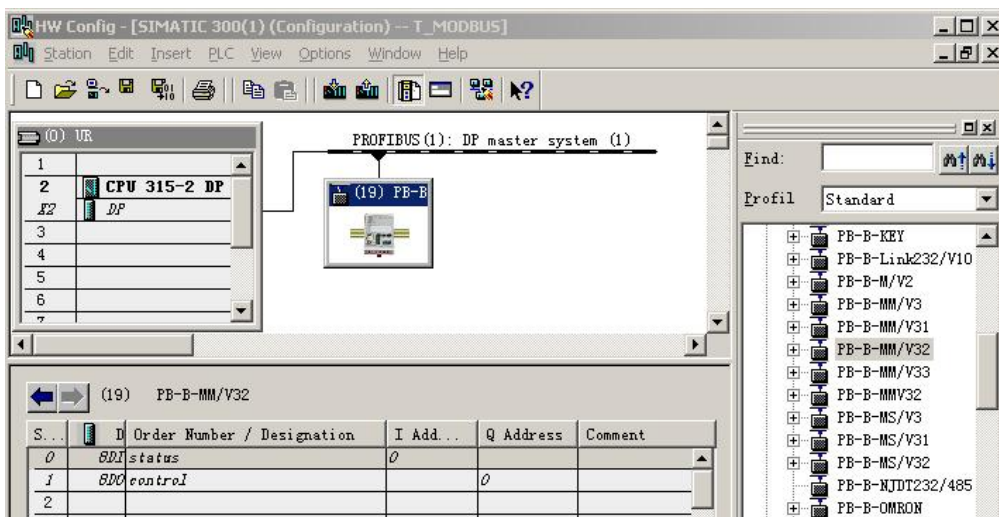


图 5-9

(2) 配置 PB-B-MM/V32 的 RS232 接口

双击 PB-B-MM/V32，弹出 PB-B-MM/V32 设备配置窗口，选择 Parameter Assignment，见图 5-10:

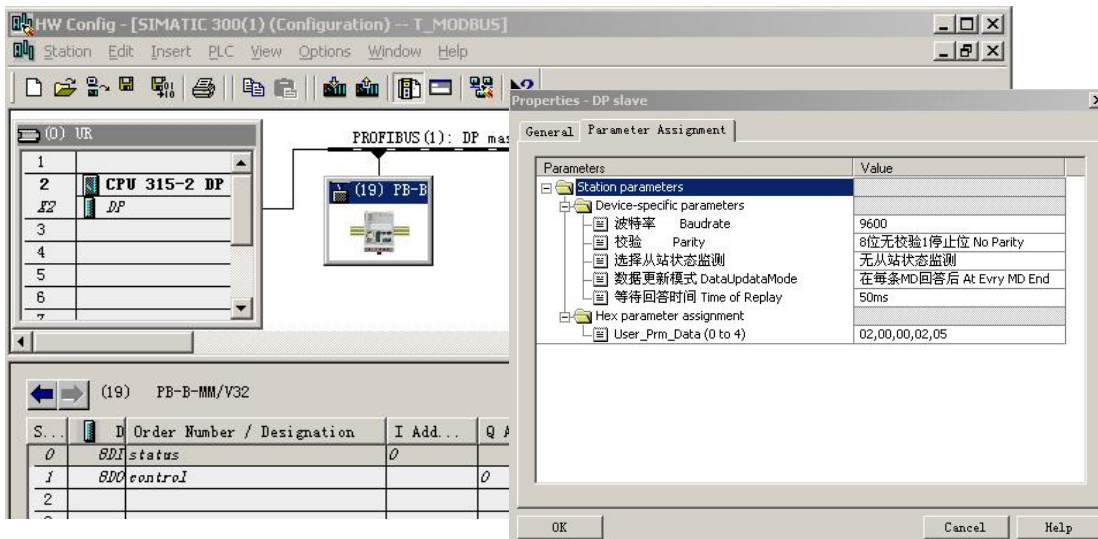


图 5-10

- ① **配置 RS232 波特率**：选中“波特率 Baudrate” → “Value”，本产品支持 2400-57.6K，见图 5-11。
- ② **选择“校验”**：同①选择“校验 Parity”，支持 8 位无校验 1 个停止位、8 位偶校验 1 个停止位、8 位奇校验 1 个停止位和 8 位无校验 2 个停止位，见图 5-11。
- ③ **“主/从”**：产品设置成主站，使用 GSD 文件 DS_MMV32.GSD，只能选择 MODBUS 主站方式。同①步骤相同选择“主站”，见图 5-11。

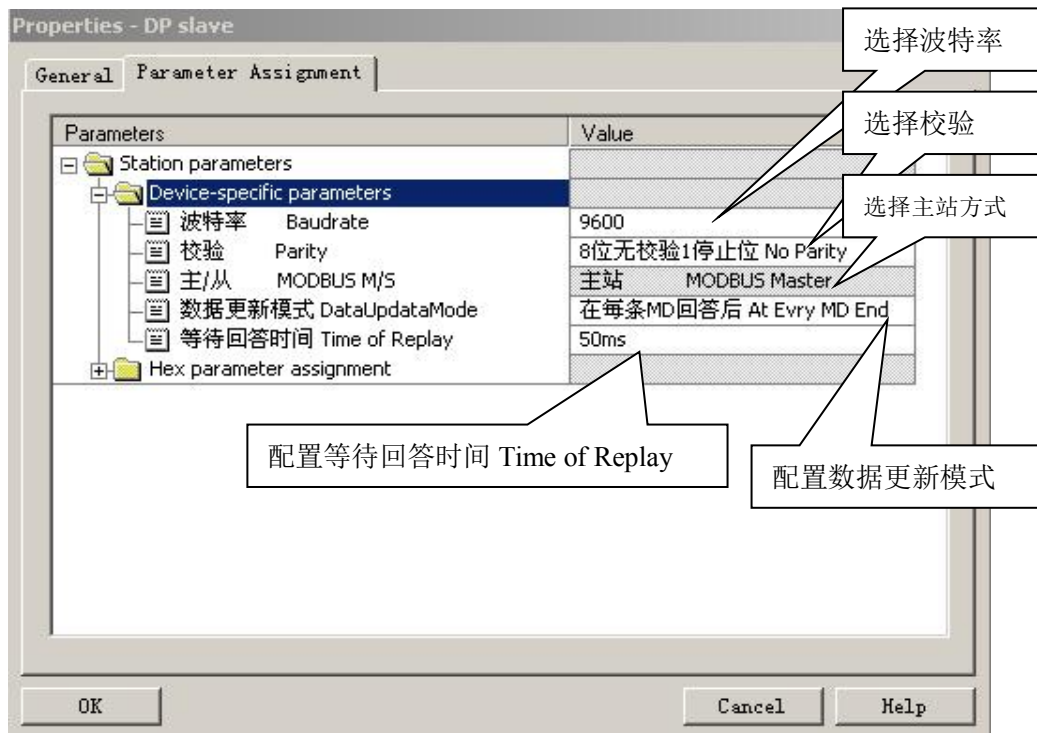


图 5-11

(3) 配置 PROFIBUS 和 MODBUS 数据更新模式

同 (2) 配置 PB-B-MM/V32 的 RS232 接口，设置窗口；选 Parameter Assignment，见图 5-11；

选中“数据更新模式 DataUpdataMode 在每条 MD 回答后 At Evry MD End” → “OK”。

PROFIBUS 和 MODBUS 数据更新模式：是用户指定何时进行 PROFIBUS 数据区与 MODBUS 数据区的数据交换。

① 在每条 MD 回答后 At Evry MD End

在 MODBUS 扫描器完成每一条 MODBUS 通信命令后，就进行一次 PROFIBUS 和 MODBUS 数据区数据交换，这是缺省方式。

这种方式保证以最快速度传递 PROFIBUS 主站到 MODBUS 设备之间的数据。

② 在 MD 扫描结束后 At MD_scan End

在 MODBUS 扫描器完成整个一次 MODBUS 报文队列扫描后，进行一次 PROFIBUS 和 MODBUS 数据区数据交换。

这种方式保证了 MODBUS 通信数据的完整性。

(4) 配置等待回答时间 Time of Replay

选中“等待回答时间 Time of Replay” → “OK”，支持 10ms—1000ms，以及无限期等待。见图 5-11。

等待回答时间(Time of Replay)M_Tsdr:

总线桥发出 MODBUS 报文后等待 MODBUS 设备回答的时间。当 MODBUS 设备超过 M_Tsdr 时间还没有回答，总线桥停止等待，继续发送下一条 MODBUS 报文。M_Tsdr 通常与 MODBUS 设备有关。MODICON PLC 的 M_Tsdr 典型值<50ms。本产品选择范围：10ms~无限期等待回答。

(四) 配置 PB-B-MM/V32 的 MODBUS 报文队列

(1) 在 Hardware catalog 中打开 PB-B-MM/V3x 目录

PB-B-MM/V32 有 0#~38#共 39 个槽（逻辑上，非物理设备），0#、1#槽已占用，剩下 37 个槽提供用户使用。每个槽可以用来插入一条 MODBUS 通信模块(报文)，所以一共可以插入 37 条 MODBUS(报文)。PB-B-MM/V32 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。如图 5-12。模块与 MODBUS 报文类型对应关系如表 5-1。

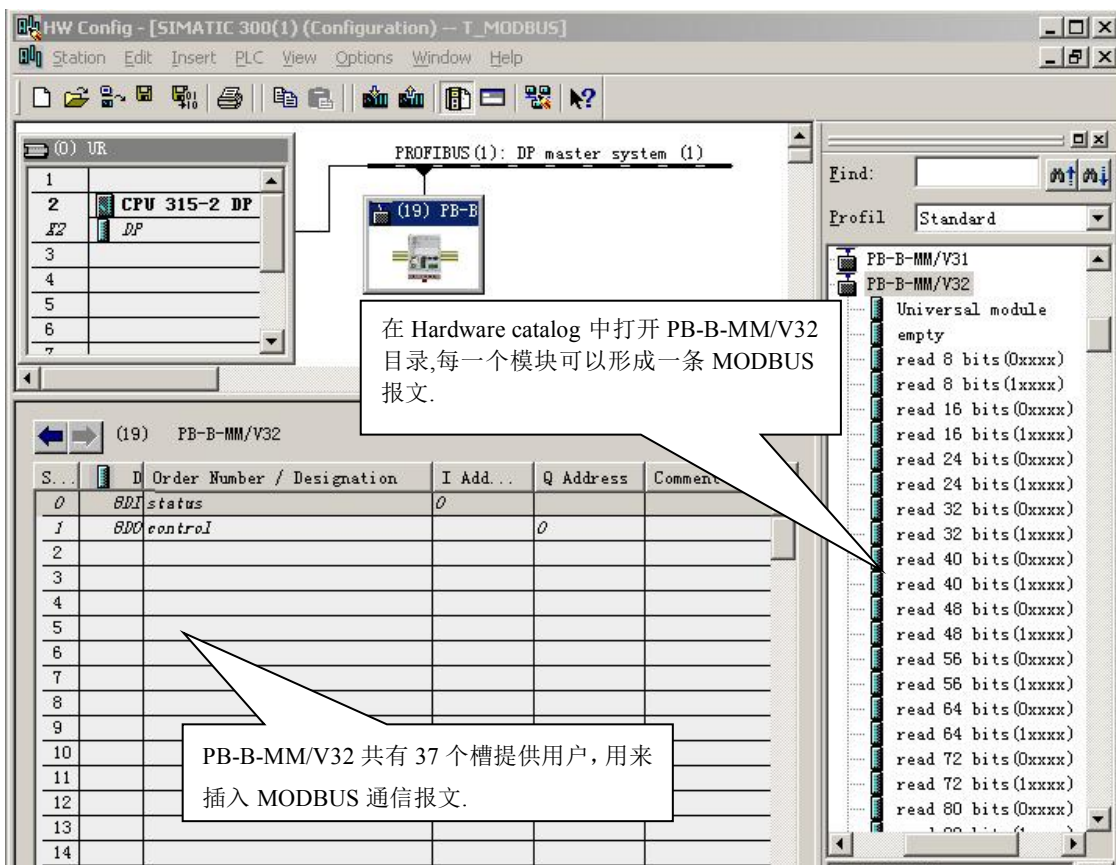


图 5-12

表 5-1 模块与 MODBUS 报文类型对应关系

模块	对应的 MODBUS 报文功能及存储区	需要进一步的配置参数
read X bits (0xxxx) X=8~256	01h 功能, 读取 X 个输出线圈 0xxxx 状态	①MODBUS 从站地址 0-255; ②输出线圈 0xxxx 起始地址 0-65535(取决于 MODBUS 设备);
read X bits (1xxxx) X=8~256	02h 功能, 读取 X 个输入线圈 1xxxx 状态	①MODBUS 从站地址 0-255; ②输出线圈 1xxxx 起始地址 0-65535(取决于 MODBUS 设备);
read X Words (4xxxx) X=1~60	03h 功能, 读 X 个保持寄存器 4xxxx 的值	①MODBUS 从站地址 0-255; ②保持寄存器 4xxxx 起始地址 0-65535(取决于 MODBUS 设备);
read X Words (3xxxx) X=1~60	04h 功能, 读 X 个输入寄存器 3xxxx 的值	①MODBUS 从站地址 0-255; ②输入寄存器 3xxxx 起始地址 0-65535(取决于 MODBUS 设备);
Write X bits (0xxxx) X=8~256	0Fh 功能, 将 X 个连续线圈 0xxxx 强置为 ON/OFF 状态。	①MODBUS 从站地址 0-255; ②输出线圈 0xxxx 起始地址 0-65535(取决于 MODBUS 设备); ③计数个数: 线圈(bit)个数 Y, Y≤X
Write X Words (4xxxx) X=1~60	10h 功能, 预置从站 X 个保持寄存器 4xxxx 值。	①MODBUS 从站地址 0-255; ②保持寄存器 4xxxx 起始地址 0-65535(取决于 MODBUS 设备);
Force single bit (05H Command)	05h 功能, 强置单线圈 0xxxx 值。	①MODBUS 从站地址 0-255; ②输出线圈 0xxxx 起始地址 0-65535(取决于 MODBUS 设备);
set single word (06H Command)"	06h 功能, 预置单保持寄存器 4xxxx 值。	①MODBUS 从站地址 0-255; ②保持寄存器 4xxxx 起始地址 0-65535(取决于 MODBUS 设备);

(2) 举例说明在 2#槽中插入 “read 24 bits(0xxxx)”

本 MODBUS 模块对应 MODBUS 的 01h 功能, 即: 读取 24 个输出线圈 0xxxx 状态。

▼第一步: 选中 2#槽, 然后双击 “read 24 bits (0xxxx)”, 见图 5-13。

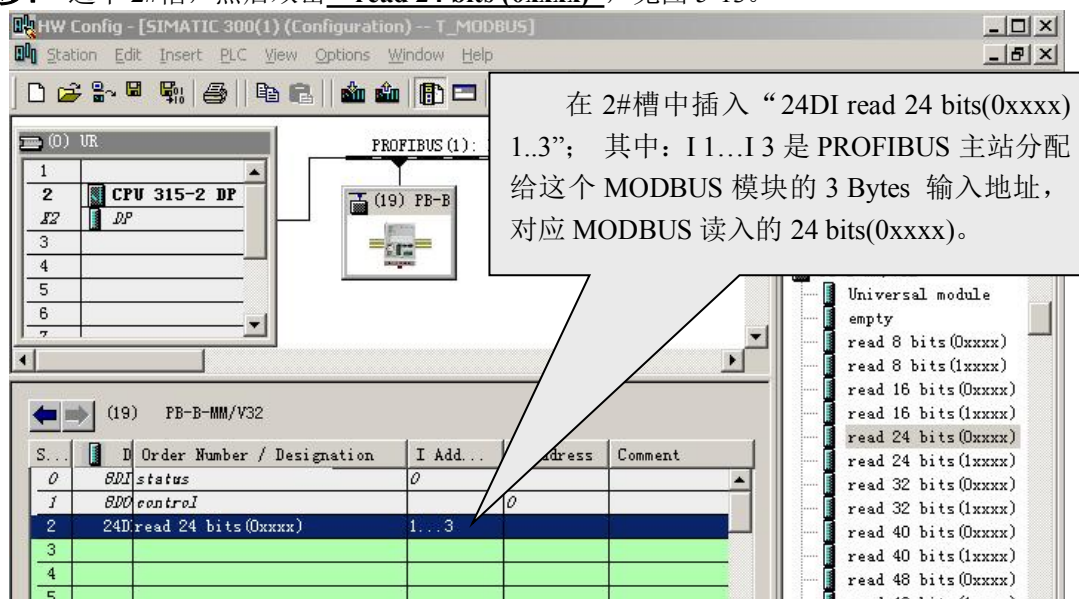


图 5-13

▼ **第二步：进一步设定 MODBUS 参数：**双击 2#槽中的“24 DI read 24 bits(0xxxx) 1..3”；选择“Parameter Assigment”，完成“从站地址”和“起始地址”的参数设定，如图 5-14 所示：

