

REDTECH

瑞德泰科



RBCM 工业总线转换模块产品手册

INDUSTRIAL BUS CONVERSION MODULE

www.redtech.cn

型号：RBCM PBMB-02

RBCM PBMB-04

版本：2.1

初始日期：2013.03.01

版本日期：2016.09.30

警告提示

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

危险

表示如果不采取相应的小心措施，将会导致死亡或者严重的人身伤害。

- › 请在本产品的外部采取安全措施，即使本产品的故障或外部原因引发异常，系统整体也可安全运转。
- › 请不要在有可燃性气体的空气介质中使用。否则可能会引起爆炸。
- › 请不要将锂电池投入火中。否则可能会引起电池及电子产品破裂。

警告

表示如果不采取相应的小心措施，可能导致死亡或者严重的人身伤害。

- › 为防止异常发热及冒烟，使用时请相对于本产品的保证特性、性能数值留有一定的余量。
- › 请不要分解、改造。否则会引起异常发热及冒烟。
- › 通电中请不要触摸端子。否则会造成触电。
- › 请在外部电路中设置紧急停止、联锁电路。
- › 请切实连接电线及接插件。若未完全连接，可能会出现异常发热或冒烟。
- › 请不要将液体、可燃物、金属等异物放入产品内部。否则会引起异常发热、冒烟。
- › 请不要在接通电源的状态下进行施工（连接、拆卸等）。否则会引起触电

小心

表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意

表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的合格人员进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。由于具备相关培训及经验，合格人员可以察

觉本产品/系统的风险，并避免可能的危险。

商标

所有带有标记符号®的都是沈阳瑞德泰科电气有限公司的注册商标。标签中的其他符号可能是一些其他商标，这是出于保护所有者权利的目地由第三方使用而特别标示的。

关于著作权及商标的记述

- › 本手册的著作权归沈阳瑞德泰科电子有限公司所有。
- › 绝对禁止对本书的随意复制。
- › 其他公司及产品名称是各公司的商标或注册商标。

责任免除

- › 我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。
- › 因商品改良，规格、外观及手册内容会有所更改，恕不另行通知，敬请谅解。

前 言

非常感谢您购买我公司的RBCM工业总线转换模块产品，希望能够在使用前详细阅读本手册，并且严格按照本手册的说明进行安装、布线、操作和调试。我们真诚的希望您能够对我们的产品和服务提出宝贵意见。

本手册目的

本手册中包含的信息可用作RBCM工业总线转换模块产品的硬件构成、模块的安装、操作、功能及其技术数据的参考资料。

需要的基本知识

本手册假定您具有一定的自动化工程领域的常识。

本手册适用范围

本手册基于手册发行时有效的数据描述各模块。

本公司有权增加每个新模块以及每个更新版本的模块的产品信息。

技术支持

如果您在使用过程中遇到问题可以通过以下方式联系我们技术服务人员：

电话：024-64691655

传真：024-64691675

MAIL：SERVICE@REDTECH.CN

网址：WWW.REDTECH.CN

版本更新

2013年03月01日，手册版本V1.1。

2014年01月01日，手册版本V1.2。

在modbus作为主站的模式中，在要写入的数据无变化的时候，modbus可以选择不执行写入命令。即05、06、0F、10命令可以选择不执行。选择方式为控制位X.4=1数据无变化不执行写入命令，X.4=0数据无变化执行写入命令。硬件V0.2版本以上有效。

2014年07月22日，手册版本V1.3。

在modbus作为主站的模式中，增加从站无回复或者回复有错误，数据清零功能，原版本是保持原来数据不可清零。选择方式为控制位X.3=1数据清零，X.3=0数据保持原来通信正确的数据。硬件V0.5版本以上有效。

在modbus作为主站的模式中，增加查询间隔可调功能，原版本固定50ms，现在可以选择到0ms-2500ms。默认为50ms。硬件V0.5版本以上，GSD文件V2.0版本以上有效。

2015年07月01日，手册版本V2.0。

产品更换了全铝合金外壳，改变了外形尺寸。

增加了串口可以利用串口调试软件进行监视诊断功能，方便modbus通信的诊断。硬件V2.0版本以上有效。GSD文件V2.0版本保持不变。

2016年09月30日，手册版本V2.1。

在modbus作为主站的模式中，更改了控制字的第二位QX.1和第三位QX.2的功能。

原来，控制字QX.1功能为启动MODBUS 扫描，只发送MODBUS 读命令，现在调整为保留。控制字QX.2功能为启动MODBUS 扫描，只发送MODBUS 写命令，现在调整为启用USB接口监视诊断功能。

硬件V2.2版本以上有效。GSD文件V2.0版本保持不变。

目 录

1 产品概述	7
1.1 产品功能	7
1.2 产品特点	8
1.3 通讯接口概述	9
1.4 RBCM 产品型号定义	10
2 产品说明	11
2.1 硬件说明	11
2.2 技术数据	15
2.3 外形尺寸	18
2.4 产品安装	19
3 协议转换原理	20
3.1 硬件结构	20
3.2 与 PROFIBUS 的连接	21
3.3 PROFIBUS 与 MODBUS 的协议转换原理	23
4 MODBUS 为主站工作模式的应用	25
4.1 建立一个项目	25
4.2 建立一个 PROFIBUS 总线	27
4.3 在项目中配置一个总线转换模块	31
4.4 配置 RBCM PBMB-04(02) 的 MODBUS 报文队列	34
4.5 MODBUS 报文详解	36
4.6 通信状态字与通信控制字	53
4.7 对从站通讯状态监测	56
4.8 MODBUS 通讯故障及排除	62
5 MODBUS 为从站工作模式的应用	68
5.1 建立一个项目	68
5.2 在项目中配置一个总线转换模块	68
5.3 配置 RBCM PBMB-04(02) 的 MODBUS 报文队列	70
5.4 MODBUS 报文详解	72
5.5 通信状态字与通信控制字	81
5.6 MODBUS 通讯故障及排除	83
6 故障和排除	87
6.1 电源及 PROFIBUS 故障及排除方法	87
6.2 MODBUS 通讯故障及排除方法	87
附录	88
A 产品订货一览表	88
B MODBUS 协议简介	88

产品概述

1

引言

本章对 RBCM 工业总线转换模块作简要的概述。

本章主要叙述了：

› 产品功能› 产品特点› 基本参数› 型号定义

1.1 产品功能

1.1.1 RBCM工业总线转换模块的功能

RBCM 工业总线转换模块可以成为不同工业现场总线之间通讯的桥梁，实现不同现场控制器的相互通讯。众所周知，现在工业现场总线协议种类很多，在很多过程控制、机械控制中由于控制器、传感器等设备的总线接口不同而难以实现相互通讯，无法完成数据采集和控制等功能。RBCM 工业总线转换模块就可以解决这个问题，使得在设计选型过程中不在考虑通讯协议的问题、使得现场控制器、传感器、执行器实现互联。

1.1.2 应用领域

RBCM 工业总线转换模块主要应用于不同总线协议的控制器、传感器、执行器之间的通讯领域。可以应用于钢铁冶金、石油化工、汽车制造、轨道交通、水处理等行业。

1.1.3 RBCM PBMB-04 (02) 主要功能

工业总线转换模块在 PROFIBUS 接口侧只能做从站，在 MODBUS 接口侧可以有两种工作模式。

MODBUS 通讯口设定为主站模式 :可以将多个具有 MODBUS RTU 协议的产品连到 PROFIBUS 总线中成为一个从站与 PROFIBUS 主站通讯，从而使他们形成一个整体。见图 1-1 。