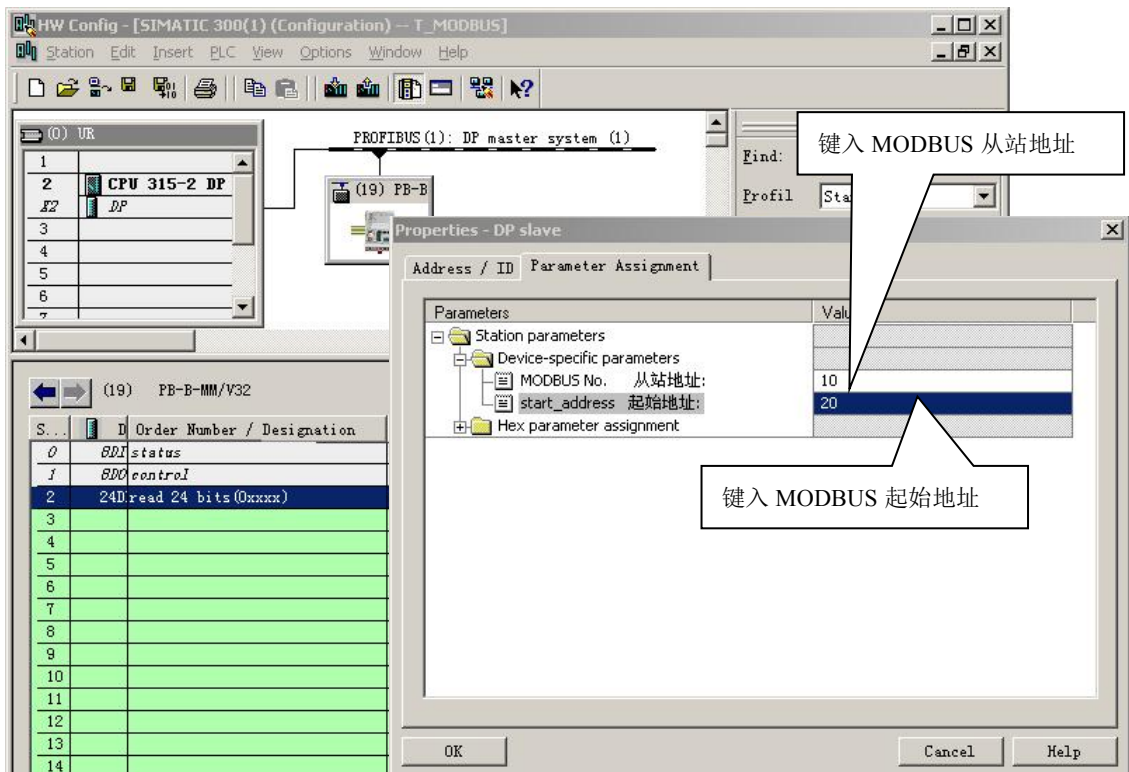


图 5-14

从站地址：指该 MODBUS 模块发送到 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，如图 5-14。

▼ “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，如图 5-14。

PROFIBUS 地址与 MODBUS 地址对应关系：

见图 5-14，其中 I1..I3 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输入地址 I1~I3，对应本 MODBUS 报文读到的 24 bits (0xxxx)，见图 5-15。

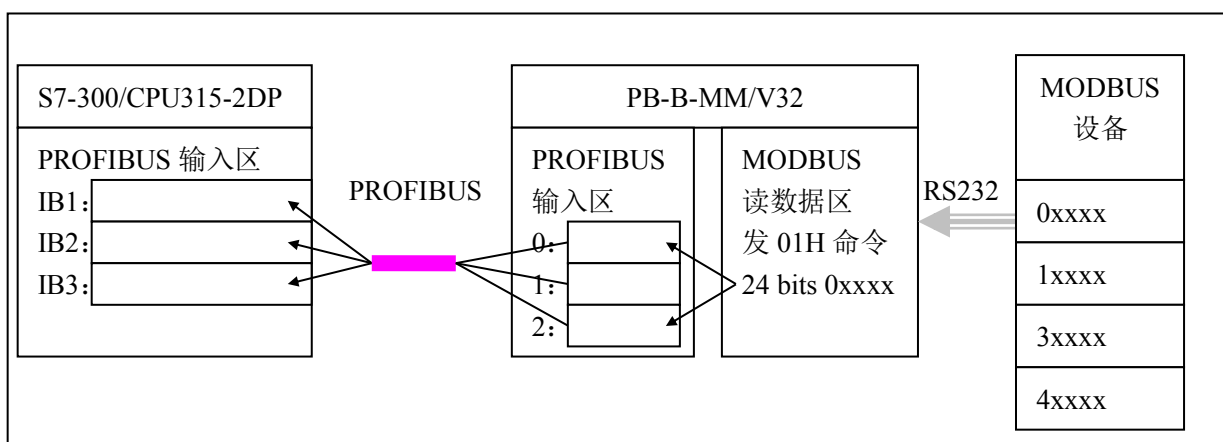


图 5-15

(3) 举例说明在 3#槽中插入 “read 4 Words (3xxxx)”

本 MODBUS 模块对应 MODBUS 的 04h 功能，即读从站输入寄存器 3xxxx 值。

▼**第一步：**选中 3#槽，然后双击 “read 4 Words (3xxxx)”。3#槽中插入 “4AI read 4 Words (3xxxx) IB256..IB263”，见图 5-16。



图 5-16

▼**第二步：**进一步设定 MODBUS 参数：双击 3#槽中的 “read 4 Words (3xxxx)”，选择 “Parameter Assignment”，完成 “从站地址” 和 “起始地址” 的参数设定，如图 5-17。

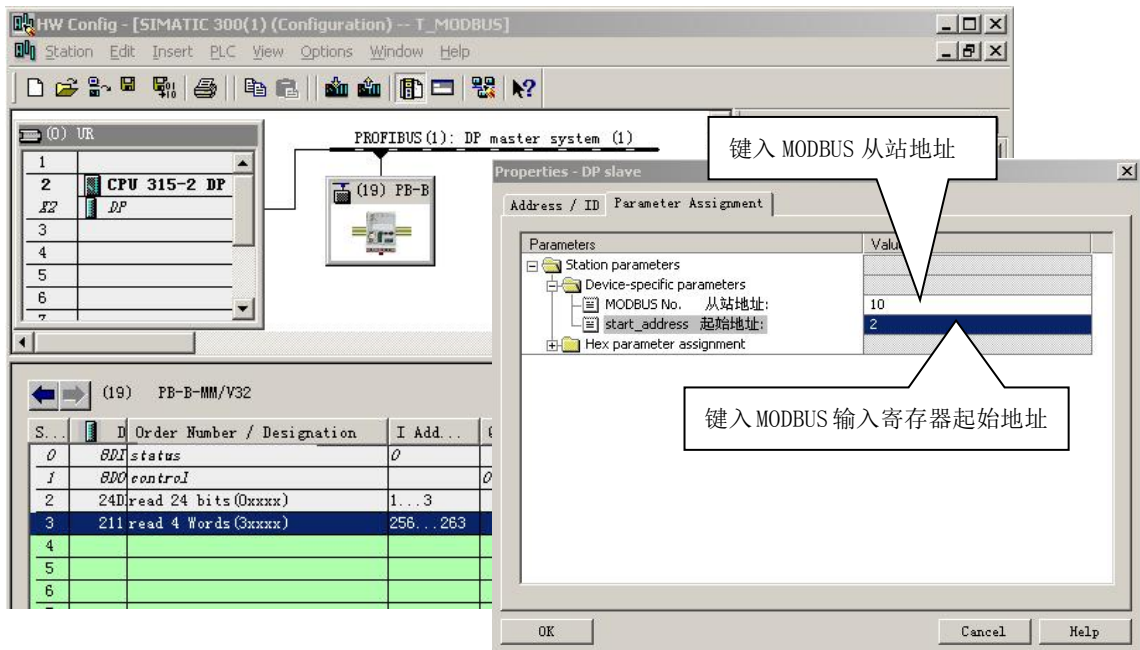


图 5-17

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，对应本 MODBUS 报文的第一个字节。

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。

▼ “MODBUS 从站地址” ⇒ “10”，键入 MODBUS 从站地址，如图 5-17。

▼ “start address 起始地址” ⇒ “2”，键入欲读取的输入寄存器 3xxxx 的起始地址 30001，如图 5-17。

PROFIBUS 地址与 MODBUS 地址对应关系:

见图 5-23，其中，IB256..IB263 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输入地址共 8 Bytes，对应本 MODBUS 报文读到的 4 Words (3xxxx)，见图 5-18:

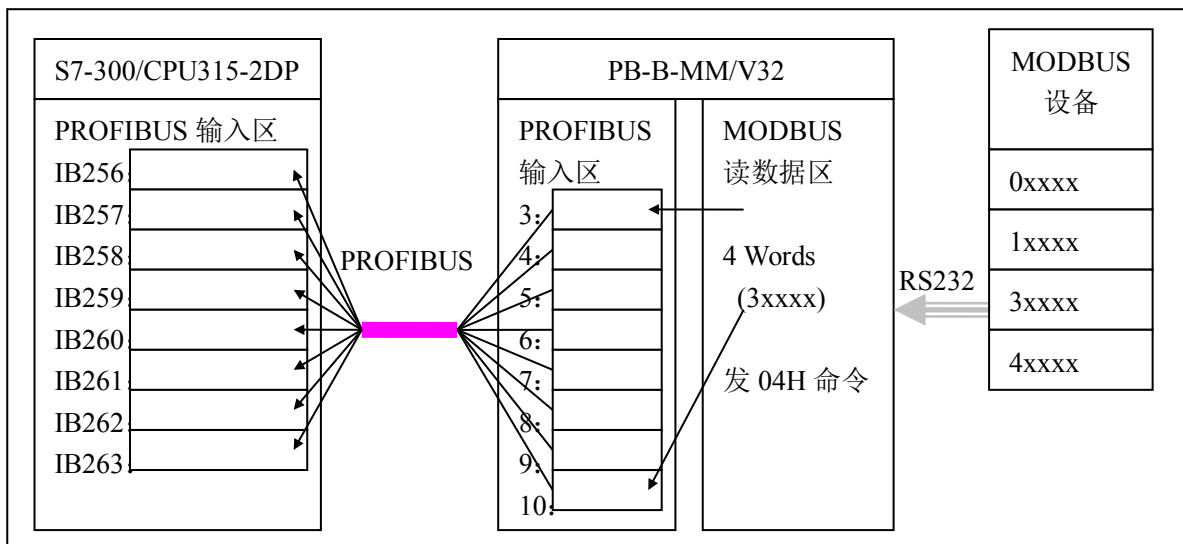


图 5-18

(4) 举例说明在 4#槽中插入 “Write 16 bits (0xxxx)”

本 MODBUS 模块对应 MODBUS 的 0Fh 功能，即将 16 个连续线圈 0XXXX 强置为 ON/OFF 状态。

▼ **第一步:** 选中 4#槽，然后双击 “Write 16 bits (0xxxx)”。4#槽中插入 “16DO Write 16 bits (0xxxx) 1..2”，见图 5-1:

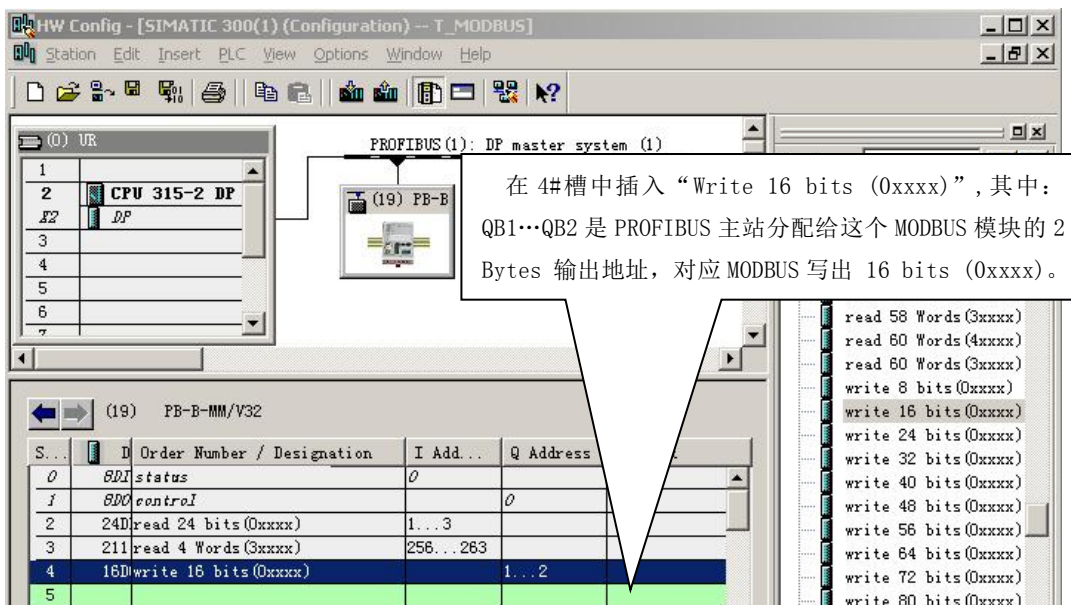


图 5-19

▼ **第二步: 进一步设定 MODBUS 参数:** 双击 4#槽中的 “Write 16 bits (0xxxx)”，选择 “Parameter

Assignment”，完成“从站地址”、“起始地址”和“计数个数”参数的设定。如图 5-20:

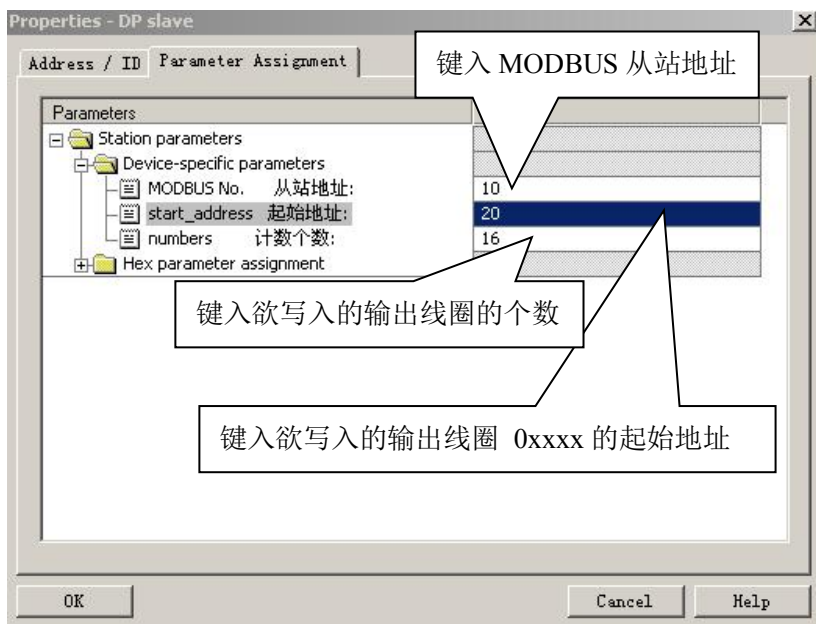


图 5-20

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，对应本 MODBUS 报文的第一个字节。

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。

计数个数：指本 MODBUS 报文要写入 0xxxx 中 bit 的个数。**注意：(本例) 计数个数=1~16，缺省值=16。**

▼ “MODBUS 从站地址” ⇒ “10”，键入 MODBUS 从站地址⇒”OK”，如图 5-20。

▼ “start address 起始地址” ⇒ “20”，键入欲写入的输出线圈 0xxxx 的起始地址，如图 5-20。

▼ “numbers 计数个数” ⇒ “16”，键入欲写入的输出线圈的个数⇒ “OK”，如图 5-20。

PROFIBUS 地址与 MODBUS 地址对应关系:

见图 5-19，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 2 Bytes (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 00021~00036，见图 5-21:

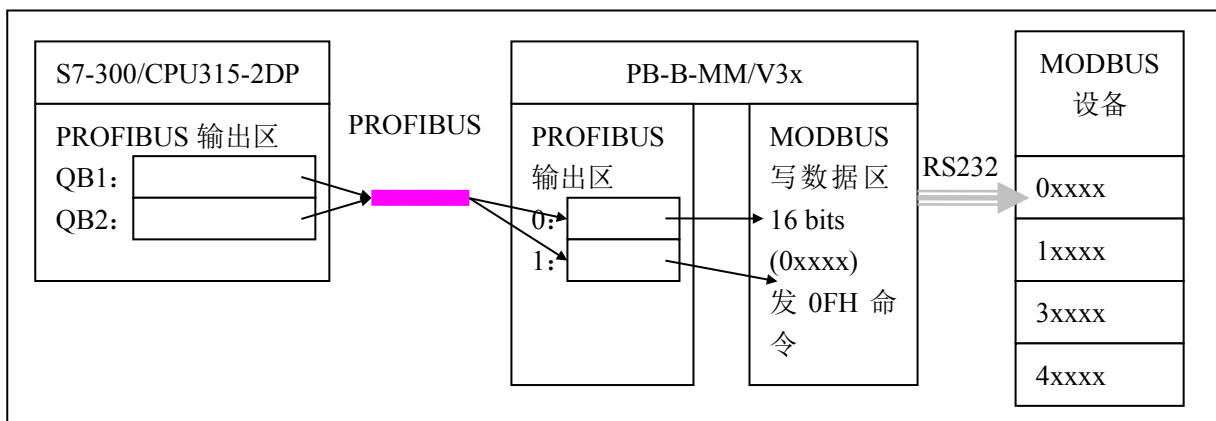


图 5-21

(5) 举例说明在 5#槽中插入 “write 4 Words (4xxxx)”

本 MODBUS 模块对应 MODBUS 的 10h 功能，即预置从站 4 个保持寄存器 4xxxx 值。

▼**第一步：**选中 5#槽，然后双击 “write 4 Words (4xxxx)”。5#槽中插入 “4AO write 4 Words (4xxxx) QB256...QB263”，见图 5-22:

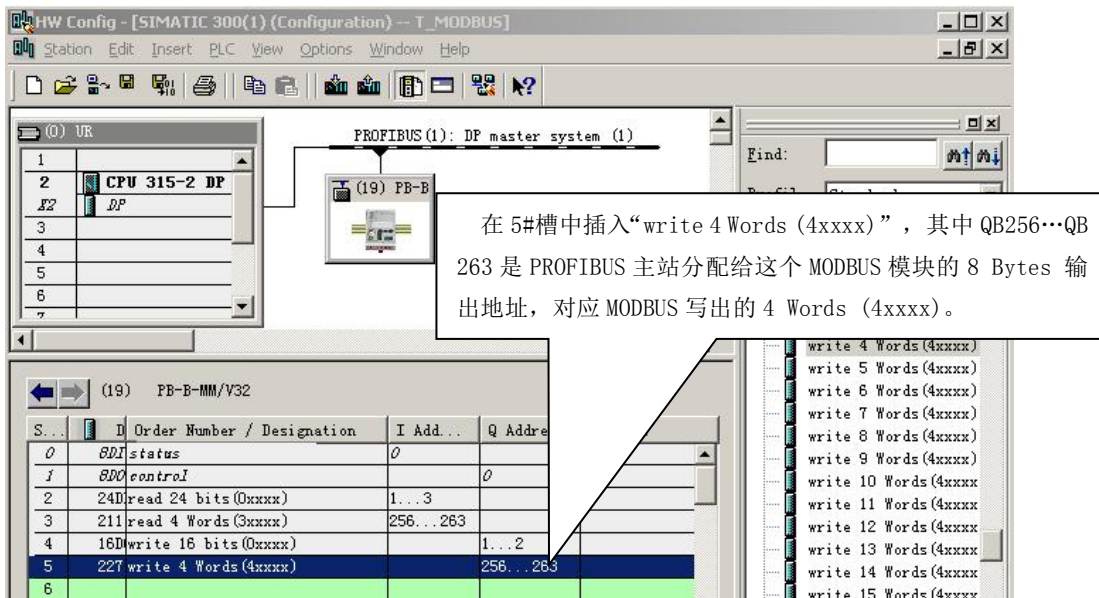


图 5-22

▼**第二步：进一步设定 MODBUS 参数：**双击 5#槽中的 “write 4 Words (4xxxx)”，选择 “Parameter Assigment”，完成 “从站地址” 和 “起始地址” 的参数设定，如图 5-23。

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，对应本 MODBUS 报文的第一个字节。

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。

▼ “MODBUS 从站地址” ⇒ “10”，键入 MODBUS 从站地址 ⇒ “OK”，如图 5-23。

▼ “start address 起始地址” ⇒ “20”，键入欲写入的保持寄存器 4XXXX 起始地址 ⇒ “OK”，如图 5-23。

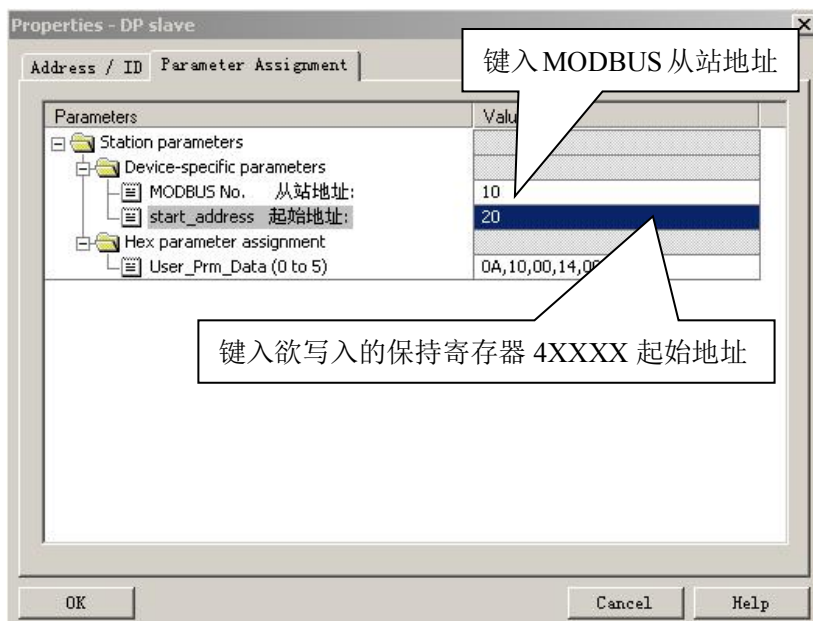


图 5-23

PROFIBUS 地址与 MODBUS 地址对应关系:

见图 5-22，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)，见图 5-24:

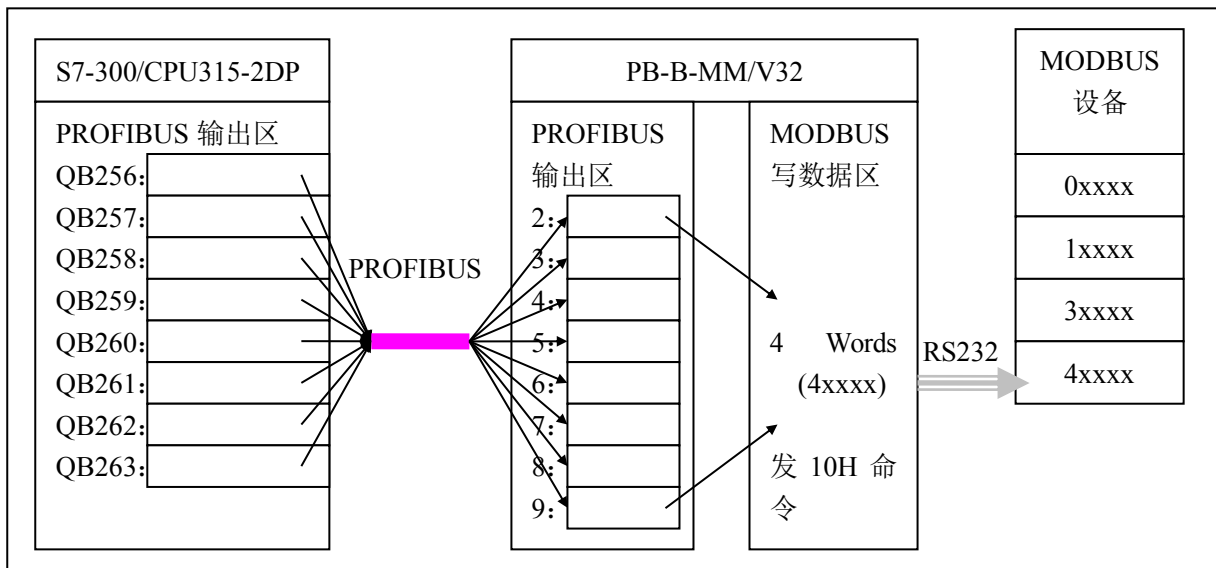


图 5-24

(6) 举例说明在 6#槽中插入 “Force single bit (05H Command)”

该 MODBUS 模块对应 MODBUS 的 05h 功能，即强置从站单线圈 0XXXX 值。

▼**第一步:**选中 6#槽，然后双击“Force single bit (05H Command)”。6#槽中插入“8D0 Force single bit (05H Command)”，见图 5-25:

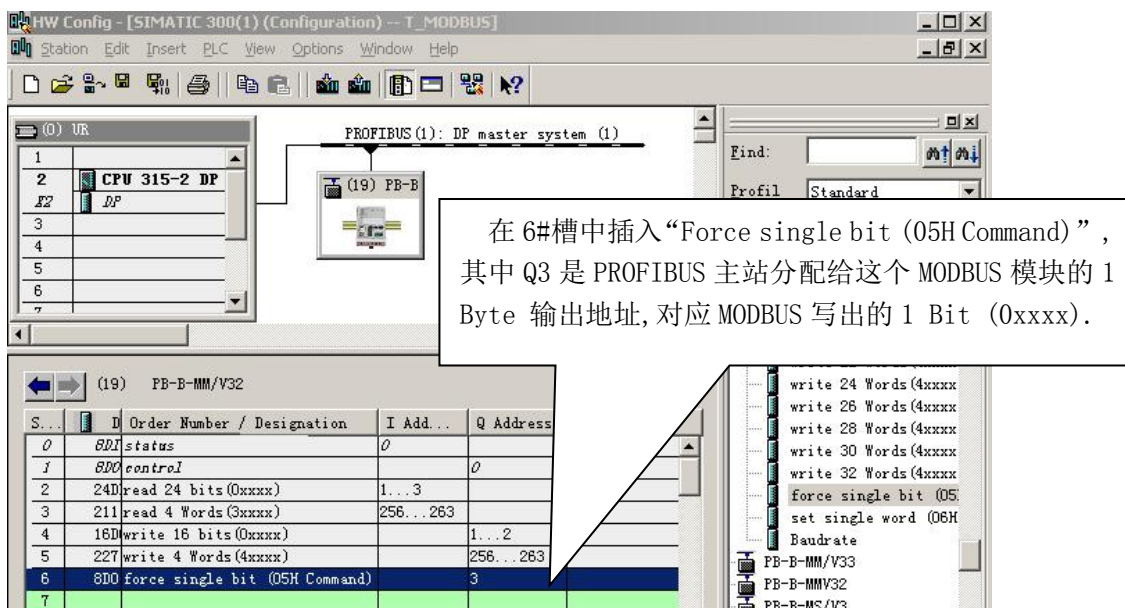


图 5-25

▼**第二步:进一步设定 MODBUS 参数:**双击 6#槽中的“Force single bit (05H Command)”，选择“Parameter Assigement”，完成“从站地址”和“起始地址”的参数设定，如图 5-26 所示:

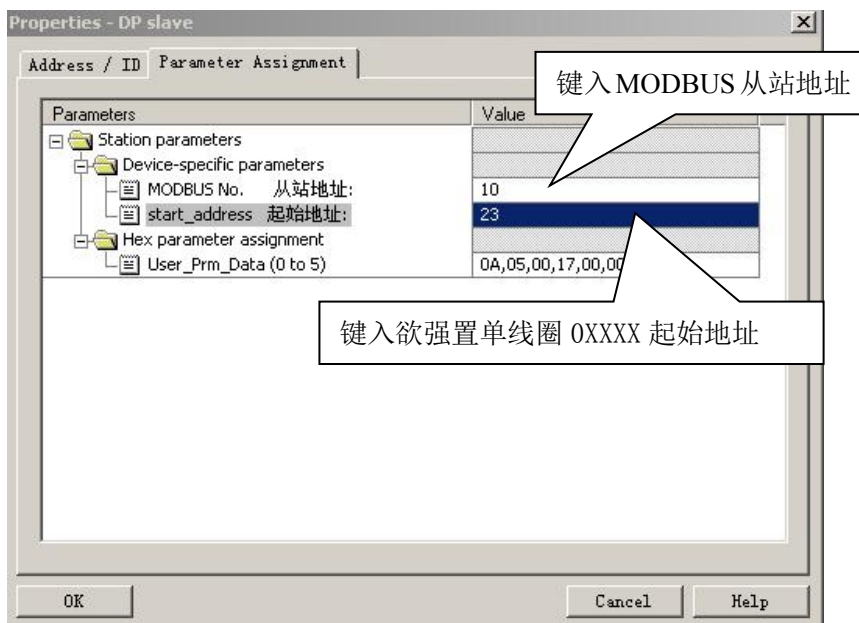


图 5-26

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，对应本 MODBUS 报文的第一个字节。

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 0000 对应设备中 00001 地址，其他顺延。

▼ “MODBUS 从站地址” ⇒ “10”，键入 MODBUS 从站地址，如图 5-26。

▼ “start address 起始地址” ⇒ “23”，键入欲强置单线圈 OXXXX 起始地址，图 5-26。

PROFIBUS 地址与 MODBUS 地址对应关系：

见图 5-25，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 00023（见图 5-39），如果：QB3=0，发单线圈 00024 置 0 命令；若 QB3≠0，发单线圈 00024 置 1 命令，见图 5-27 所示：

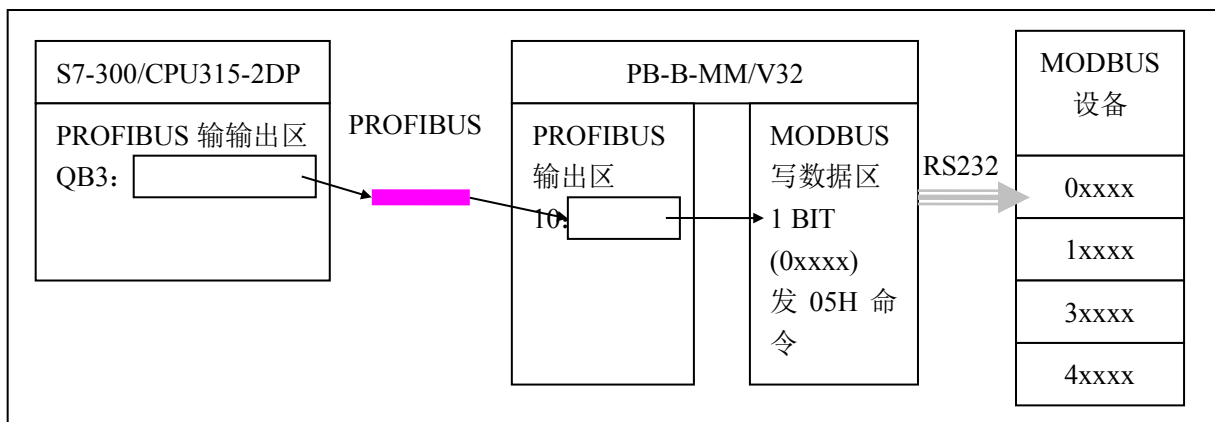


图 5-27

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

本 MODBUS 模块对应 MODBUS 的 06H 功能，即预置单保持寄存器 4XXXX 的值。

▼ **第一步：**选中 7#槽，然后双击“set single word (06H command)”。7#槽中插入“1AO set single word (06H command) QB264...QB265”，见图 5-28：

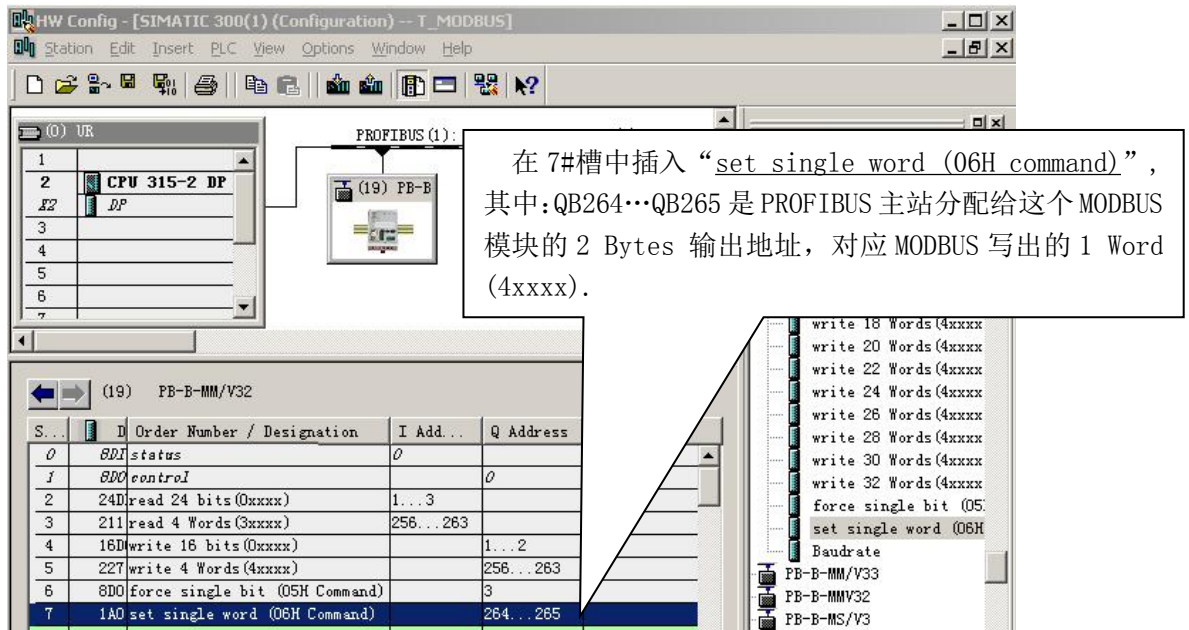


图 5-28

▼ **第二步：**进一步设定 MODBUS 参数，双击 7#槽中的“set single word (06H command)”，选择“Parameter Assignment”，完成“从站地址”和“起始地址”的参数设定，如图 5-29。

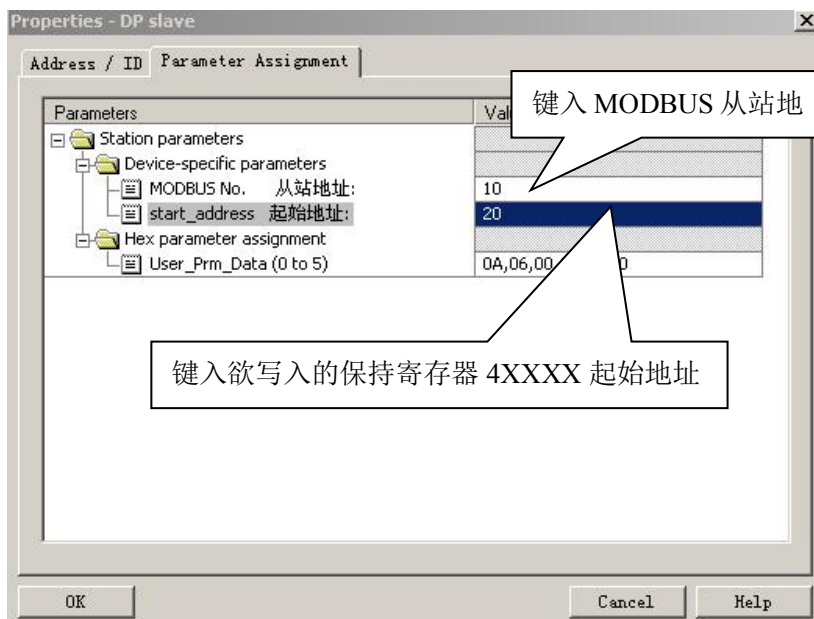


图 5-29

从站地址：指本 MODBUS 报文发送到的 MODBUS 从站的地址，对应本 MODBUS 报文的第一个字节。

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。

▼ “MODBUS 从站地址” ⇒ “10”键入 MODBUS 从站地址，如图 5-29。

▼ “start address 起始地址” ⇒ “20”键入欲写入的保持寄存器 4XXXX 起始地址，如图 5-29。

PROFIBUS 地址与 MODBUS 地址对应关系:

见图 5-27, 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 1 Word (4xxxx), 见图 5-30:

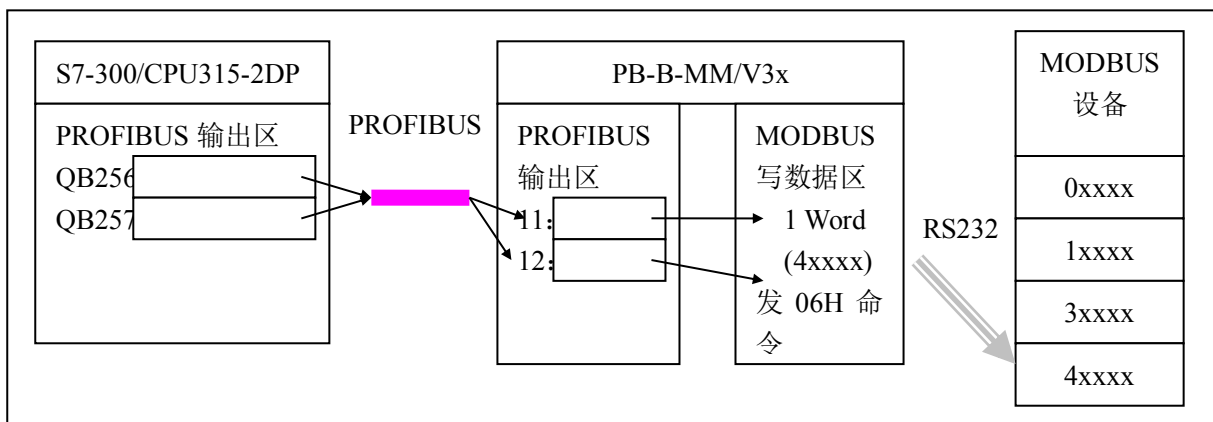


图 5-30

(五) “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 5-31:

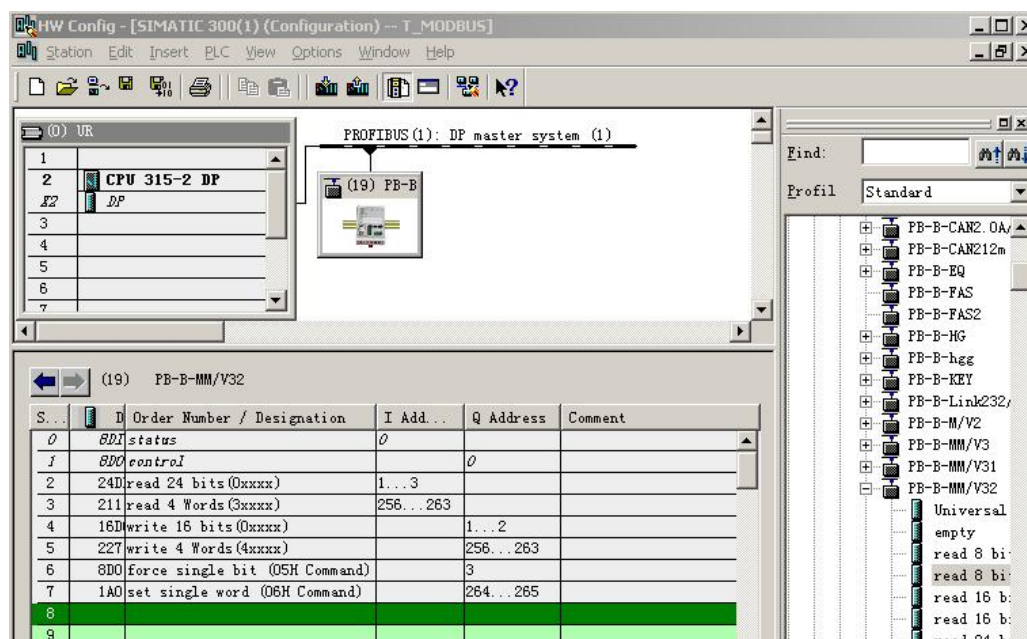


图 5-31

3. 通信控制字与通信状态字

从 PB-B-MM/V32 的硬件配置中可以看到 0#、1#槽被接口占用, 0#槽是一个字节输入, 用作接口 MODBUS 通信的状态字 status, 本例中占用 PROFIBUS 输入地址 IB0。1#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, 见图 5-32。

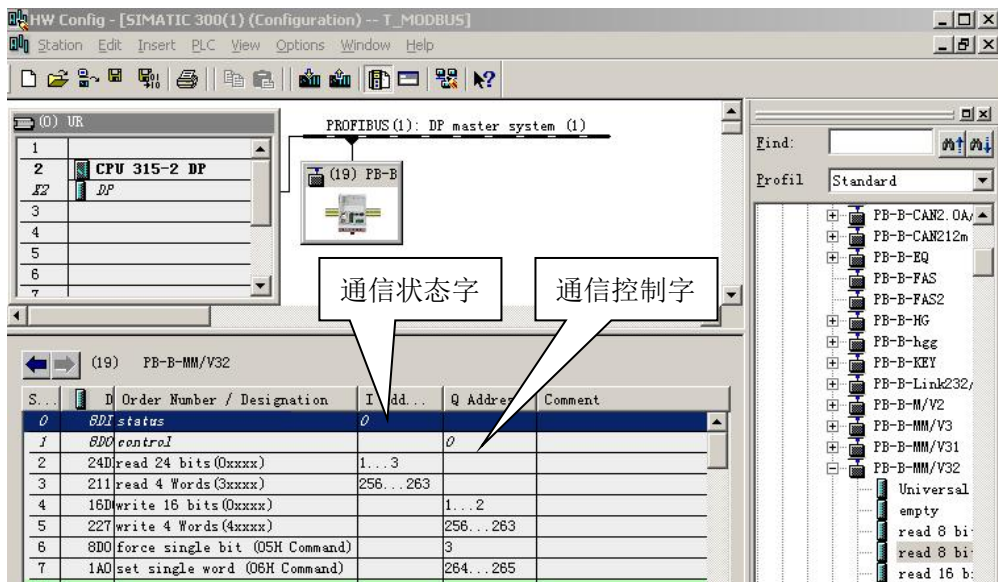


图 5-32

(1) 通信状态字格式

D7: oe_er	D6: CRC_er	D5: Tmdr_O	D4~D1: M_ER_CODE	D0: re_tr
奇偶校验错	CRC 校验错	等待 M 回答到时间	MODBUS 异常应答码	接收/发送

① 接收完毕/发送允许 D0: re_tr

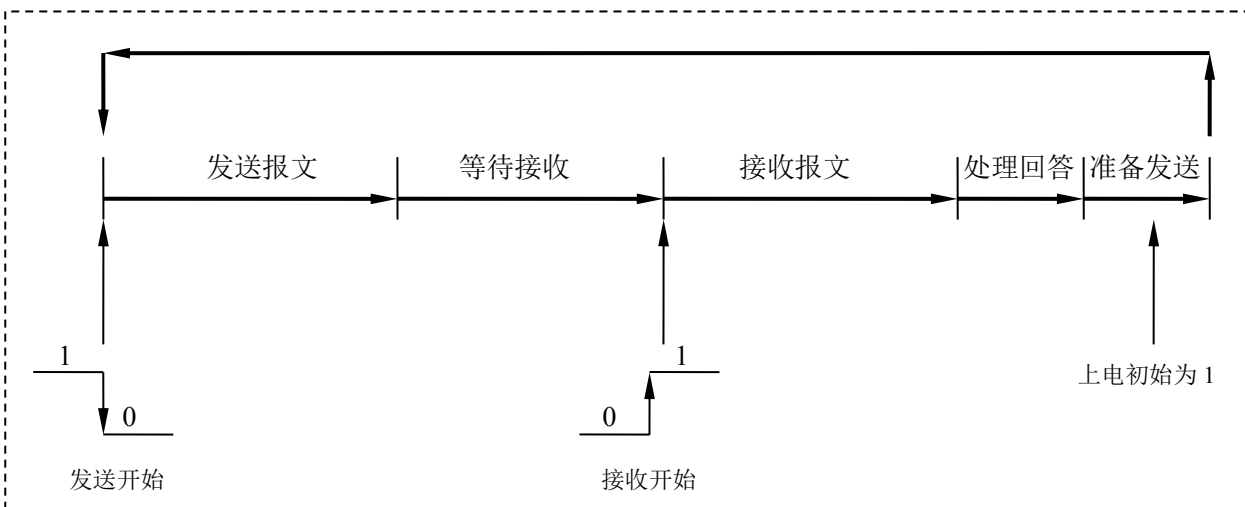


图 5-33 接收/发送 re_tr 标识状态转换图

re_tr=1: 接口正在接收或处理接收报文或准备发送的状态。本手册描述 PB-B-MM/V32 产品，只作 MODBUS 设备的主站。因此，接口上电后自动进入“接收/发送 re_tr=1”状态。

re_tr=0: 接口处在发送报文、等待接收状态。

② MODBUS 异常应答码 M_ER_CODE

MODBUS 异常应答码: 当接口发送一条 MODBUS 报文后，从机接收到的主机报文，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时，从机将以“异常应答”回答之。详见“第三章

MODBUS 技术简介—3. 异常应答”中的介绍。

注意:整个 MODBUS 报文队列最多有 37 条 MODBUS 报文，而只有一个通信状态字。因此，当多条 MODBUS 出现异常应答时，通信状态字中的异常应答码是滚动的。

③ 等待 M 回答到时 Tmdr_O

总线桥发出 MODBUS 报文后，按配置的“等待回答时间 Time of Replay”等待 MODBUS 设备回答，如果等待时间到时，Tmdr_O=1。MODBUS 扫描器转向发送下一条 MODBUS 报文。

④ CRC 校验错 CRC_er

CRC_er=1: 当接口接收到一条 MODBUS 回答报文，CRC 校验出现错误时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 PROFIBUS 对应数据区交换。

⑤ 奇偶校验错 oe_er

串口接收字符中发现字符奇偶校验错。此时，本产品认为 MODBUS 回答数据不可靠，废弃不用，不与 PROFIBUS 对应数据区交换。

(2) 通信控制字格式

D7: reset_M	D6: escape_M	D5: clear_er	D4-D3	D2: M_w_en	D1: M_r_en	D0: start_M
强置 MODBUS 扫描复位	停止等待	清错误标记	不用	MODBUS 写允许	MODBUS 读允许	启动 MODBUS 扫描

① 启动 MODBUS 扫描 D0:start_M

启动 MODBUS 扫描，MODBUS 扫描器从当前 MODBUS 扫描器指针开始，发送对应 MODBUS 报文，详见表 5-2。

② MODBUS 读允许 D1:M_r_en

只发送 MODBUS 报文队列中的读类命令：即 01H、02H、03H、04H 命令，详见表 5-2。

③ MODBUS 写允许 D2:M_w_en

只发送 MODBUS 报文队列中的写类命令：即 05H、06H、0FH、10H 命令，详见表 5-2。

以上三个控制位（start_M、M_r_en、M_w_en）配合使用，主站可以完成“先读（设备状态）→判断→再写（控制设备）等更复杂的功能。

表 5-2 三个控制位（M_w_en、M_r_en、start_M）控制功能

D2: M_w_en MODBUS 写允许	D1: M_r_en MODBUS 读允许	D0: start_M 启动 MODBUS 扫描	功能
×	×	0	停止 MODBUS 扫描
0	0	1	启动 MODBUS 扫描，发送所有 MODBUS 读\写命令
1	1	1	
0	1	1	启动 MODBUS 扫描，只发送 MODBUS 读命令
1	0	1	启动 MODBUS 扫描，只发送 MODBUS 写命令

④ 清错误标记 D5:clear_er

clear_er=1: 总线桥清除通信状态字中错误标记位 D7~D1。

⑤ 停止等待 D6:escape_M

escape_M=1: MODBUS 扫描器发出一条 MODBUS 报文后等待 MODBUS 设备回答。在此状态下, 如果 **escape_M=1**, 扫描器停止等待, 继续扫描下一条 MODBUS 报文。该功能通常配合“等待回答时间 Time of Reply: 无限期等待回答 Waiting…….”的选择使用。

注意 1: 如果 **escape_M** 保持为 1, 那么, 下一条 MODBUS 报文发出后, 没有等待, 立刻转向发送再下一条 MODBUS 报文。因此, **escape_M** 应配合 **start_M** 使用。如下指令系列所示:

```

↓
↓
MODBUS 扫描器处在无限期等待回答中.....
start_M=0;
escape_M=1;
escape_M=0;
start_M=1;
MODBUS 扫描器停止等待, 转向发送下一条 MODBUS 报文.....
↓
↓
    
```

⑥ 强置 MODBUS 扫描复位 D7:reset_M

reset_M=1: 强置 MODBUS 扫描器指针回到第一条 MODBUS 报文位置, MODBUS 扫描器处在复位状态。此时, 启动 MODBUS 扫描 **start_M** 无效。

reset_M=0: “强置 MODBUS 扫描器复位”无效。

注意 2: **reset_M** 与 **escape_M** 同时作用无效。

reset_M	escape_M	功能
0	0	无作用
0	1	停止等待
1	0	强置 MODBUS 扫描复位
1	1	无作用

4. PB-B-MODBUS/V32 工作状态及转换

(1) 工作状态流程图

为正确使用产品, 用户粗略了解一下 PB-B-MODBUS/V32 工作状态流程是有好处的。见下页的图 5-34: PB-B-MODBUS/V32 工作状态流程图。