MODBUS通讯为主站工作模式

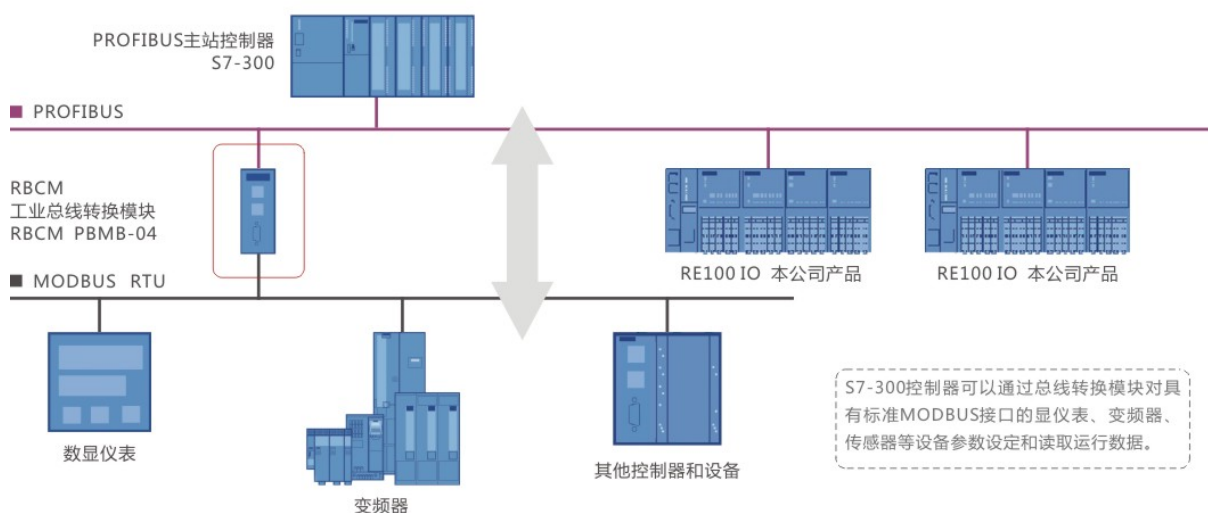


图 1-1

MODBUS 通讯口设定为从站模式：可以将 PROFIBUS 主站和多个 MODBUS RTU 主站连接到一起，使得两个不同协议的主站相互通讯。见图 1-2。

MODBUS通讯为从站工作模式

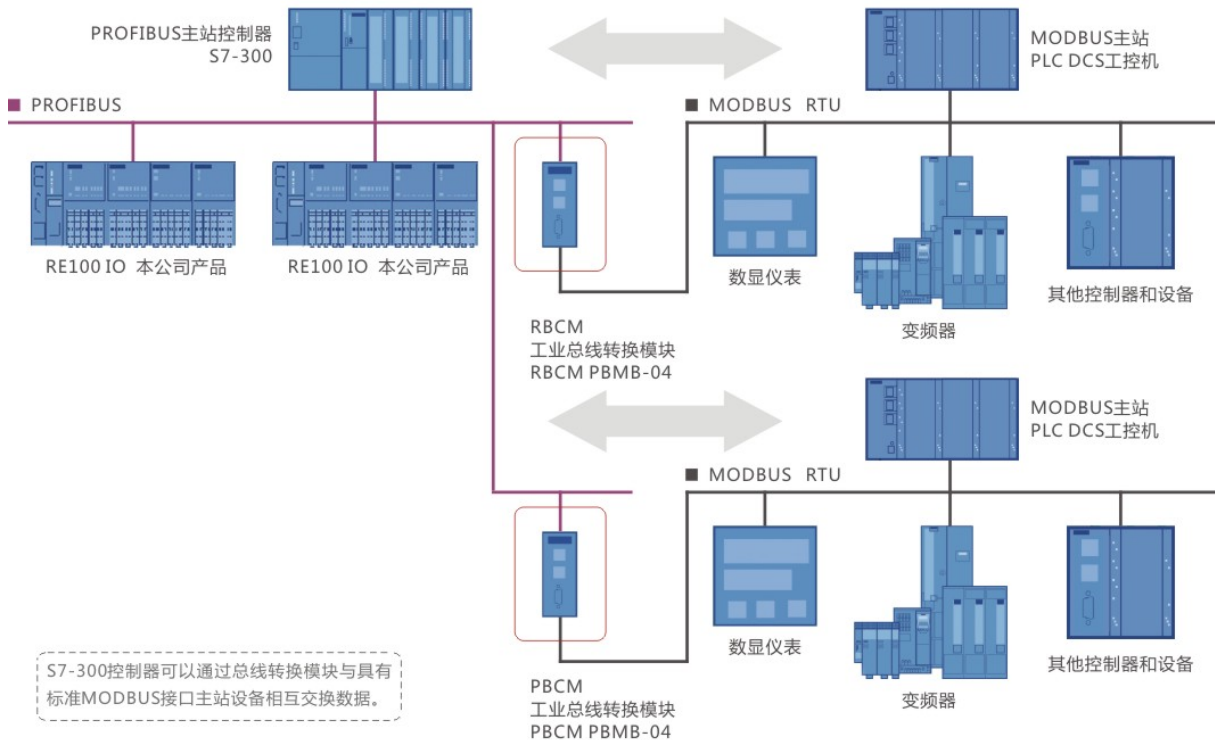


图 1-2

1.2 产品特点

› 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。

› 多种工作模式

一个型号同时具备MODBUS主站工作模式和MODBUS从站工作模式，可应于不同的场合，只需要使用不同的GSD文件即可实现工作模式的转换。

› 透明通讯

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。

› 强大的模块诊断

模块附带USB接口，利用串口调试软件可以监测模块与PROFIBUS通信状态，和MODBUS通信代

码的发送和接收状态。

› 工业设计

- 双路冗余 DC24V 宽电压供电，输入电压范围为 18V ~ 36V。
- PROFIBUS 接口和 MODBUS 接口都具有 1500V 电气隔离。
- 铝合金外壳，IP30 防护等级。
- 标准的 35mm 导轨安装。

› 应用广泛

凡是具有模块 MODBUS RTU 标准通讯协议的产品,不管是主站协议还是从站协议都可以通过 RBCM PBMB-04(02)工业总线转换模块实现与 PROFIBUS 主站接口的互联。

1.3 通讯接口概述

1.3.1 PROFIBUS 接口概述

- › RBCM PBMB-04(02)工业总线转换模块在PROFIBUS侧是一个PROFIBUS-DP从站接口。
- › 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。
- › PROFIBUS-DP 从站，波特率自适应，最大波特率12M。
- › PROFIBUS 输入/输出数量可自由设定，最大PROFIBUS 输入/输出；
 - Input Bytes + Output Bytes \leq 232 Bytes
 - Max Input Bytes \leq 224 Bytes
 - Max Output Bytes \leq 224 Bytes

1.3.2 MODBUS 接口概述

- › RBCM PBMB-04(02)工业总线转换模块在MODBUS一侧即可以工作在MODBUS主站模式也可以工作在MODBUS从站模式。
- › 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。
- › MODBUS RTU支持01H、02H、03H、04H、05H、06H、0FH、10H功能。
- › MODBUS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。
- › RBCM PBMB-04工业总线转换模块MODBUS接口是标准的RS485 接口。

RBCM PBMB-02工业总线转换模块MODBUS接口是标准的RS232接口。

1.4 RBCM 产品型号定义

产品系列	协议一	协议二	序号
RBCM	PB	MB	-04

RBCM : REDTECH Bus Conversion Module

PB : PROFIBUS 协议

MB : MODBUS 协议

02 : 标准 RS232 接口

04 : 标准 RS485 接口

引言

本章详细地阐述了 RBCM PBMB-04 (02) 工业总线转换模块技术数据，包括：

- › 产品各部分说明
- › 详细的技术数据
- › 外形尺寸
- › 产品安装

2.1 硬件说明

2.1.1 模块组成

- ①产品商标和产品名称
- ②电源指示灯
- ③模块 USB 诊断接口
- ④PROFIBUS 地址编码
- ⑤PROFIBUS 通讯状态灯
- ⑥PROFIBUS 通讯接口
- ⑦MODBUS 通讯状态灯
- ⑧电源端子
- ⑨模块固定器
- ⑩MODBUS 通讯接口

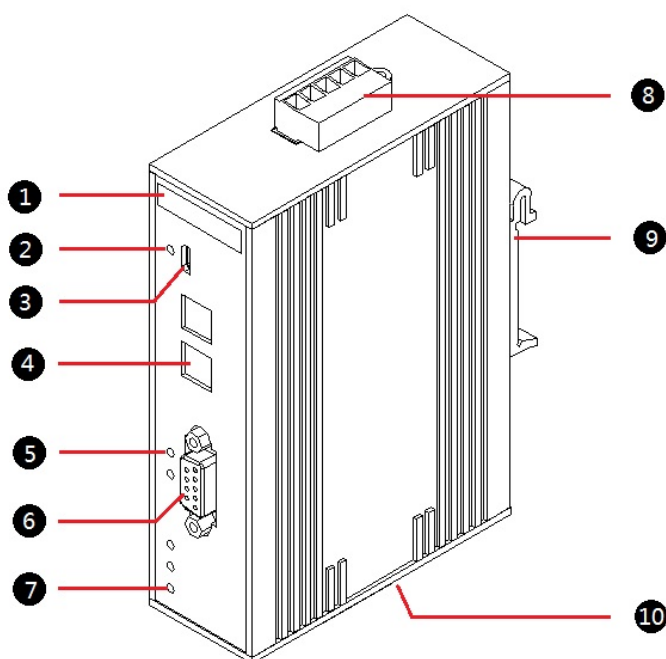


图 2-1

2.1.2 顶视面板图



图 2-2

2.1.3 指示灯说明

› PROFIBUS 通信状态指示灯说明

P LED	BF LED	BC LED	含义	补救措施
灭	灭	灭	电源电压缺失或不足。	查看供电电源电压
亮	亮	灭	未建立到PROFIBUS控制器的总线网络中。	检查profibus通信电缆，组态以及编码地址。
亮	灭	亮	建立到PROFIBUS控制器的总线网络中。	

› MODBUS 通信状态指示灯说明

TD LED	RD LED	ALM LED	含义	补救措施
灭	灭	亮	MODBUS接口无任何数据发送和接收。	
闪	灭	亮	MODBUS接口只发送数据无接收数据。	见故障处理章节
灭	闪	亮	MODBUS接口只接收数据无发送数据。	见故障处理章节

			MODBUS接口正常发送和接收数据。
闪	闪	灭	

2.1.4 地址编码开关说明

› 地址的设定

视图	名称	举例
 <p>X10</p>	×10编码开关为地址的十位设定	×10编码开关=5 ×1编码开关=5 PROFIBUS从站地址: $5 \times 10 + 5 \times 1 = 55$ 最大编码地址为99
 <p>X1</p>	×1编码开关为地址的个位设定	

› 更改 PROFIBUS 地址

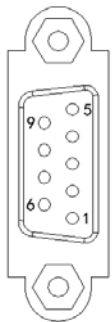
可以在任何时候更改 PROFIBUS 地址。但是仅在切断/接通 24 V DC 电源后才采用新的 PROFIBUS 地址。

2.1.5 PROFIBUS 总线接口

› 接口符合 PROFIBUS 标准

DP-V0协议 符合标准IEC 61784-1 :2002 Ed1 CP 3/1及中国国家标准GB/T20540-2006 : 测量和控制数字数据通信工业控制系统用现场总线的第3部分：PROFIBUS 规范。

› PROFIBUS 接口引脚定义

视图	名称	
	1	屏蔽
	3	信号B(+)
	4	RTS
	5	0V
	6	5V
	8	信号A (-)
	2.7.9	未定义

› PROFIBUS 接口的连接

产品采用标准PROFIBUS 9 针D 形插座（孔），建议用户使用标准PROFIBUS 插头和 PROFIBUS 电缆连接。有关PROFIBUS 安装规范请用户参照有关PROFIBUS 技术标准。当 PROFIBUS 插头位于总线终端时，必须将插头上的终端电阻拨码开关拨到“ON”的位置，即将PROFIBUS 终端电阻接入到总线中；否则插头上的小拨码开关拨到“OFF”位置。

2.1.6 MODBUS 通讯接口

› RBCM PBMB-04工业总线转换模块的RS485接口

-RS485通讯接口位于总线中间的接线图，见图2-3。

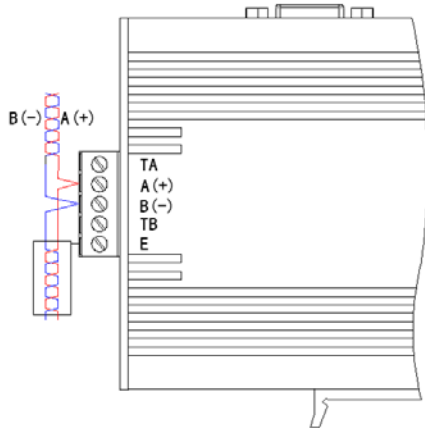


图2-3

-RS485通讯接口位于总线两端的接线图，见图2-4。

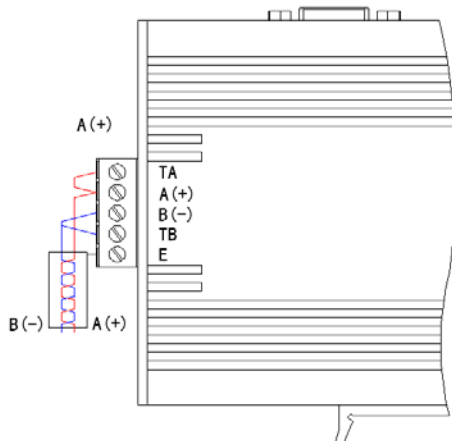


图2-4

-RS485传输技术基本特征

™ 网络拓扑：线性总线，两端有有源的总线终端电阻；

+ 传输速率：2400 bit/s~57.6Kbit/s；

- 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）；

× 站点数：每分段32个站（不带中继），最多可达到127个站（带中继）；

÷ 插头连接：5针端子

-RS485传输设备安装要点

™ 全部设备均与RS485 总线连接；

+ 每个分段上最多可接32个站；

- 每段的两端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。

× 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。

÷ A 型电缆参数：

阻抗：135-165W 电容：< 30pf/m

回路电阻：110W线规：0.64mm 导线面积：>0.34mm²/W

= 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覆盖，以保持良好的传导性，另外建议数据线与高压线隔离。

› RBCM PBMB-02工业总线转换模块的RS232接口

-MODBUS RS232接口连接器为5针端子。

-MODBUS RS232接口定义

RBCM PBMB-02 5 针端子	
3	Received Data
2	Transmit Data
1	Signal Ground
5	地

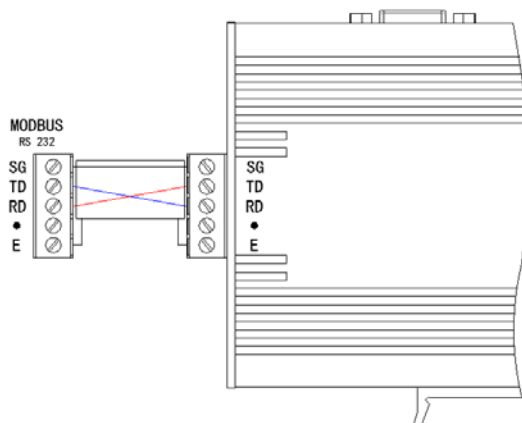


图 2-5

2.1.7 模块 USB 诊断接口

-模块诊断接口是调试的辅助通信接口。可以诊断 PROFIBUS 的通信状态，也可以通过 MODBUS 接口收发报文的分析，来辅助与 MODBUS 设备的调试。

-模块诊断接口连接器为 USB micro（与移动电话的充电接口相符）。

-可以利用串口调试软件，来接收模块的诊断信息。

2.1.8 电源接口

-采用双电源冗余设计

-电源输入额定电压 DC24V(-25%...+30%)