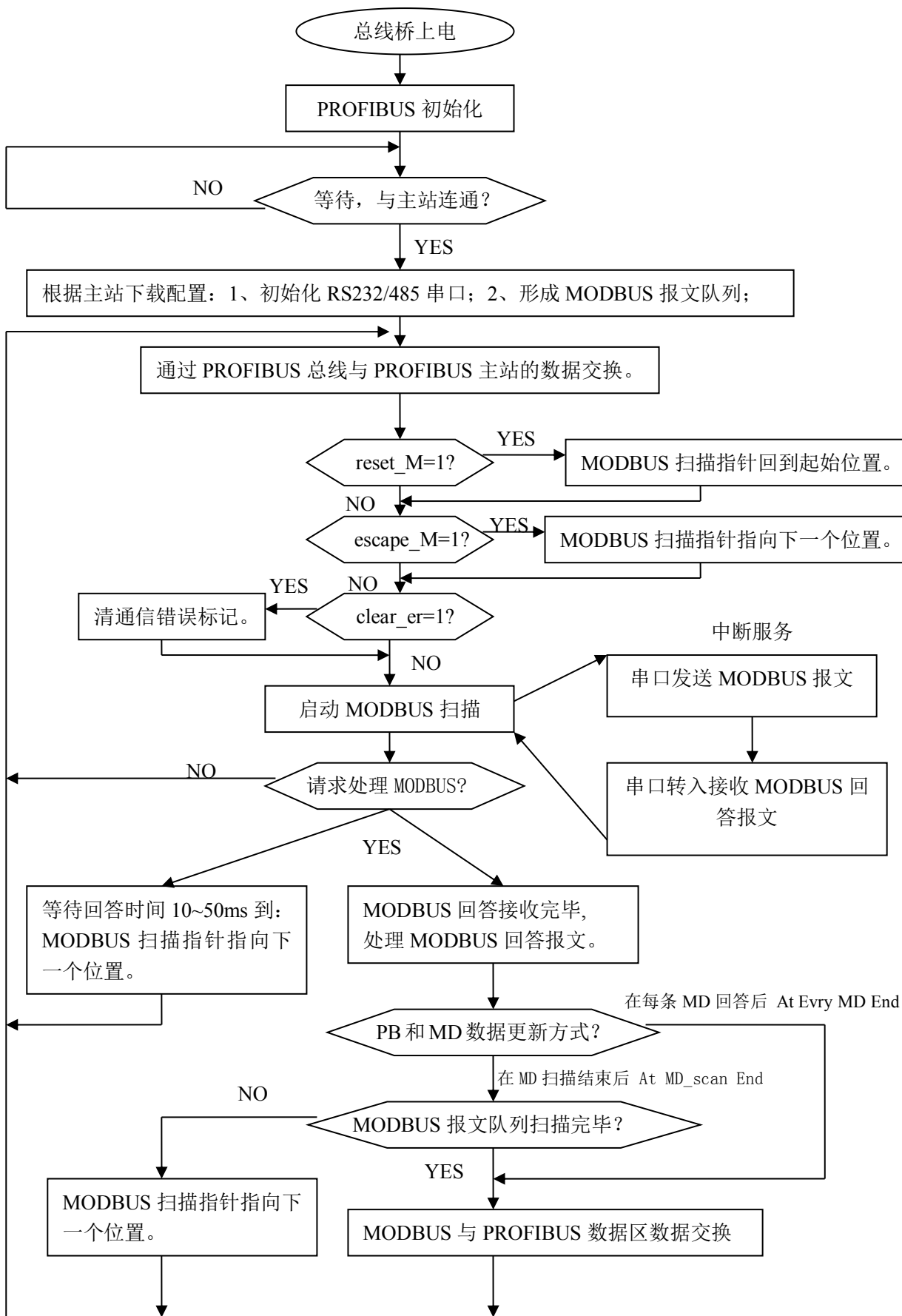


图 5-34 PB-B-MODBUS/V32 工作状态流程图

(2) 上电后 MODBUS 启动

上电后若要启动 MODBUS 扫描，首先要与“主站连通”，然后按“启动方法”启动，见图 5-35。

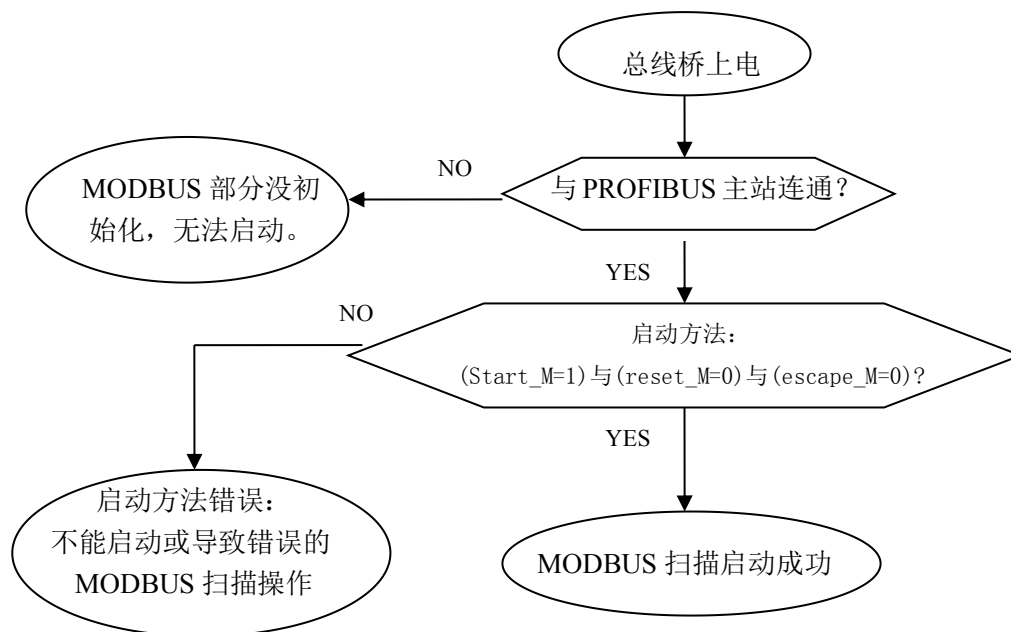


图 5-35 上电后启动 MODBUS 扫描

(3) 几种错误和故障状态及解除方法

① MODBUS 扫描在无限期待回答

I、**产生原因**: 如果在总线桥配置“等待回答时间 Time of Reply”中选择了“无限期待等待 Waiting.....”, 当总线桥 MODBUS 扫描发出一条 MODBUS 报文后, 如果该报文对应的 MODBUS 设备 (由于报文错、设备故障、其它因素等) 没有回答, 则 MODBUS 扫描处在无限期待回答中。

II、**现象**: 通信状态字“接收完毕/发送允许 reok_tren=0”, MODBUS 扫描等待回答。

III、**解除方法**: 用户根据需要选择以下两种解除等待方法。

(i) 使用“停止等待 D6:escape_M”, 使 MODBUS 扫描器停止等待, 转向发送下一条 MODBUS 报文。

↓
↓

MODBUS 扫描器处在无限期待回答中.....

start_M=0;

escape_M=1;

escape_M=0;

start_M=1;

MODBUS 扫描器停止等待, 转向发送下一条 MODBUS 报文.....

↓
↓

(ii) 使用“强置 MODBUS 扫描复位 D7: reset_M”, 使 MODBUS 扫描器停止等待, 扫描指针复位到起始位置, 发送第一条 MODBUS 报文。

↓
↓

MODBUS 扫描器处在无限期等待回答中.....

start_M=0;
 reset_M=1;
 reset_M=0;
 start_M=1;

MODBUS 扫描器停止等待、复位、发送第一条 MODBUS 报文.....



② 由于 D7:reset_M 保持有效使 MODBUS 扫描器反复回到起始位置

I、产生原因：比如使用了下图 5-36 的启动操作：

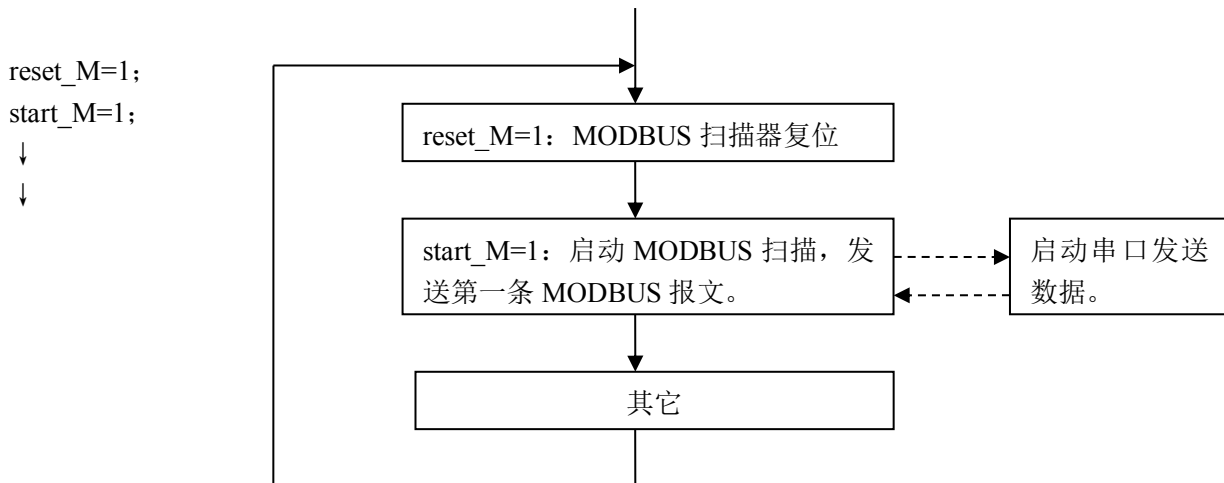


图 5-36

II、现象：串口可能还没有发送完数据，MODBUS 扫描器又复位，重新启动发送第一条 MODBUS 报文。

如此往复下去。

III、解除方法：使用正确的启动方法，启动时(reset_M=0)与(escape_M=0)指令。

③ 由于 D6:escape_M 保持有效使 MODBUS 扫描器没有等待而跳到下一个位置

I、产生原因：比如使用了如图 5-37 的启动操作方式：

escape_M=1;
 start_M=1;
 ↓
 ↓

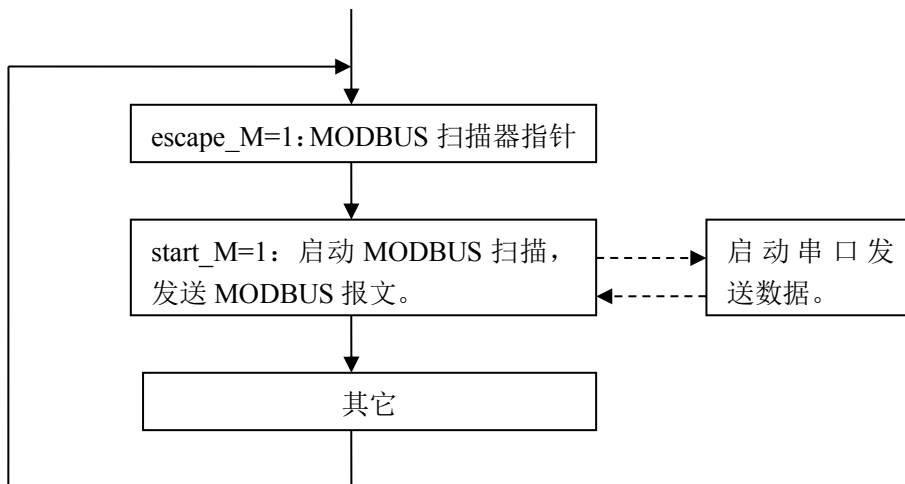


图 5-37

II、**现象：**串口可能还没有发送完数据，MODBUS 扫描器就将指针下移，重新启动发送下一条 MODBUS 报文。如此往复下去。

III、**解除方法：**使用正确的启动方法，启动时(reset_M=0)与(escape_M=0)

④ MODBUS 异常应答

I、**产生原因：**MODBUS 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；

II、**现象：**从机将以“异常应答”回答之。见“第三章 MODBUS 技术简介 3. 异常应答”。通信状态字 D4~D1 是 MODBUS 异常码。

注意：整个 MODBUS 报文队列最多有 37 条 MODBUS 报文，而只有一个通信状态字，因此，当多条 MODBUS 出现异常应答时，通信状态字中的异常应答码是滚动的。

III、**解除方法：**查找异常码含义，排除错误。通常 MODBUS 设备运行状态变化，引起 MODBUS 回答异常。

⑤ 通信奇偶错与 CRC 错误

I、**产生原因：**总线桥接收到的 MODBUS 回答报文有字符奇偶校验错或 CRC 校验错。

II、**现象：**如果总线桥接收到的 MODBUS 回答报文有字符奇偶校验错或 CRC 校验错，总线桥认为此回答报文数据不可靠，拒绝将回答数据写入 MODBUS 读数据区，拒绝对 PROFIBUS 输入数据更新，视为此次通信无效，继续扫描下一条 MODBUS 报文。同时将通信状态字奇偶校验错 D7: oe_er 置 1 或将 CRC 效验错 D6: CRC_er 置 1。

III、**解除方法：**字符奇偶校验错或 CRC 校验错不影响 MODBUS 扫描进行，但错误标志将保留。可以使用控制字“清错误标记” clear_er=1 将错误标记清除。clear_er=1 不影响 MODBUS 扫描器。clear_er 保持为 1，将保持清除错误标记功能有效。

5. 如何在主站中启动读/写 MODBUS 通信数据

主站中编程必须以硬件配置中的 I/O 地址为依据。为了方便起见，我们将本章“产品配置与通信方法实例”的硬件配置拷贝至此，见图 5-1: 产品配置与通信方法的实例、表 5-3: 全部举例的地址对照汇总表、图 5-38: PB-B-MM/V32 中各 MODBUS 模块的 PROFIBUS I/O 地址、图 5-39: S7-300 PLC 中 8DI、8DO 的 I/O 地址。

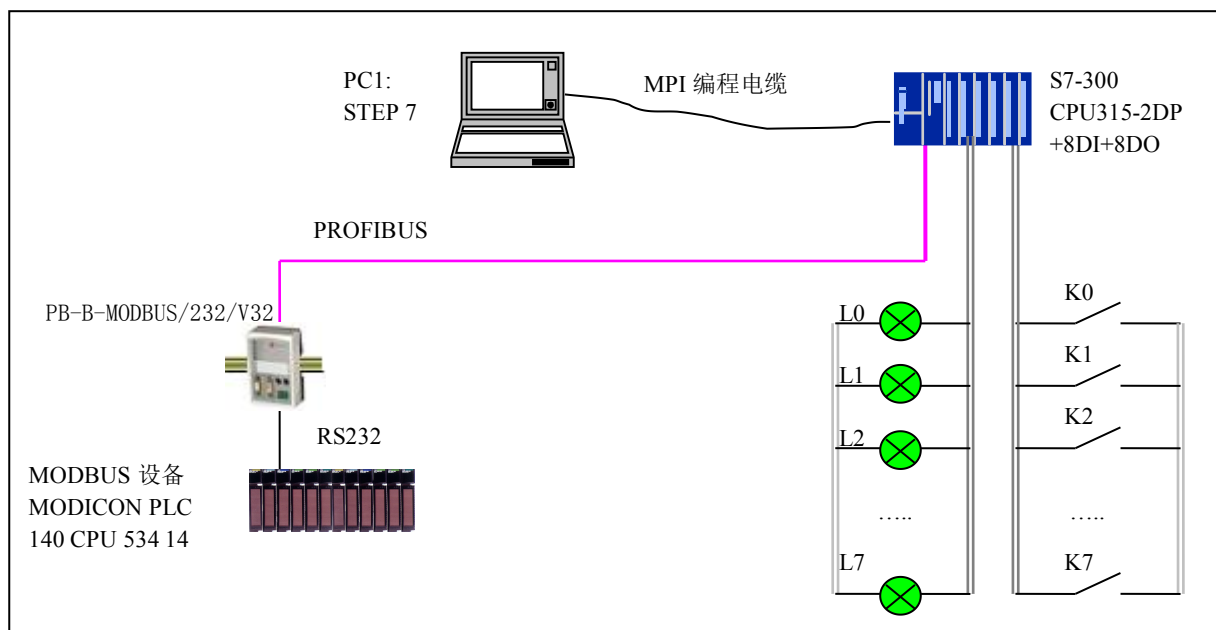


图 5-1 产品配置与通信方法的实例

S...	D	Order Number / Designation	I Add...	Q Address	Comment
0	8DI	status	0		
1	8DO	control		0	
2	24D	read 24 bits (0xxxx)	1...3		
3	21I	read 4 Words (3xxxx)	256...263		
4	16D	write 16 bits (0xxxx)		1...2	
5	22I	write 4 Words (4xxxx)		256...263	
6	8DO	force single bit (05H Command)		3	
7	1A0	set single word (06H Command)		264...265	
8	22I	read 40 Words (4xxxx)	264...295		
9	22I	--> read 40 Words (4xxxx)	296...327		
10	21I	--> read 40 Words (4xxxx)	328...343		

图 5-38 PB-B-MM/V32 中各 MODBUS 模块的 PROFIBUS I/O 地址

表 5-3 全部举例的地址对照汇总表

槽号	模块名称	PROFIBUS 地址	MODBUS 配置	MODBUS 命令
2#	read 24 bits (0xxxx)	输入 IB1~IB3 8bytes=24 bits	站号: 10 起始地址: 0	发 01H 命令读线圈 00001~00024, 存入 IB1~IB3。
3#	read 4 Words (3xxxx)	IW256~IW262: 4 Words 输入	站号: 10 起始地址: 0	发 04H 命令读模拟量输入 30001~30004, 存入 IW256~IW262。
4#	write 16 bits (0xxxx)	QB1~QB2: 2×8=16 bits 输出	站号: 10 起始地址: 0	发 0FH 命令, 将 QB1~QB2 写入线圈 00001~00016。
5#	Write 4 Words (4xxxx)	QW256~QW262: 4 Words 输出	站号: 10 起始地址: 0	发 10H 命令, 将 QW256~QW262 写入保持寄存器 40001~40004
6#	force single bit (05H Command)	QB3: 1 Byte 输出	站号: 10 起始地址: 23	发 05H 命令, 根据 Q3 置线圈 00024
7#	set single word (06H Command)	QW264: 1 Word 输出	站号: 10 起始地址: 39	发 06H 命令, 将 QW264 置入保持寄存器 40040
8#~10#	Read 40 Words (4xxxx)	IW264~IW342: 40 Words 输入	站号: 10 起始地址: 0	发 03H 命令读保持寄存器 40001~40040, 存入 IW264~IW342。

S...	Module	Order number	MPI address	I add...	Q address	Comment
1						
2	CPU 315-2 DP	6ES7 315-2AF03-0AB0	2			
2.2	DP Master			1023*		
3						
4	DI8/DO8x24V/0.5A	6ES7 323-1BH00-0AA0		4	4	
5						

图 5-39 S7-300 PLC 中 8DI、8DO 的 I/O 地址

(1) 设备与地址对应关系

表 5-4 设备与地址对应关系表

按钮	I/O 地址	指示灯	I/O 地址
K0	I4.0	L0	Q4.0
K1	I4.1	L1	Q4.1
K2	I4.2	L2	Q4.2
K3	I4.3	L3	Q4.3
K4	I4.4	L4	Q4.4
K5	I4.5	L5	Q4.5
K6	I4.6	L6	Q4.6
K7	I4.7	L7	Q4.7

(2) 通信状态字及通信控制字 PROFIBUS 对应关系

表 5-4 通信状态字及通信控制字与 PROFIBUS 地址对应关系表

PB-B-MM/V32 通信状态字	PROFIBUS 地址	PB-B-MM/V32 通信控制字	I/O 地址
D0: 接收/发送 re_tr	I0.0	D0:启动 MODBUS 扫描 start_M	Q0.0
D4-D1:异常应答码 M_ER_CODE	I0.1~I0.4	D5:清错误标记 clear_er	Q0.5
D6:CRC 效验错 CRC_er	I0.6	D6:停止等待 escape_M	Q0.6
D7:奇偶校验错 oe_er	I0.7	D7:强置 MODBUS 扫描复位 reset_M	Q0.7

(3) 如何获取通信状态字

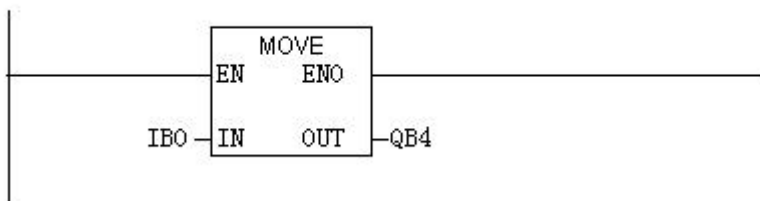
见梯形图中的 Network 1，启动 MODBUS 扫描后，可以看到 L0=Q4.0=I0.0=接收/发送 re_tr 在闪动。

OB1 : “Main Program Sweep (Cycle)”

这是为说明应用PB-B-MM/V32做MODBUS主站通信而编写的例程，包括了：MODBUS 启动、复位和读/写MODBUS数据功能。

Network 1: Title:

I0.0是PB-B-MM/V32的通信状态字，QB4是指示灯L0~L7，本指令是将总线桥通信状态字送到指示灯L0~L7显示。启动MODBUS扫描后，可以看到Q4.0=I0.0=接收/发送re_tr在闪动。



(4) 如何在主站中实现 MODBUS 启动、复位、停止等待、清除错误标志等

从梯形图 Network 2~5 看出：

按钮 K7 可实现强置 MODBUS 扫描复位 reset_M；

按钮 K6 可实现对停止等待 escape_M；

按钮 K5 可实现清错误标记 clear_er；

按钮 K0 可实现 MODBUS 扫描启动 start_M

至于启动、复位、停止等待、清除的方法和注意事项叙述，见“4. PB-B-MODBUS/V32 工作状态及转换(3) 几种错误和故障状态及解除方法。”

Network 2: Title:

I4.7=按钮K7, Q0.7=强置MODBUS扫描复位reset_M. 本指令功能是使用K7对总线桥MODBUS通信复位。



Network 3: Title:

I4.6=按钮K6, Q0.6=停止等待 escape_M. 本指令功能是使用K6令MODBUS扫描跳出等待回答, 转入下一条MODBUS报文发送。



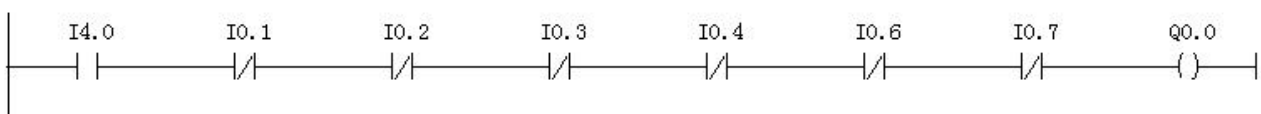
Network 4: Title:

I4.5=按钮K5, Q0.5=清错误标记clear_er. 本指令功能是使用K5清除通信状态字中的错误标记 I0.1~I0.7.