-电源接口定义

1L+	电源 1 正端
1M	电源 1 负端
2L+	电源 2 正端
2M	电源 2 负端
E	地

-电源接线图

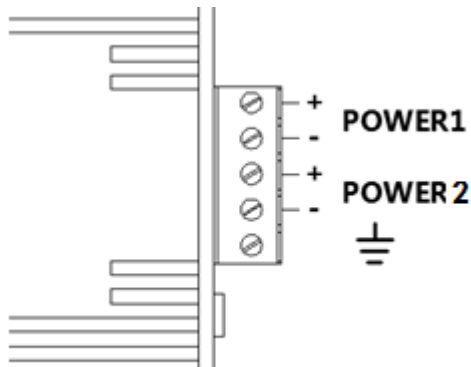


图 2-5

-注意：要保证良好的接地。

2.2 技术数据

电源参数	
供电电压	DC24V(-25%...+30%)
电源冗余	有
电源隔离	1500V 电气隔离
极性保护	有
额定电流	125mA
PROFIBUS 通讯接口参数	
符合 PROFIBUS 通讯接口标准	符合 PROFIBUS DP 通讯接口 V0 标准
隔离保护	1500V 电气隔离
波特率	自适应，最大 12M
PROFIBUS 最大输入输出量	
-Input Bytes + Output Bytes	≤232 Bytes
-Max Input Bytes	≤224 Bytes
-Max Output Bytes	≤224 Bytes
MODBUS 通讯接口参数	

物理接口	RS485 , 插拔式连接器(RBCM PBMB-04)
	RS232 , 插拔式连接器(RBCM PBMB-02)
隔离保护	1500V 电气隔离
MODBUS 协议	支持标准的MODBUS RTU协议 , 支持01H、02H、03H、04H、05H、06H、0FH、10H功能码
波特率	2400、4800、9600、19.2K、38.4K、57.6K 115.2K可选
校验位和停止位	可设定
综合参数	
工作温度	-10°C ~ 60°C
存储温度	-40°C ~ +85°C
允许湿度	5% ~ 95%不结露
防护等级	IP20
外壳	铝合金外壳
安装类型	DIN35mm 导轨
尺寸 (宽/高/深)	35/149/100mm
重量	340g
抗振动	符合 IEC 60068-2-6 标准
抗冲击	符合 IEC 60068-2-27 标准
EMC-抗干扰性	符合 IEC 61000-4 标准
EMC-辐射干扰	符合 EN55011 标准