Network 5: Title:

I4.0=按钮K0, Q0.0=启动MODBUS扫描start_M, 启动条件是：清除通信状态字中的错误标记 I0.1~I0.7均为0.

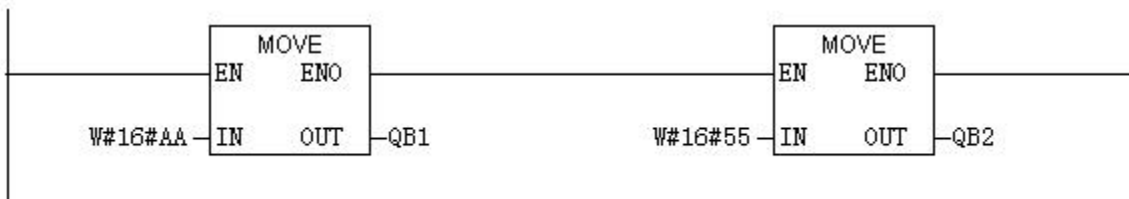


(5) 如何在主站中将数据写入 MODBUS 数据区 0XXXX、4XXXX

- ① 给 QB1~QB2 置值, 4#槽 MODBUS 的 0FH 命令将 QB1~QB2 写到 MODBUS 线圈 00001~00016。

Network 6: Title:

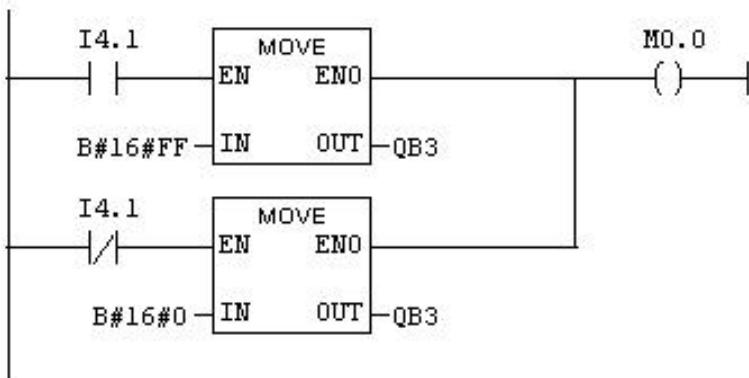
本指令与4#槽命令OFH功能有关，4#槽MODBUS命令是将Q1~Q2=16bits写入MODBUS线圈00001~00016。本指令是对Q1~Q2置值AA55H。



② 利用 K1 给 QB3 置 00/FF， 6#槽 MODBUS 05H 命令，根据 QB3=00/FF，将线圈 00024 置 0 或置 1。

Network 7: Title:

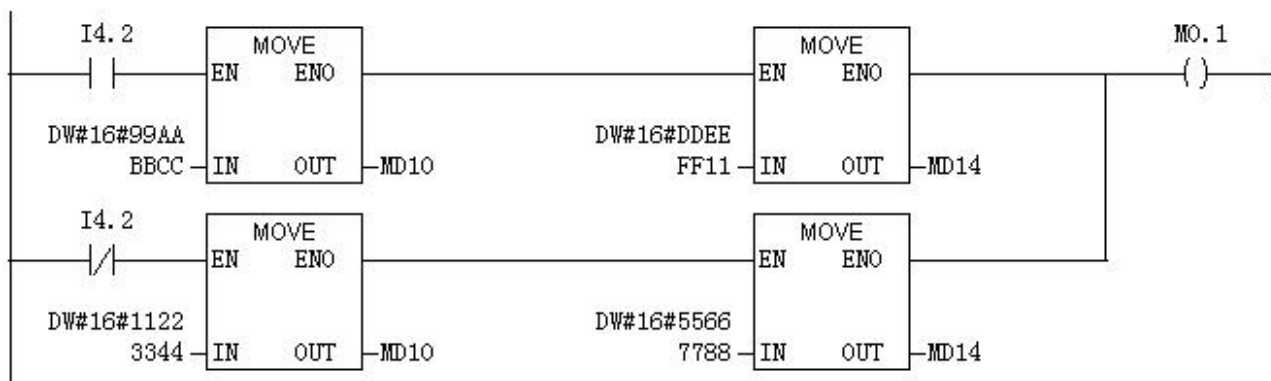
I4.1=按钮K1,用来选择置QB3=00/FF。本指令与6#槽MODBUS命令05H功能有关，6#槽MODBUS命令是：若QB3=0，将线圈00024（配置中起始地址=00023）置0；若QB3=FF，将线圈00024置1。



③ 利用 K2 给 MW10~MW16 置值,应用 SFC15 将 MW10~MW16 传送到 QW256~QW262;5#槽 MODBUS 10H 命令将 QB256~QB263 写到 MODBUS 保持寄存器 40001~40004。

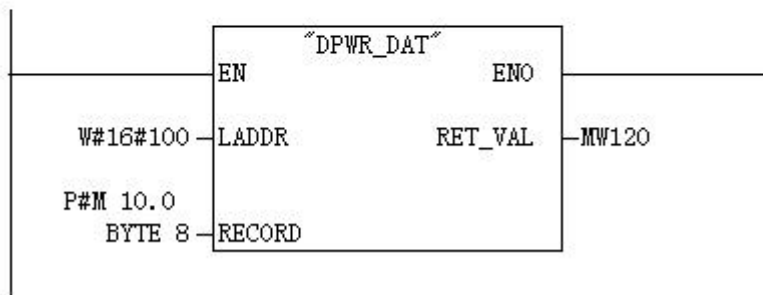
Network 8: Title:

I4.2=按钮K2,用来选择置MW10~MW16(共4 WORDS)为:99AA、BBCC、DDEE、FF11或者说1122、3344、5566、7788，本指令为下一级指令准备。



Network 9 : Title:

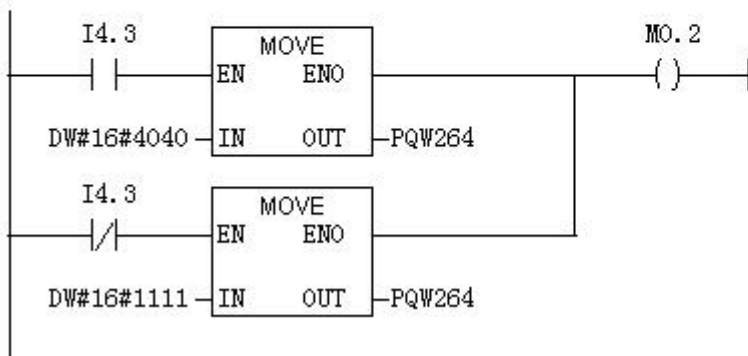
本指令与5#槽MODBUS命令10H功能有关，5#槽MODBUS命令是将QW256~QW262(4 WORDS)写入MODBUS保持寄存器40001~40004；本指令应用SFC15将MW10为首地址 (P#M10.0 BYTE 8)共8 BYTES写入QW256(W#16#100)，MW10~MW16的数据在上一级置入。



④ 利用 K3 给 QW264 置值；7#槽 MODBUS 06H 命令将 QW264 写到 MODBUS 保持寄存器 40040。

Network 10 : Title:

I4.3=按钮K3，用来选择置QW264 (1 WORDS) 为4040或1111，本指令与7#槽MODBUS命令06H功能有关，7#槽MODBUS命令是将QW264的数据写入MODBUS保持寄存器40040。(MODBUS起始地址配置为：00039)



(6) 如何在主站得到 MODBUS 数据区 0XXXX、1XXXX、3XXXX、4XXXX 数据

① 在 PC1 在线监测可以看到 IB1~IB3 的数据，如下图 5-39:

	Address	Symbol	Display fo	Status value	Modify value
1	IB 1		HEX	B#16#AA	
2	IB 2		HEX	B#16#55	
3	IB 3		HEX	B#16#00	

图 5-39

数据 AA55 是 Network 6 置入 QB1~QB2 的值，由 4#槽 MODBUS 0FH 命令将 QB1~QB2 写到 MODBUS 线圈 00001~00016。而 2#槽 MODBUS 01H 命令读 MODBUS 线圈 00001~00024，对应送到 IB1~IB3，故 PC1 在线监测可以看到 IB1~IB2 的数据 AA、55。

另外，6#槽 MODBUS 命令 05H 功能是：若 QB3=0，将线圈 00024（配置中起始地址=00023）置 0；若 QB3=FF，将线圈 00024 置 1。Network 7 利用按钮 K1 选择置 QB3=00/FF。因此，按动 K1 可观察到 I3.7=线圈 00024 的变化，如下图 5-40:

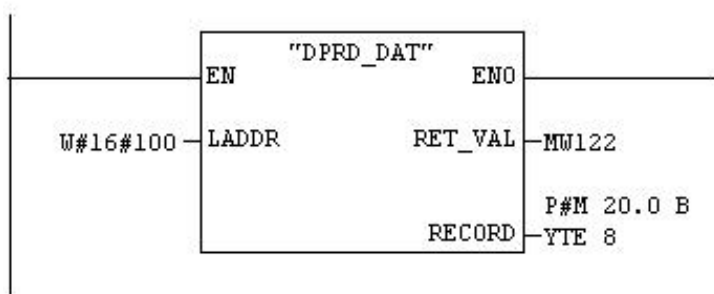
	Address	Symbol	Display fo	Status value	Modify value
1	IB 1		HEX	B#16#AA	
2	IB 2		HEX	B#16#55	
3	IB 3		HEX	B#16#80	

图 5-40

② 应用 SFC14 将 IW256~IW262 传送到 MW20~MW26；IW256~IW262 中的数据是 3#槽 MODBUS 的 04H 命令从 MODBUS 输入寄存器 30001~30004 读到的。在 PC1 上在线监测可以看到 MW20~MW26 数据。

Network 11 : Title:

本指令与3#槽MODBUS命令04H功能有关，3#槽MODBUS命令是将MODBUS输入寄存器30001~30004读到IW256~IW262（4 WOEDS）。本指令应用SFC14将IW256（W#16#100）为首地址共8 BYTES传送到MW20~MW26（P#M20.0BYTE8）



在 PC1 在线监测可以看到 MW20~MW26 数据：1234、5678、9ABC、DEF1；这组数据来自 MODBUS 30001~30004，由 MODBUS 主站置入，如图 5-41：

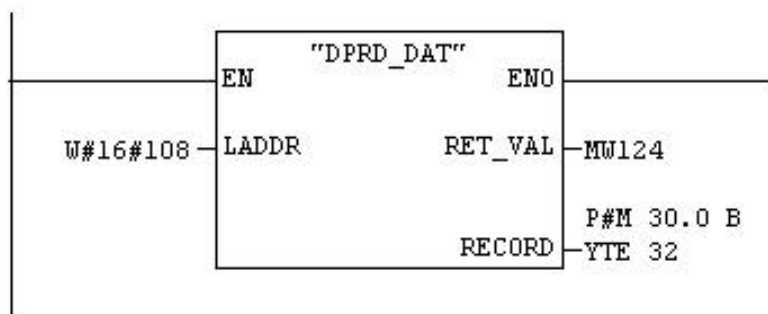
4	MW 20	HEX	W#16#1234
5	MW 22	HEX	W#16#5678
6	MW 24	HEX	W#16#9ABC
7	MW 26	HEX	W#16#DEF1

图 5-41

③ 8#槽 MODBUS 命令 03H 功能读取 MODBUS 保持寄存器 40001~40040 存到 IW264~IW342（40 WOEDS）。本指令应用 SFC14，仅将 IW264~IW294（16 Words）传送到 MW30~MW60

Network 12 : Title:

本指令与8#槽MODBUS命令03H功能有关，8#槽MODBUS命令是将MODBUS保持寄存器40001~40040读到IW264~IW342（40 WOEDS）。本指令应用SFC14，仅将IW264（W#16#108）为首地址共16 WORDS（32 BYTES）传送到MW30~MW60（P#M30.0BYTE32）；其它40-16=24 WORDS 在Network 13~14中传送。



回顾一下 Network 8~9，利用 K2、 SFC15 及 5#槽 MODBUS 10H 命令将 99AA、 BBCC、 DDEE、 FF11 或 1122、 3344、 5566、 7788 写到 MODBUS 保持寄存器 40001~40004。所以在 PC1 在线监测可以看到 MW30~MW36（对应 40001~40004）的数据。

PC1 在线监测 MW30~MW36（MW30~MW36←←IW264~IW270←←40001~40004←MW10~MW16）的数据，图 5-42:

8	MW	30	HEX	W#16#1122
9	MW	32	HEX	W#16#3344
10	MW	34	HEX	W#16#5566
11	MW	36	HEX	W#16#7788
12	MW	38	HEX	W#16#0000
13	MW	40	HEX	W#16#0000

图 5-42

按 K2，可以看到数据变化，图 5-43:

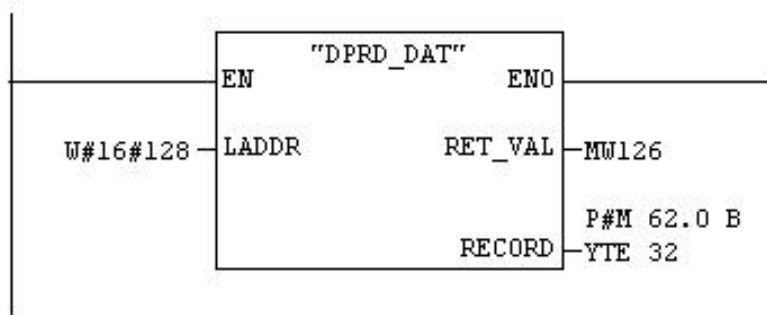
8	MW	30	HEX	W#16#99AA
9	MW	32	HEX	W#16#BBCC
10	MW	34	HEX	W#16#DDEE
11	MW	36	HEX	W#16#FF11
12	MW	38	HEX	W#16#0000
13	MW	40	HEX	W#16#0000

图 5-43

- ④ Network 13 接续 Network 12，应用 SFC14，仅将 IW296~IW326（16 Words）传送到 MW62~MW92；
- Network 14 接续 Network 13，应用 SFC14，仅将 IW328~IW342（8 Words）传送到 MW94~MW108；

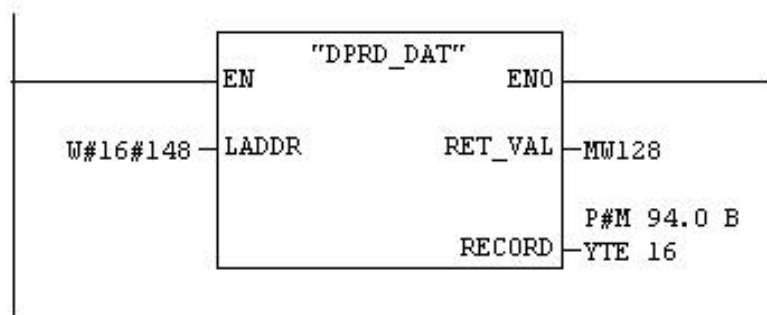
Network 13 : Title:

本指令接续 Network 12，应用 SFC14，仅将 IW296（W#16#128）为首地址共 16 WORDS（32 BYTES）传送到 MW62~MW92（P#M62.0BYTE32）；其它 40-32=8 WORDS 在 Network 14 中传送。



Network 14 : Title:

本指令接续 Network 13，应用 SFC14，仅将 IW328（W#16#148）为首地址共 8 WORDS（16 BYTES）传送到 MW94~MW108（P#M94.0BYTE16）。



注意：PC1 在线监测的 MW108（对应 40040）数据： Network 10 利用 K3 给 QW264 置值 1111/4040；7# 槽 MODBUS 06H 命令将 QW264 写到 MODBUS 保持寄存器 40040。因此 PC1 在线监测的 MW108（对应 40040）数据是 1111，见下图 5-44：

44	MW 102	HEX	W#16#0000
45	MW 104	HEX	W#16#0000
46	MW 106	HEX	W#16#0000
47	MW 108	HEX	W#16#1111

图 5-44

按动 K3 变化为 4040；见下图 5-45：

44	MW 102	HEX	W#16#0000
45	MW 104	HEX	W#16#0000
46	MW 106	HEX	W#16#0000
47	MW 108	HEX	W#16#4040

图 5-45

6. 从站状态检测

(1) “MODBUS 从站状态监测” 功能

当总线桥做 MODBUS 主站，带有多个 MODBUS 从站时，PB-B-MM/V33 可以使 PROFIBUS 主站监测到 MODBUS 从站的通信状态，见图：附录 5-46。从站站地址分别设为 02H、0CH、04H、0FH、10H。