2.3 外形尺寸

2.3.1 RBCM PBMB-04(02)工业总线转换模块外形尺寸图

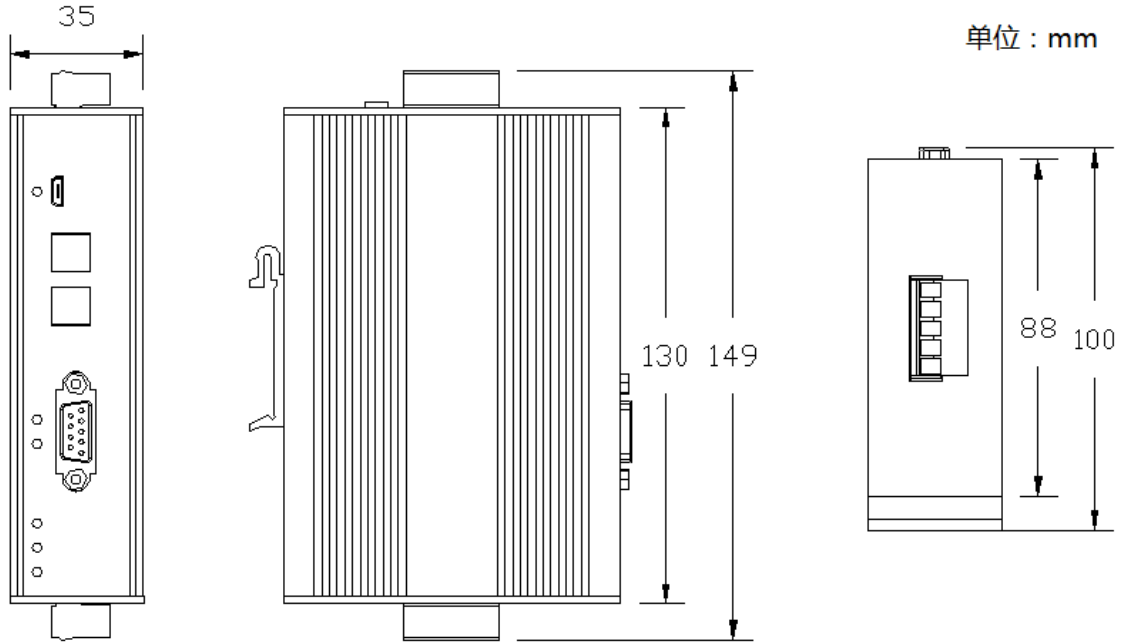


图 2-6

2.4 产品安装

2.4.1 产品安装方式

- › 标准的 35mm 导轨安装

2.4.2 安装空间

- › 上下安装空间

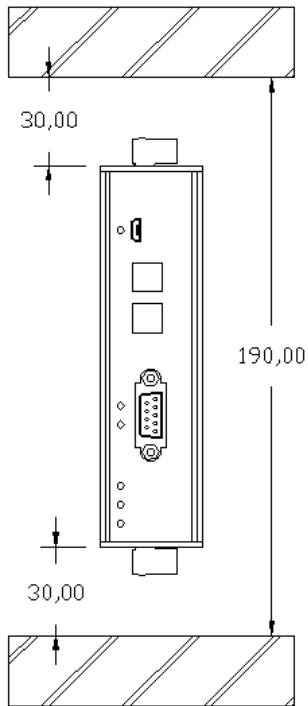


图 2-7

- › 顶部安装空间

因为模块顶部可能用 PROFIBUS 总线连接器，要留有一定的安装空间。

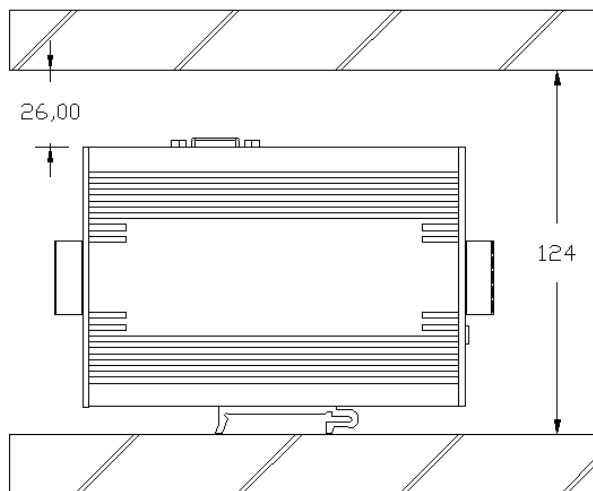


图 2-8

引言

本章详细地阐述了 RBCM PBMB-04 (02) 工业总线转换模块技术数据，包括：

- › 产品各部分说明
- › 详细的技术数据
- › 外形尺寸
- › 产品安装

3.1 硬件结构

RBCM PBMB-04(02)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。

- › RBCM PBMB-04硬件结构图

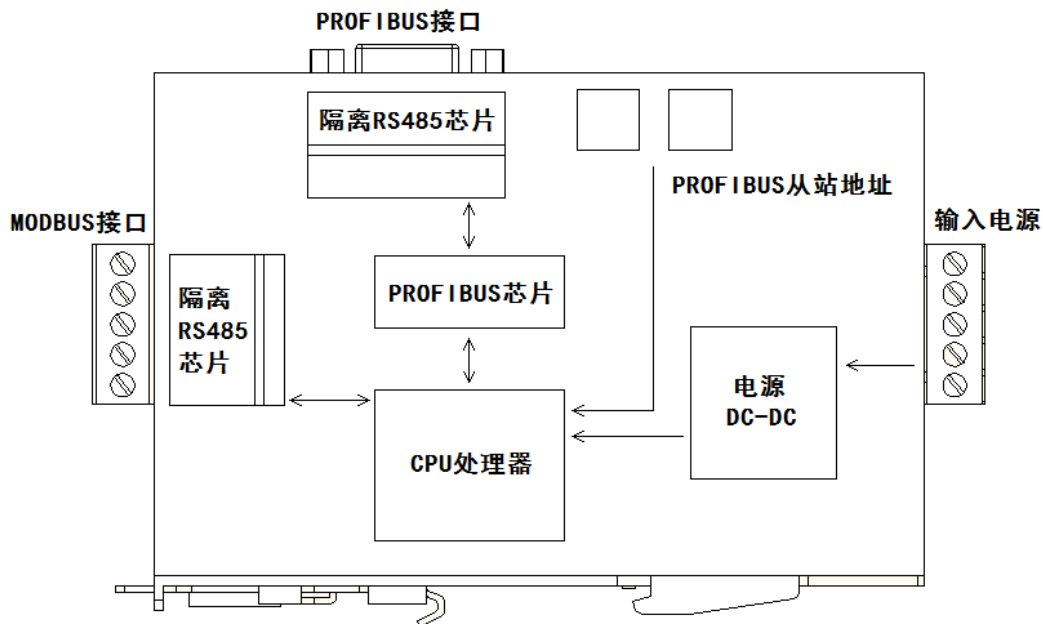


图3-1

› RBCM PBMB-02硬件结构图

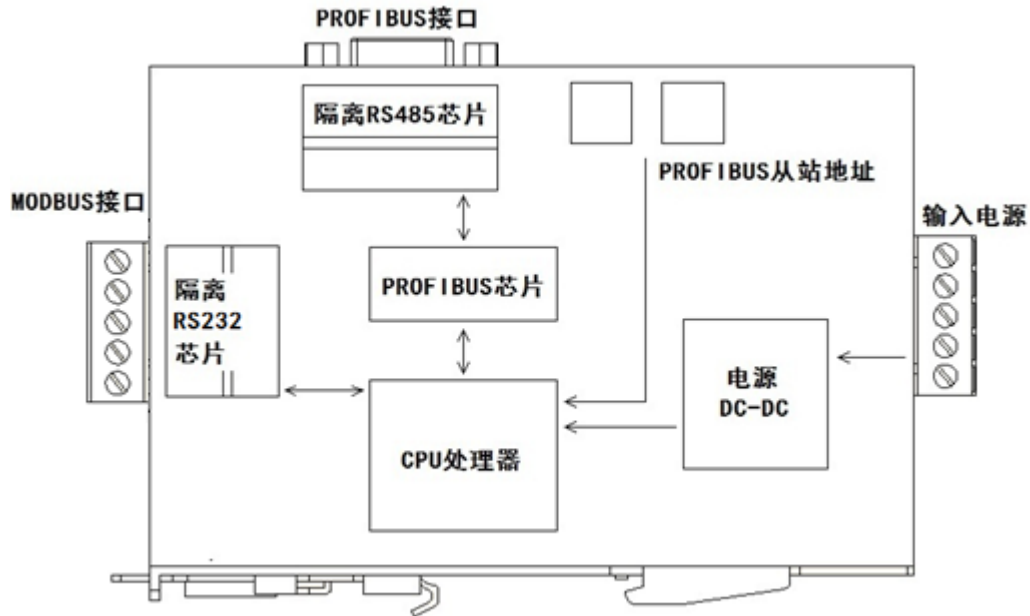


图3-2

- PROFIBUS标准驱动电路，由光隔及RS485 驱动组成。
- MODBUS接口电路由光隔及RS232或者驱动芯片组成。
- CPU 通过对PROFIBUS芯片控制实现PROFIBUS 的通信，并在RAM 中建立PROFIBUS 通信数据缓冲区。
- CPU通过MODBUS接口电路实现和外部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。

3.2 与 PROFIBUS 的连接

3.2.1 MODBUS接口为从站工作模式与PROFIBUS的连接

在PLC 为主站的PROFIBUS 系统中，RBCM PBMB-04(02)是PROFIBUS 从站；另外一侧，RBCM PBMB-04(02)通过485/RS232与MODBUS 设备连接，是一个MODBUS 设备的从站，即：等待接收MODBUS 主站设备发送的MODBUS 通信报文并回答。PLC为主站的PROFIBUS 系统中使用RBCM PBMB-04(02)将MODBUS 主站设备或一个MODBUS局域网连接到PROFIBUS上。如图3-3。

MODBUS通讯为从站工作模式

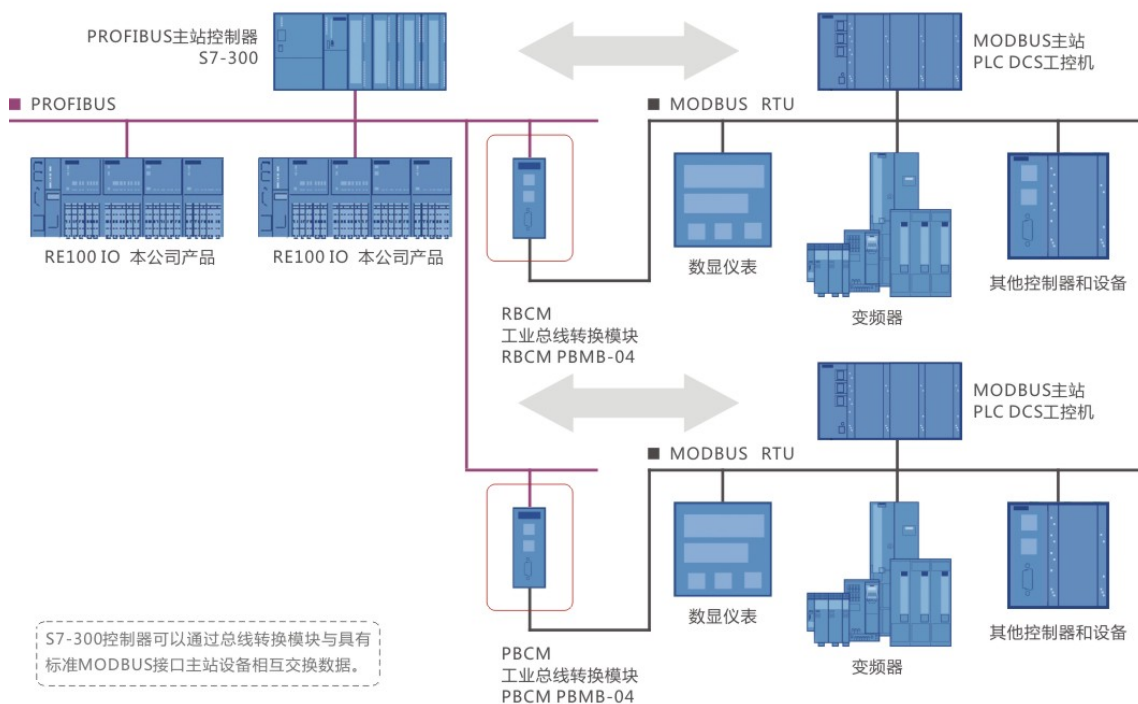


图3-3

3.2.1 MODBUS 接口为主站工作模式与 PROFIBUS 的连接

在 PLC 为主站的 PROFIBUS 系统中，RBCM PBMB-04(02) 是一个 PROFIBUS 从站，另一侧 RBCM PBMB-04(02) 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。PLC 为主站的 PROFIBUS 系统中使 RBCM PBMB-04(02) 将一个或多个 MODBUS 设备连接到 PROFIBUS 上。如图 3-4。