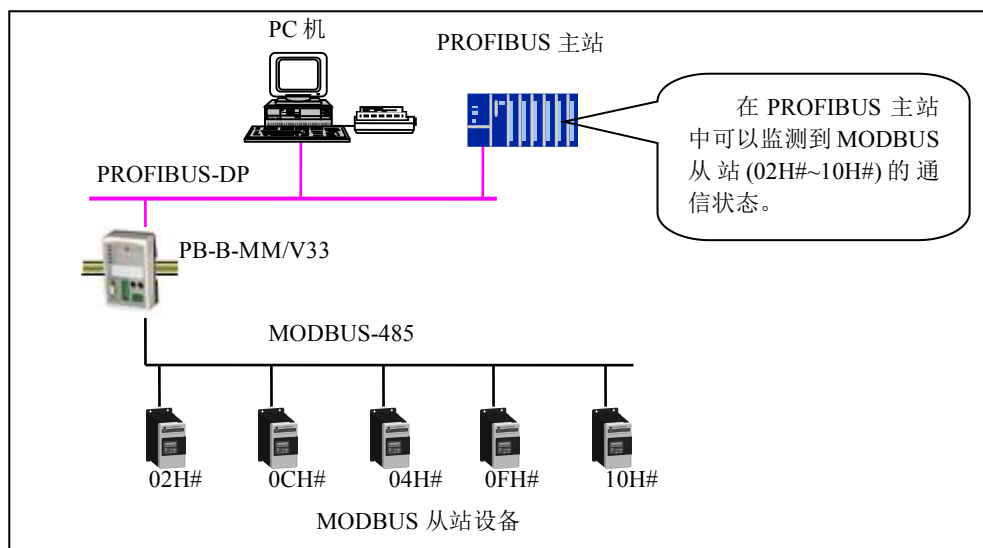


图 5-46 PB-B-MM/V33 可以使 PROFIBUS 主站监测到 MODBUS 从站（02H#~10H#）的通信状

(2) 举例说明 1：MODBUS 从站通信状态（位）监测

在本例配置中 PB-B-MM/V33 有 5 个 MODBUS 从站(02H#、0CH#、04H#、0FH#、10H#)；在 PROFIBUS 主站中可对 MODBUS 从站通信状态（位）进行监测。

第一步：选择“有从站状态监测（8 位）”，见图 5-47。缺省时为：“无从站状态检测”。

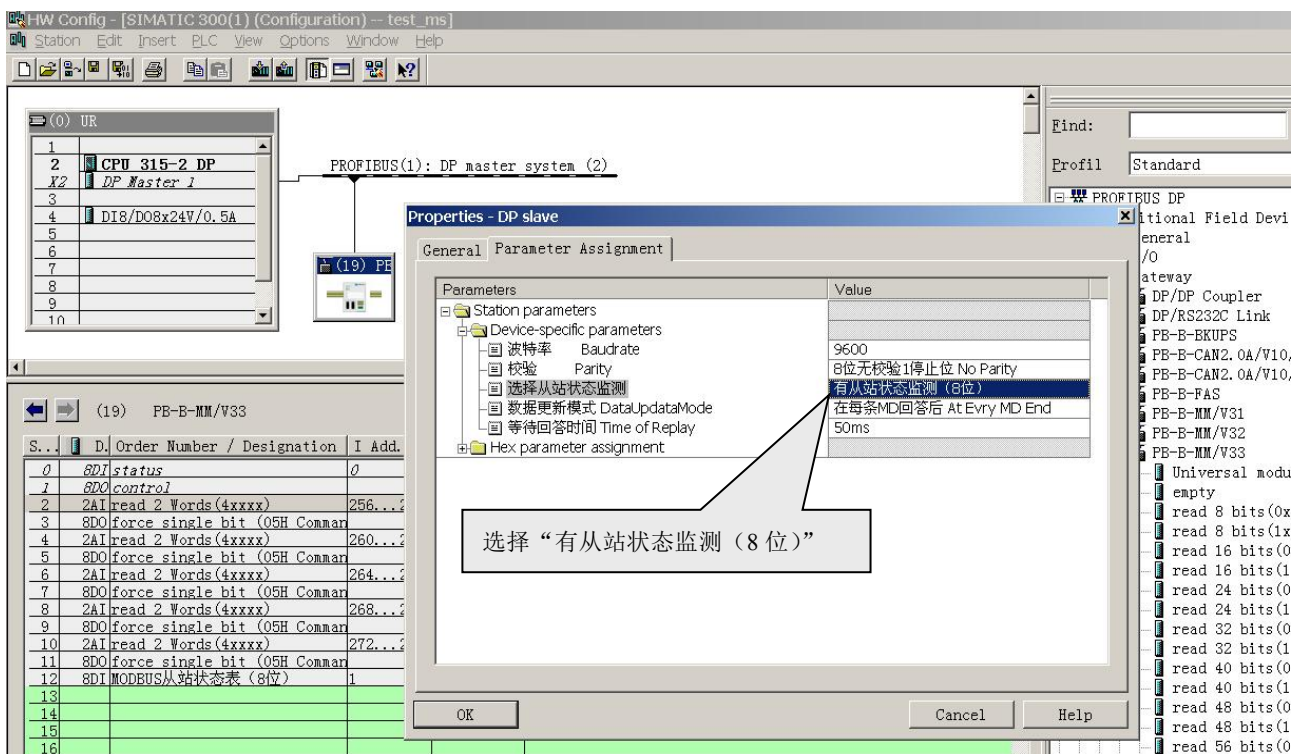


图 5-47 选择“从站状态监测 (8 位)”

第二步：配置 MODBUS 报文。 每个从站配置两条报文：读两个字 read 2 Words(4xxxx)并有一个置位 force single bit(05h Command)，注意：每条报文都要设置 MODBUS 从站地址。如下图 5-48 所示。

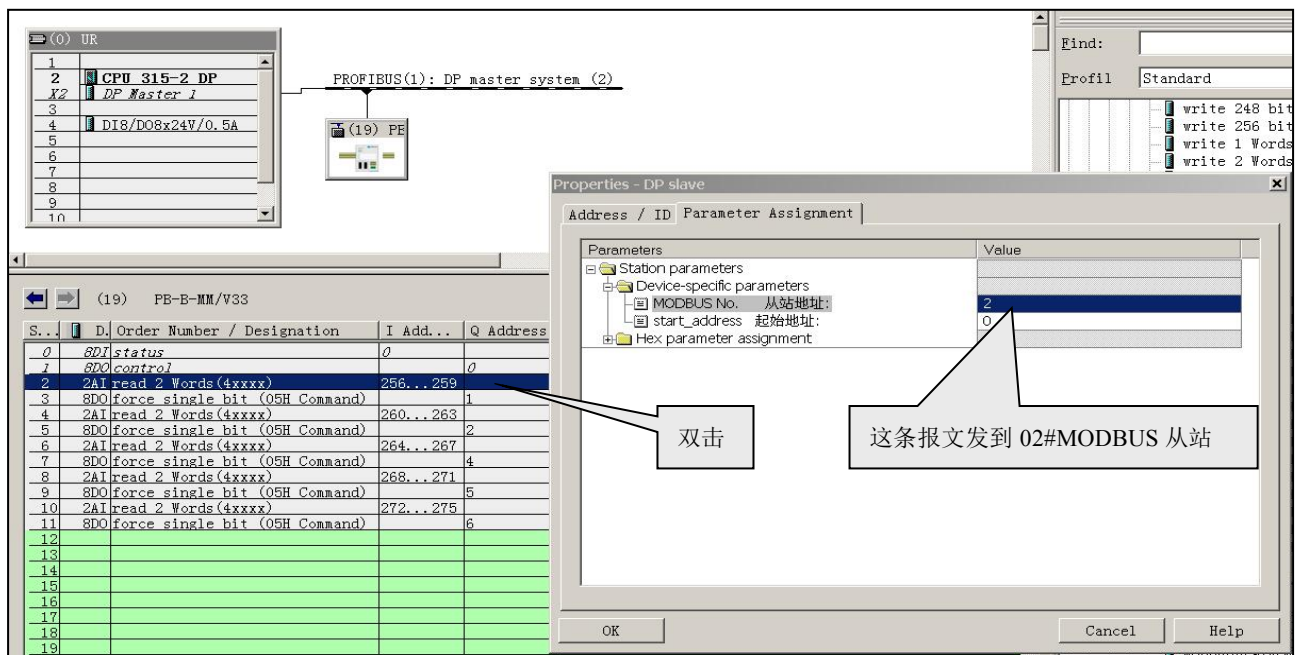


图 5-48 每个从站配置两条报文

第三步：插入“MODBUS 从站状态表 (8 位)”，见图 5-49。键入 MODBUS 从站地址表：02、0C、04、0F、10，其他可随意设置。

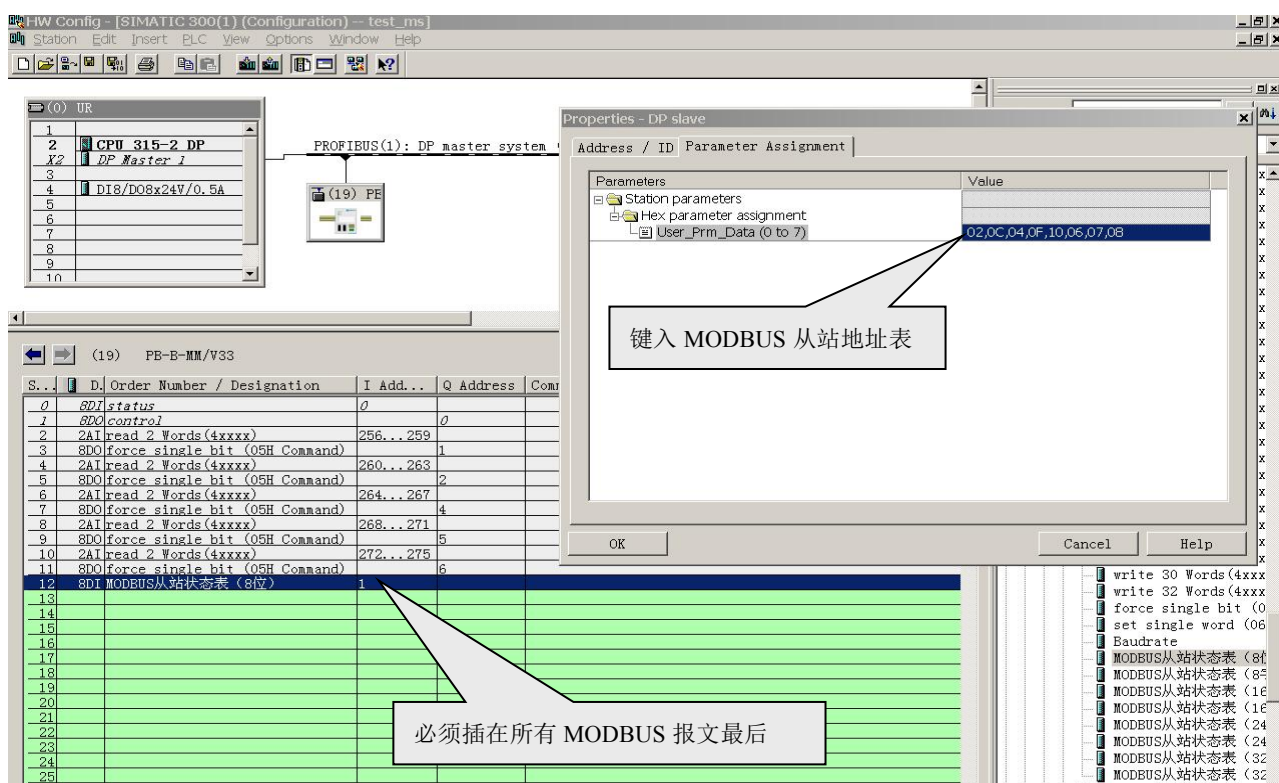


图 5-49 插入“MODBUS 从站状态表 (8 位)”键入 MODBUS 从站地址表：02、0C、04、0F、10

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

第四步：程序运行后，可在 PROFIBUS 地址 IB1 中见到 MODBUS 从站 02、0C、04、0F、10 的通信状态的显示：

IB1:

D7	D6	D5	D4	D3	D2	D1	D0
不用	不用	不用	10H 站通信状态	0FH 站通信状态	04H 站通信状态	0CH 站通信状态	02H 站通信状态

其中 D0 = 02H 站通信状态：

D0=0: MODBUS 主站 (PB-B-MM/V33) 向 02H 从站发送报文，超过 Tsdr 时间之后没有收到从站回答或 02H 从站根本没有接到可使其回答的 MODBUS 主站报文。其中“Tsdr 时间”见本手册“第五章---2.、系统配置方法---- (三)、(4) 配置等待回答时间 Time of Reply”。

D0=1: 02H 站在接收到 MODBUS 主站 (PB-B-MM/V33) 报文后在 Tsdr 时间之内作出了回答，并且 MODBUS 主站 (PB-B-MM/V33) 接收到的回答报文正确。

D1-D4: 与上面 D0 作用相同。

(3) 举例说明 2: MODBUS 从站通信状态 (字节) 监测

在例 2 中有 5 个 MODBUS 从站 (02H#、0CH#、04H#、0FH#、10H#), 在 PROFIBUS 主站中进行 MODBUS 从站通信状态 (字节) 的监测。

第一步：选择“有从站状态监测 (字节)”，见图 5-50。缺省时为：“无从站状态检测”。

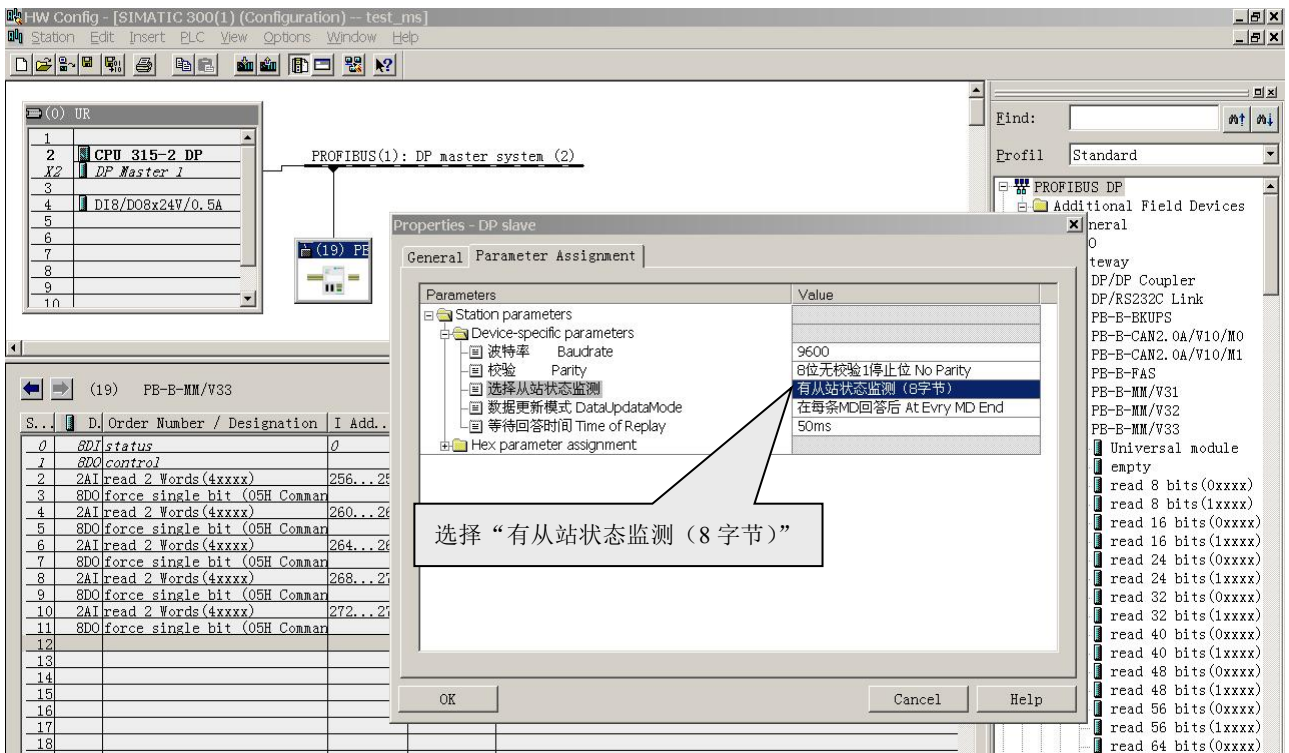


图 5-50 选择“从站状态监测（8字节）”

第二步：配置 MODBUS 报文。每个从站配置两条报文：读两个字 read 2 Words(4xxxx)并有一个置位 force single bit(05h Command)。