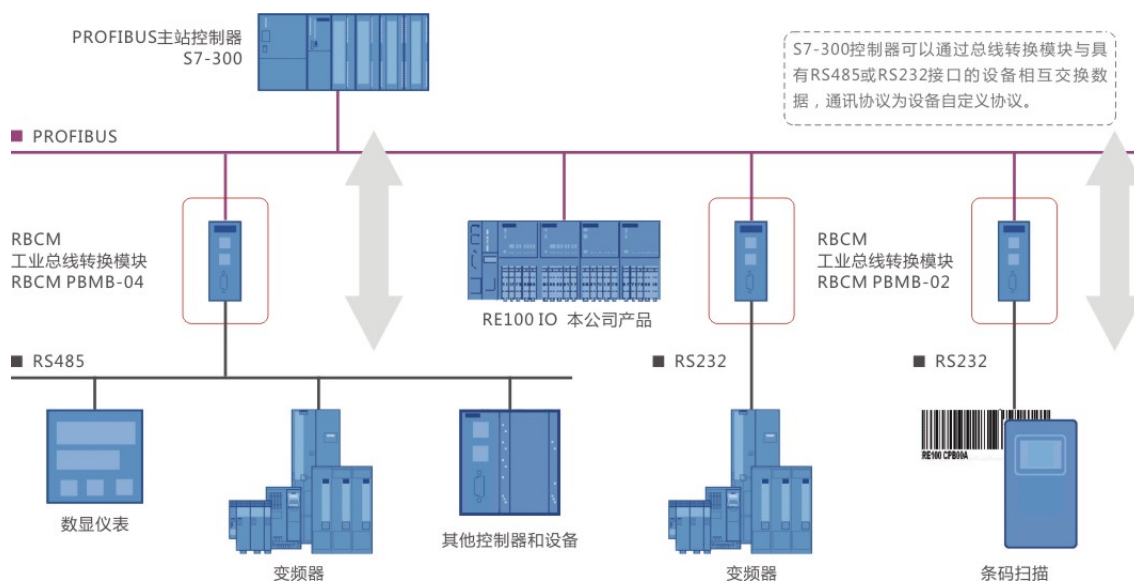


图3-4

3.3 PROFIBUS 与 MODBUS 的协议转换原理

3.3.1 MODBUS接口为从站工作模式与PROFIBUS协议转换原理

› MODBUS存储区

模块MODBUS接口作为主站与标准MODBUS 设备一样，有4个存储区。

存储区	名称	类型	读写	存储单元地址
0XXXX	线圈	位	读/写	最大224 BYTES = 1792 BITS ; 地址：00001 ~ 01792
1XXXX	数字量输入	位	只读	最大224 BYTES = 1792 BITS ; 地址：10001 ~ 11792
3XXXX	输入寄存器	字	只读	最大224 BYTES = 112 WORDS ; 地址：30001 ~ 30112
4XXXX	保持寄存器	字	读/写	最大224 BYTES = 112 WORDS ; 地址：40001 ~ 40112

› MODBUS存储区MODBUS存储区与PROFIBUS输入/输出对应关系

RBCM PBMB-04(02)通过PROFIBUS输入/输出与对应的MODBUS存储区数据交换，实现MODBUS到PROFIBUS 的数据通信

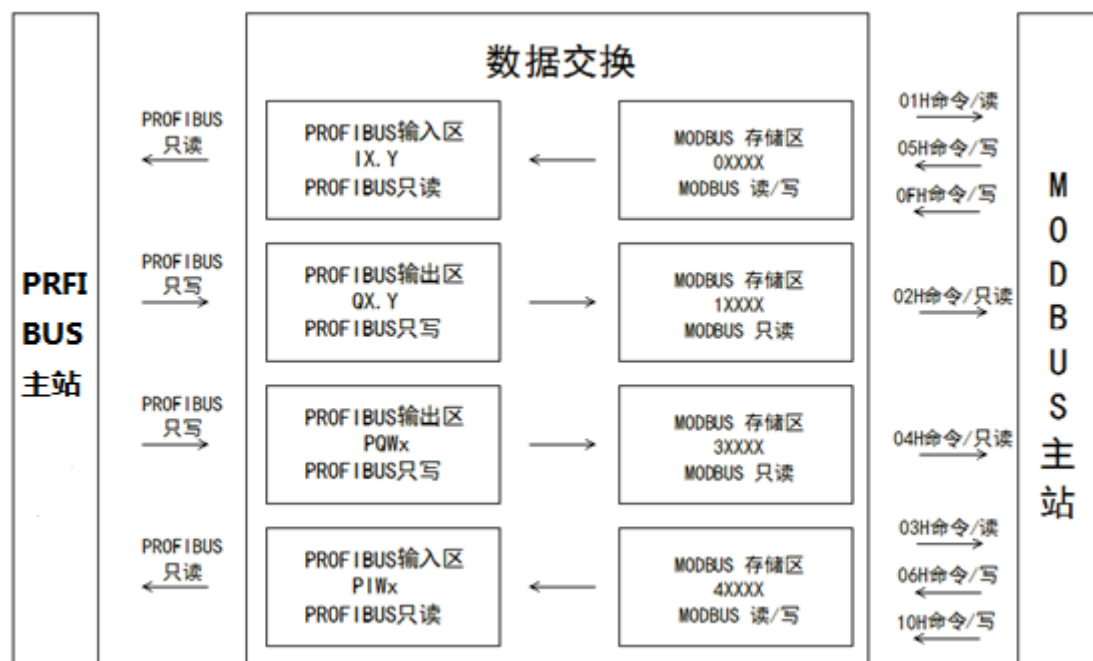


图3-5

3.3.2 MODBUS接口为主站工作模式与PROFIBUS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。

(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。

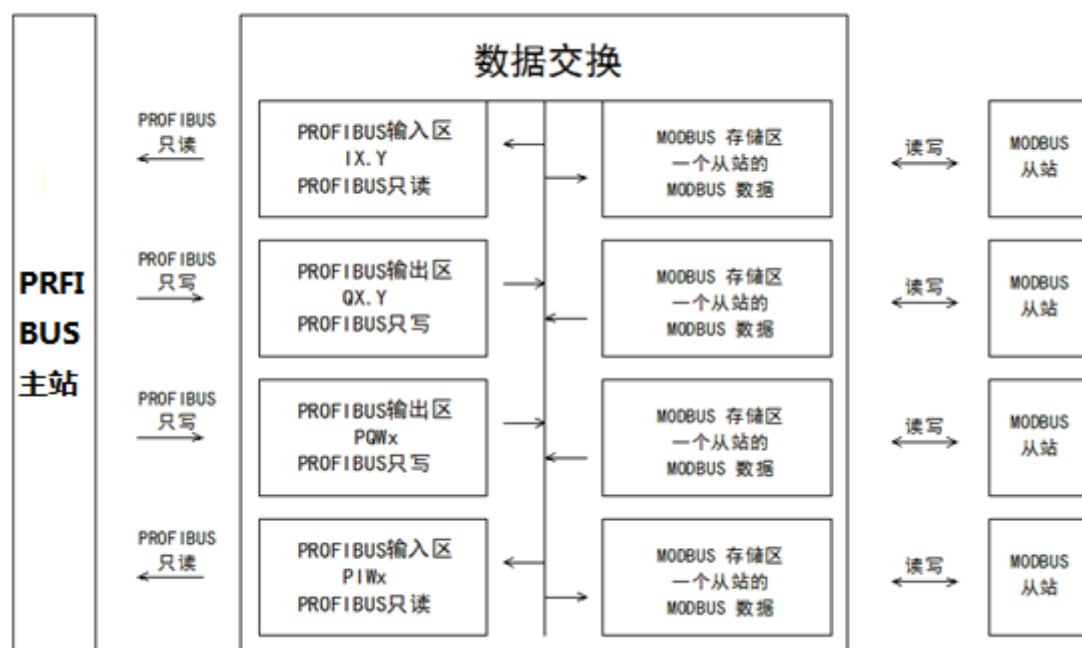


图3-6

(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。

MODBUS 为主站工作模式的应用

4

引言

本章使用 S7300 作为 PROFIBUS 主站，STEP7 为配置和调试软件详细的介绍了 PBCM PBMB-04(02)模块的 MODBUS 为主站工作模式的应用方法，包括：

- › S7300工程的建立
- › MODBUS通讯接口的设定
- › 实例列举了01H、02H、03H、04H、0FH、10H、05H、06H MODBUS功能码的配置
- › PBCM PBMB-04(02)模块的状态字和控制字介绍

如果您对 STEP7 软件非常熟悉，那么您可以从“4.3 在项目中配置一个总线转换模块”开始阅读。如果您是一般的使用者，模块的基本功能就满足您的要求，您可以阅读到“4.6 通信状态字与通信控制字”部分。

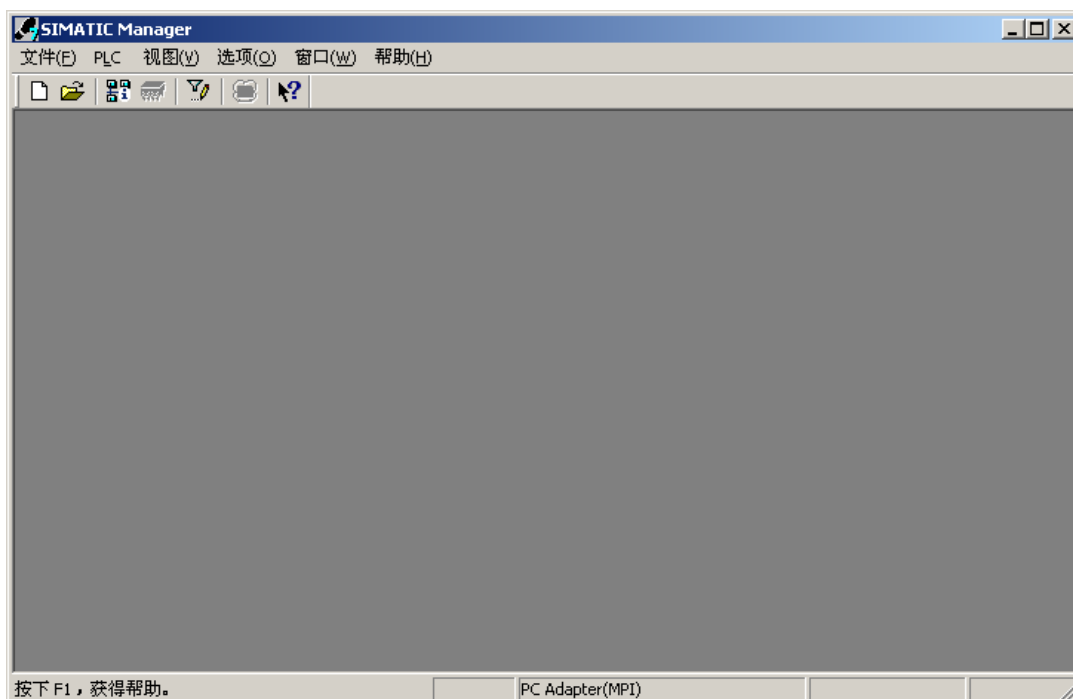
4.1 建立一个项目

- › 将 BC-MSV10.gsd 和 BC-MMV10.gsd 文件复制到 step7 安装目录下的“.\Siemens\Step7\S7DATA\GSD”文件夹中。

比如默认的 c 盘的安装路径“C:\Program Files\Siemens\Step7\S7DATA\GSD”。



- › 打开“SIMATIC Manager”，启动后的界面如图 4-1 所示：



- › 点击菜单栏中的“文件->新建(N)...”,在出现的“新建 项目”对话框中输入项目的名称“MODBUS-Master” 其他使用默认。然后左键点击“确定”,如图 4-2 所示。