注意：每条报文都要设置 MODBUS 从站地址。如下图 5-51。

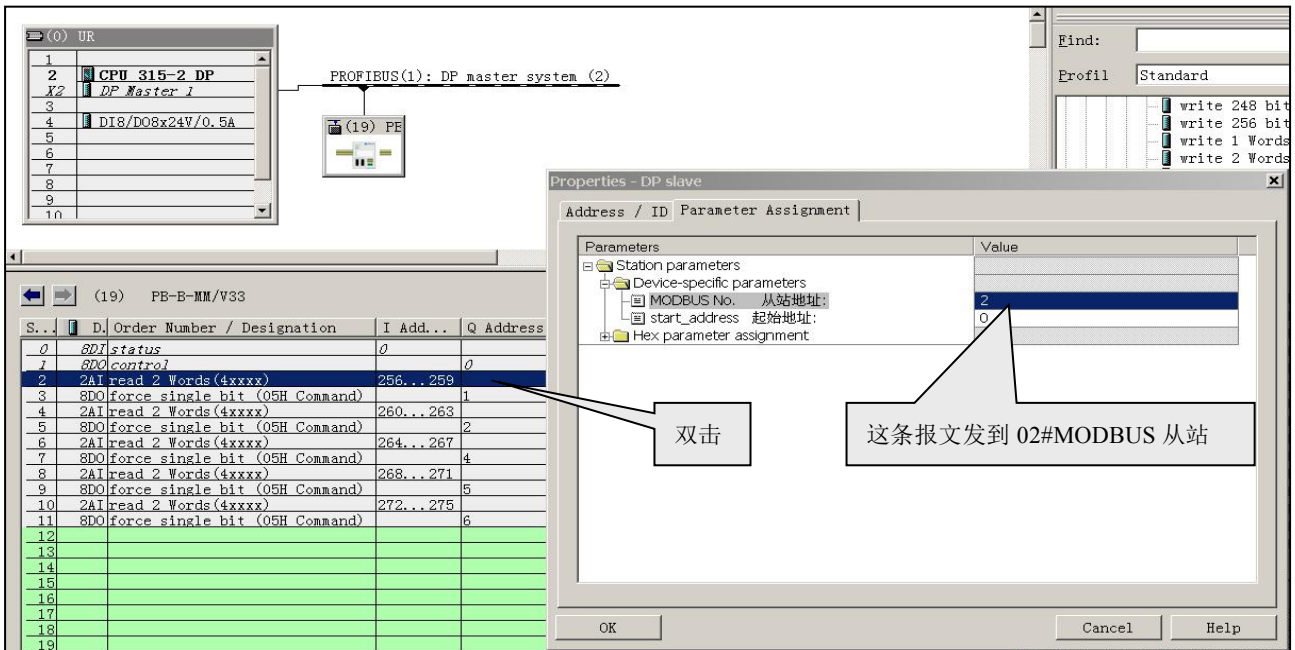


图 5-51 每个从站配置两条报文

第三步：插入“MODBUS 从站状态表（8 字节）”，见图 5-52。键入 MODBUS 从站地址表：02、0C、04、0F、10，其它可以任意设置。

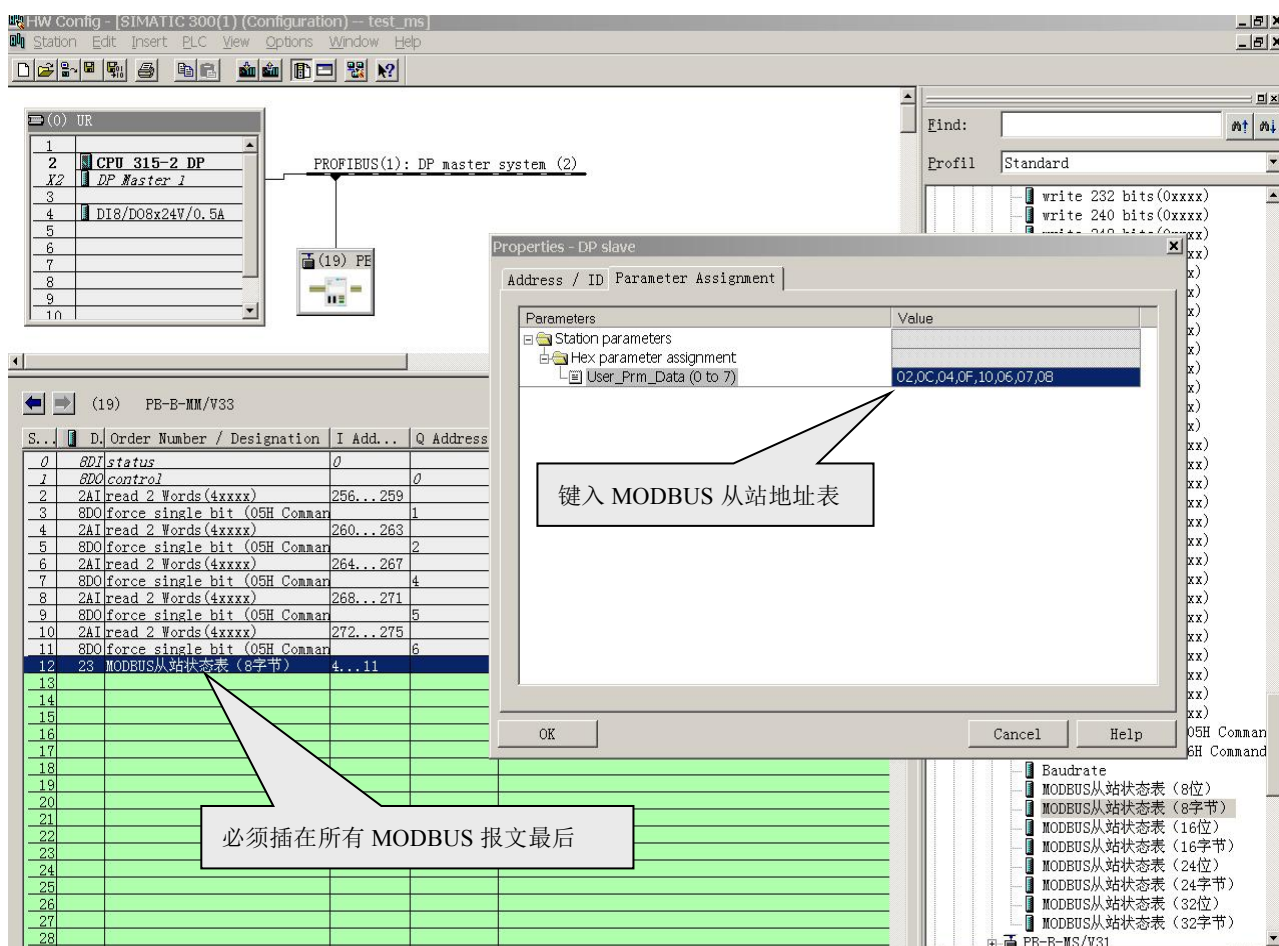


图 5-52 插入“MODBUS 从站状态表 (8 位)”键入 MODBUS 从站地址表：02、0C、04、0F、10

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

第四步：运行程序后，在 PROFIBUS 主站地址 IB4~IB8 中，可显示对应 MODBUS 从站号 02、0C、04、0F、10 的通信状态字节。

IB4：对应 02H 号 MODBUS 从站的状态字节；

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	MM 等待回答超时

其中：

① D0: Tmdr_0 = MM 等待回答超时：

D0=0：MODBUS 主站 (PB-B-MM/V33) 向 02H 号从站发送报文，超过 Tsdr 时间之后没有收到回答或 02H 从站根本没有接到可使其回答的 MODBUS 主站报文。其中“Tsdr 时间”见本手册“第五章 ---2.、系统配置配方法--- (三) 配置 PB-B-MM/V32 作为 PROFIBUS 从站--- (4) 配置等待回答时间 Time of Reply”。

D0=1：02H 号从站接收到 MODBUS 主站 (PB-B-MM/V33) 报文后在 Tsdr 时间之内作出了回答，并且 MODBUS 主站 (PB-B-MM/V33) 接收到的回答报文是正确的。

② D4~D1: M_ER_CODE= MODBUS 异常应答码:

当 MODBUS 主站 (PB-B-MM/V33) 发送一条 MODBUS 报文后, 02H 号从站接收到的主站报文, 没有传输错误; 但从站无法正确执行主站命令或无法作出正确应答; 从站将以“异常应答”回答之。详见“第三章 MODBUS 技术简介-3. 异常应答”。

③ D6: CRC_er =CRC 效验错

CRC_er=1: MODBUS 主站 (PB-B-MM/V33) 接收到一条 MODBUS 回答报文时 CRC 校验错误, 此时, MODBUS 主站 (PB-B-MM/V33) 认为 MODBUS 回答数据不可靠、废弃不用, 不与 PROFIBUS 对应数据区交换。

④ D7: 奇偶校验错 oe_er

MODBUS 主站 (PB-B-MM/V33) 接收字符中发现字符奇偶校验错。此时, MODBUS 主站 (PB-B-MM/V33) 认为 MODBUS 回答数据不可靠、废弃不用, 不与 PROFIBUS 对应数据区交换。

其它 MODBUS 状态字节:

IB5: 对应 0CH 号 MODBUS 从站的状态字节;

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB6: 对应 04H 号 MODBUS 从站的状态字节;

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB7: 对应 0FH 号 MODBUS 从站的状态字节;

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

IB8: 对应 10H 号 MODBUS 从站的状态字节;

D7: oe_er	D6: CRC_er	D5	D4~D1: M_ER_CODE	D0: Tmdr_O
奇偶校验错	CRC 效验错	不用	MODBUS 异常应答码	等待回答到时

(4) 几种特例

(1) 如果在 MODBUS 报文配置中配置了 02H 号从站的报文, 见图 3 或图 6, 而在键入 MODBUS 从站地址表中 (见图 4 或图 7) 没有键入 02H 地址; 当 MODBUS 主站 (PB-B-MM/V33) 发出 02H 从站报文后, 如果接收 (或没有接收) 到回答, 但 MODBUS 主站 (PB-B-MM/V33) 在从站地址表中找不到 02H, 此时, MODBUS 主站 (PB-B-MM/V33) 将**总状态字 (IB0)** 中 D4~D1 “MODBUS 异常码” 置 F, 不对“有从站状态检测 (位)” 或“有从站状态检测 (字节)” 进行任何操作。

总状态字 IB0

D7: oe_er	D6: CRC_er	D5: Tmdr_O	D4~D1: MODBUS 异常应答码	D0: re_tr
奇偶校验错	CRC 校验错	等待 M 回答到时	1111	接收/发送

(2) 如果 MODBUS 主站 (PB-B-MM/V33) 接收到一个带有异常应答码的 MODBUS 回答报文，正常情况是：在 MODBUS 从站地址表中找到该报文 MODBUS 地址，将收到的异常应答码存入相应的“MODBUS 从站通信状态字节”中。但如果：在 MODBUS 从站地址表中没有找到该报文 MODBUS 地址，则将**总状态字 IB0**中 D4~D1 “MODBUS 异常码”置 F。此时，不对“MODBUS 从站通信状态字节”进行任何操作。

(3) 如果 MODBUS 主站 (PB-B-MM/V33) 接收到的报文有 CRC 校验错或奇偶校验错，正常情况是：在 MODBUS 从站地址表中找到该报文的 MODBUS 地址，对相应的“MODBUS 从站通信状态字节”置标志位。但如果：在 MODBUS 从站地址表中没有找到该报文的 MODBUS 地址，则将**总状态字 IB0**中 D4~D1 “MODBUS 异常码”置 F，不对“MODBUS 从站通信状态字节”进行任何操作。

(5) 注意事项—配置从站最大报文条数

PB-B-MM/V33 型产品与原有 V32 型产品的不同之处是增加了对从站的状态监测功能，即在插槽的最末位置配置了 MODBUS 从站的状态监测表。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。所以 PB-B-MM/V33 配置的报文除了要求最大插槽数为 39 个，输入/输出最大字节总数不超过 232 个外，还与总的用户参数字节数有关。用户在使用不同的“有从站状态监测类型”时所能配置的最大从站报文条数是不相同。现对所有“有从站状态监测类型”作出归纳以供参考，具体报文条数见下表：

有从站状态监测类型与最大报文数对照表

有从站状态监测类型	所配从站的 最大报文条数	有从站状态监测类型	所配从站的 最大报文条数
从站状态监测类型 (8 位)	36	从站状态监测类型 (8 字节)	36
从站状态监测类型 (16 位)	34	从站状态监测类型 (16 字节)	34
从站状态监测类型 (24 位)	33	从站状态监测类型 (24 字节)	33
从站状态监测类型 (32 位)	32	从站状态监测类型 (32 字节)	32

7. V34 新功能介绍

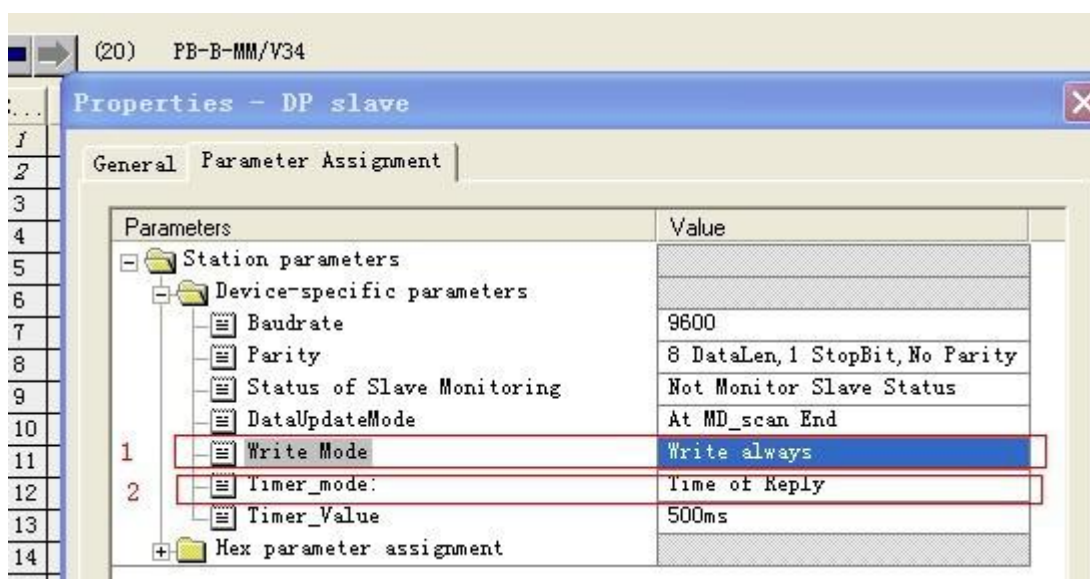
(1) 周期性发送报文功能

PB-B-MM/V33 及以前的版本在参数设置中可以设置“等待回答时间 Time of Replay”的时间，在设

定的时间内，如没有接受到应答报文，则视为从站无应答，发送下一条报文；如有接收到应答报文，则在接收到应答报文之后马上发送下一条报文。由于部分 MODBUS 设备在发送完一条报文后需要一段调整和反应的时间，所以这种主站连续发报文的方式很容易导致从站失去反应，发生通讯故障。基于上述原因，我们开发了 PB-B-MM/V34 版本，拥有周期性发送报文的功能，可以按照设置的时间间隔周期性发送报文，这样可以给从站调整的时间，解决了由于主站报文发送太快，从站没有反应时间而导致的通讯故障。

(2) 使用方法

PB-B-MM/V34 的使用方法与 V33 基本相同，唯一的不同点在于参数分配的设置。如图附录 1-1 所示。



附录 1-1 PB-B-MM/V34 的参数配置

- ① **Baudrate:** 为 MODBUS 的波特率从 300 到 57.6K 可选。
- ② **Patity:** 为数据位、停止位、校检，可选。
- ③ **Status of Slave Monitoring:** 选择有无从站状态监测。
- ④ **Data Update Mode:** 配置 PROFIBUS 和 MODBUS 数据更新模式。

PROFIBUS 和 MODBUS 数据更新模式: 是用户指定何时进行 PROFIBUS 数据区与 MODBUS 数据区的数据交换。

1、在每条 MD 回答后 At Evry MD End

在 MODBUS 扫描器完成每一条 MODBUS 通信命令后，就进行一次 PROFIBUS 和 MODBUS 数据区数据交换，这是缺省方式。

这种方式保证以最快速度传递 PROFIBUS 主站到 MODBUS 设备之间的数据。

2、在 MD 扫描结束后 At MD_scan End

在 MODBUS 扫描器完成整个一次 MODBUS 报文队列扫描后，进行一次 PROFIBUS 和 MODBUS 数

据区数据交换。

这种方式保证了 MODBUS 通信数据的完整性。

⑤ **Write Mode:** 实现对写命令的控制功能。

“Write always”: 总线桥启动后, 写指令就发送;

“Write on change” 总线桥启动后, 当写的数据有改变时才发送。

⑥ **Timer_mode:** 对发送时间控制。

“Time of Reply”: 超时时间(Timer_Value), 即等待接收时间到后, 马上发送下一条报文;

“Same Interval”: 按设置好的时间值(Timer_Value)定时发送, 即按照设置的时间间隔周期性发送报文。

⑦ **Timer_Value:** 选择时间值。如果“Timer_mode”选择了“Time of Reply”, 则此处设置的时间值为等待从站应答的时间, 超过这个时间, 则认为从站无应答, 发送下一条报文; 如果“Timer_mode”选择了“Same Interval”, 则此处设置的时间值为发送报文的时间间隔。

第六章 有毒有害物质表

根据中国《电子信息产品污染控制管理办法》的要求出台

部件名称	有毒有害物质和元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr (VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
塑料外壳	0	0	0	0	0	0
电路板	X	0	0	0	0	0
铜螺柱	0	0	0	0	0	0
贴膜	0	0	0	0	0	0
插座/插头	X	0	0	0	0	0

0: 表示在此部件所用的所有同类材料中, 所含的此有毒或有害物质均低于 SJ/T1163-2006 的限制要求;

X: 表示在此部件所用的所有同类材料中, 至少一种所含的此有毒或有害物质高于 SJ/T1163-2006 的限制要求。

注明: 引用的“环保使用期限”是根据在正常温度和湿度条件下操作使用产品而确定的。

现场总线 PROFIBUS (中国) 技术资格中心
北京鼎实创新科技股份有限公司

电话: 010-82078264、010-62054940 传真: 010-82285084
 地址: 北京德胜门外教场口 1 号, 5 号楼 A-1 室 邮编: 100120
 Web: www.c-profibus.com.cn Email: tangjy@c-profibus.com.cn