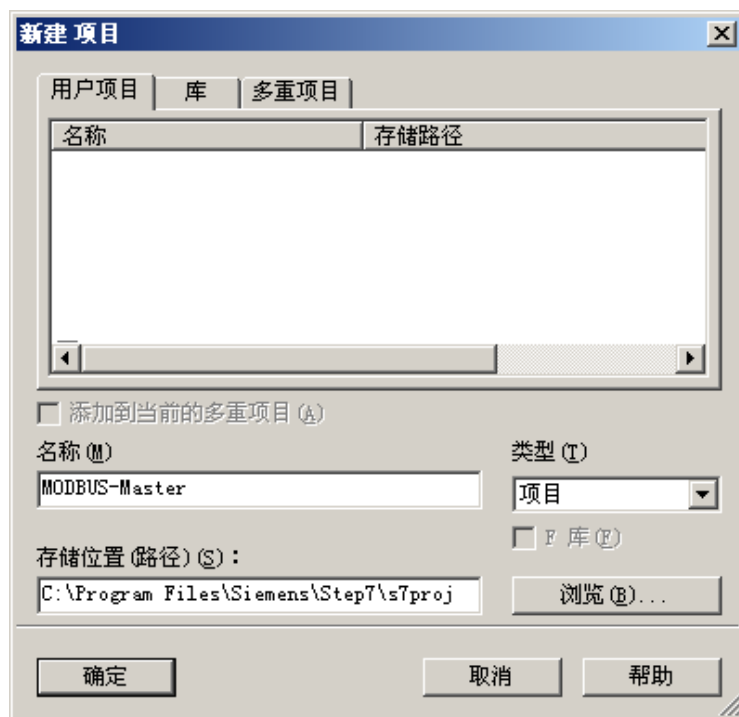


图 4-2

- › 建立一个 S7300 的工程，点击菜单栏中的“插入->站点->SIMATIC 300 站点”结果如图 4-3 所示。

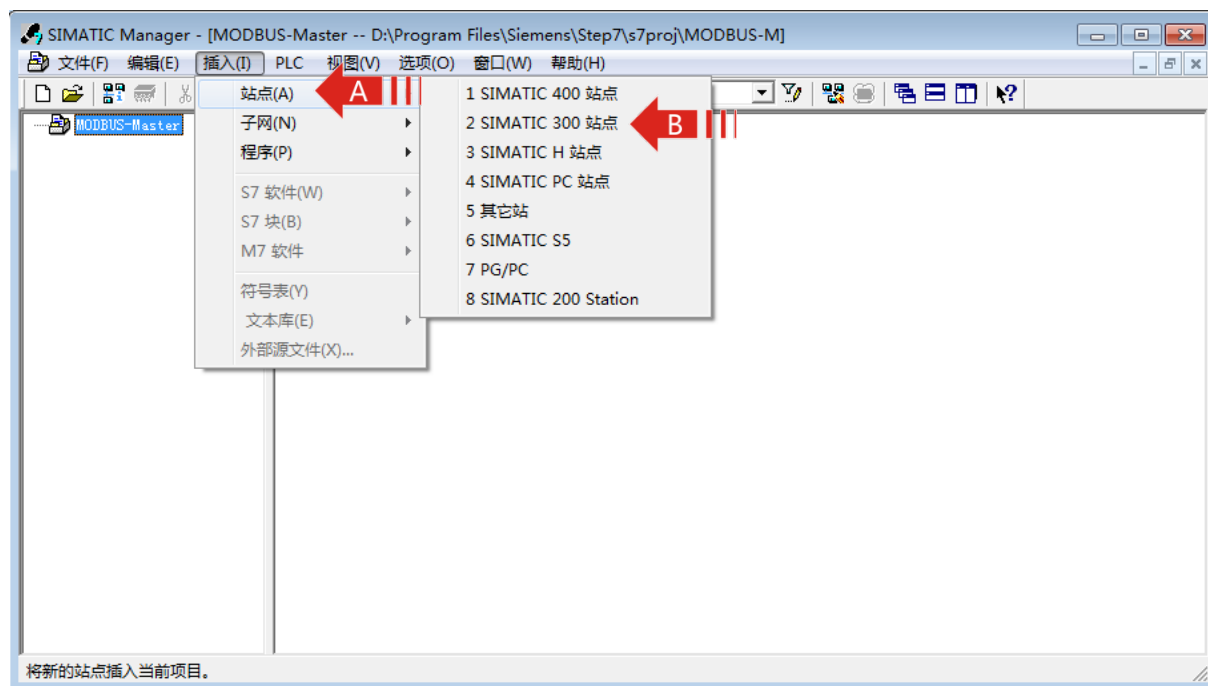


图 4-3

- › 这样一个 S7300 工程的建立完成了，双击 STMATIC 300(1)，进入 S7300 (1) 系统如图 4-4。

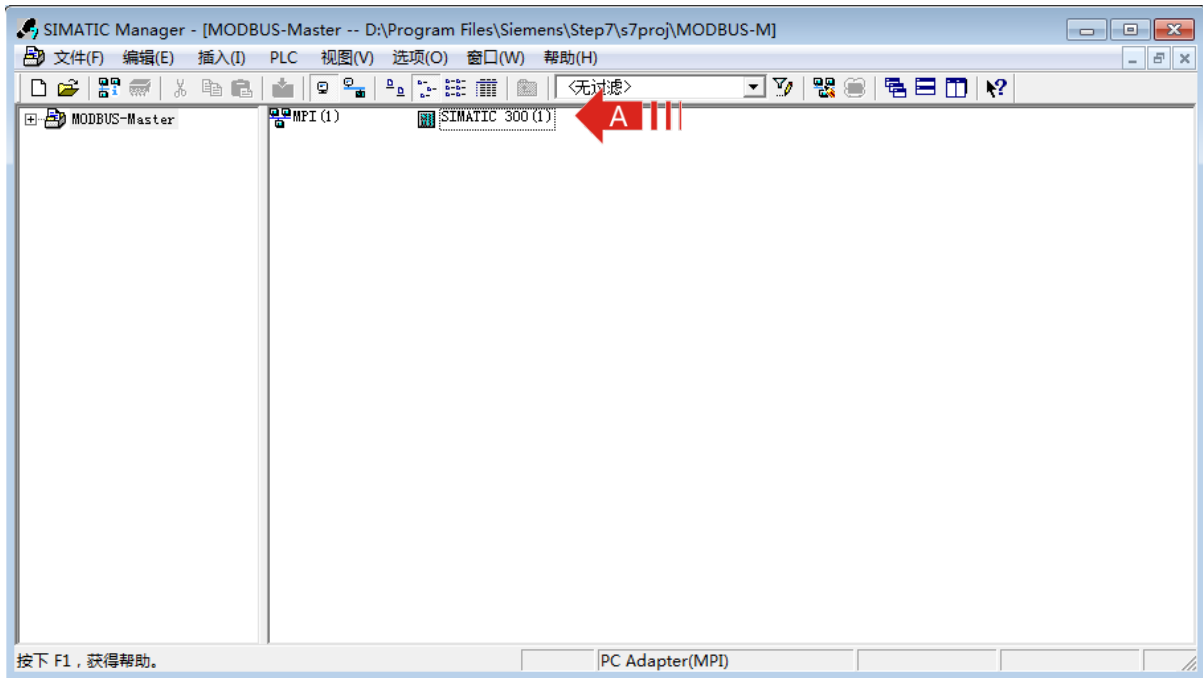


图 4-4

› 完成了进入 S7300 (1) 系统如图 4-5。

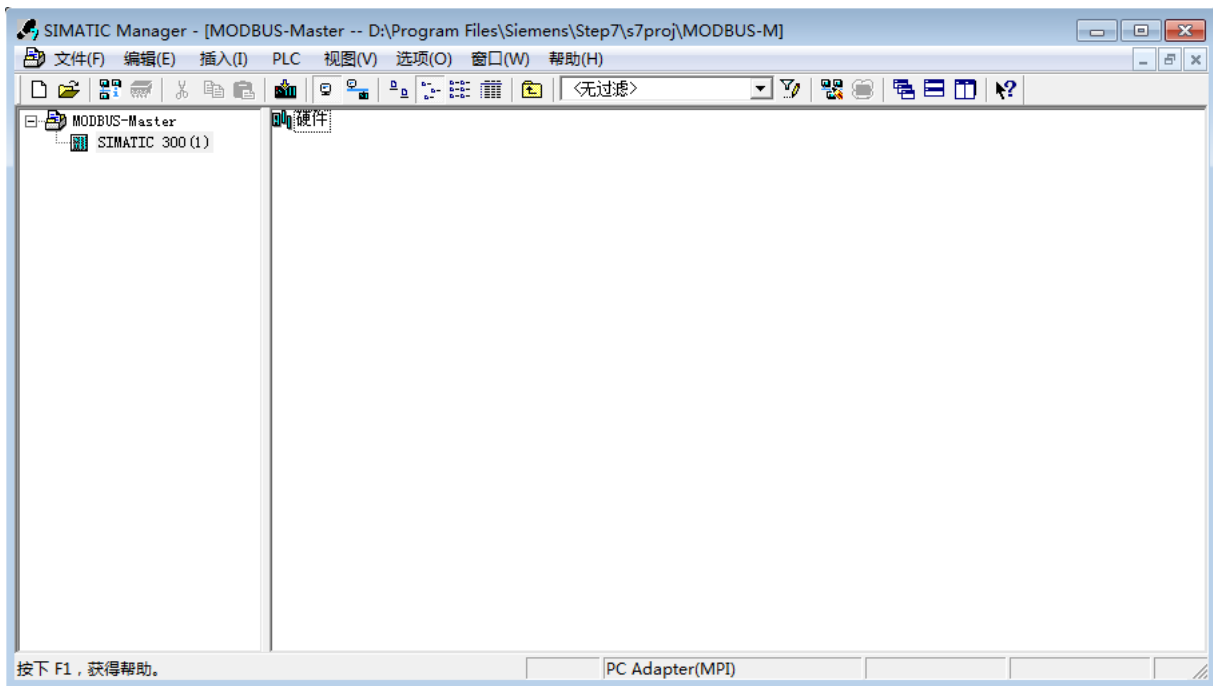


图 4-5

4.2 建立一个 PROFIBUS 总线

› 双击左键图 4-5 中的硬件打开“HW Config”硬件配置窗口。点击菜单栏中的“选项->更新目录”，将 GSD 文件 BC-MSV10.gsd 和 BC-MMV10.gsd 文件加入软件的目录中。如图 4-6 所示。

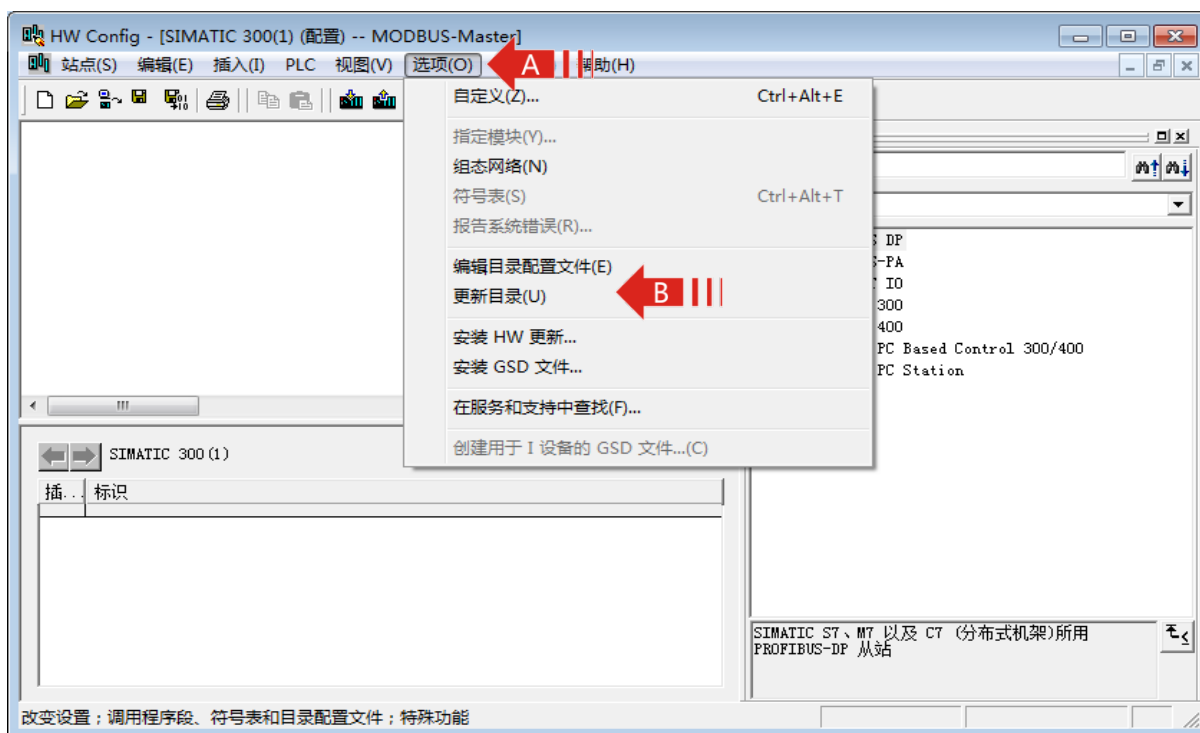


图 4-6

在右边的设备目录栏中出现了 PBMB-M-V1.0 和 PBMB-S-V1.0 的两个设备，PBMB-M-V1.0 设备为 MODBUS 接口作为主站时的工作模式，PBMB-S-V1.0 的设备为 MODBUS 接口作为从站时的工作模式。如图 4-7 所示。

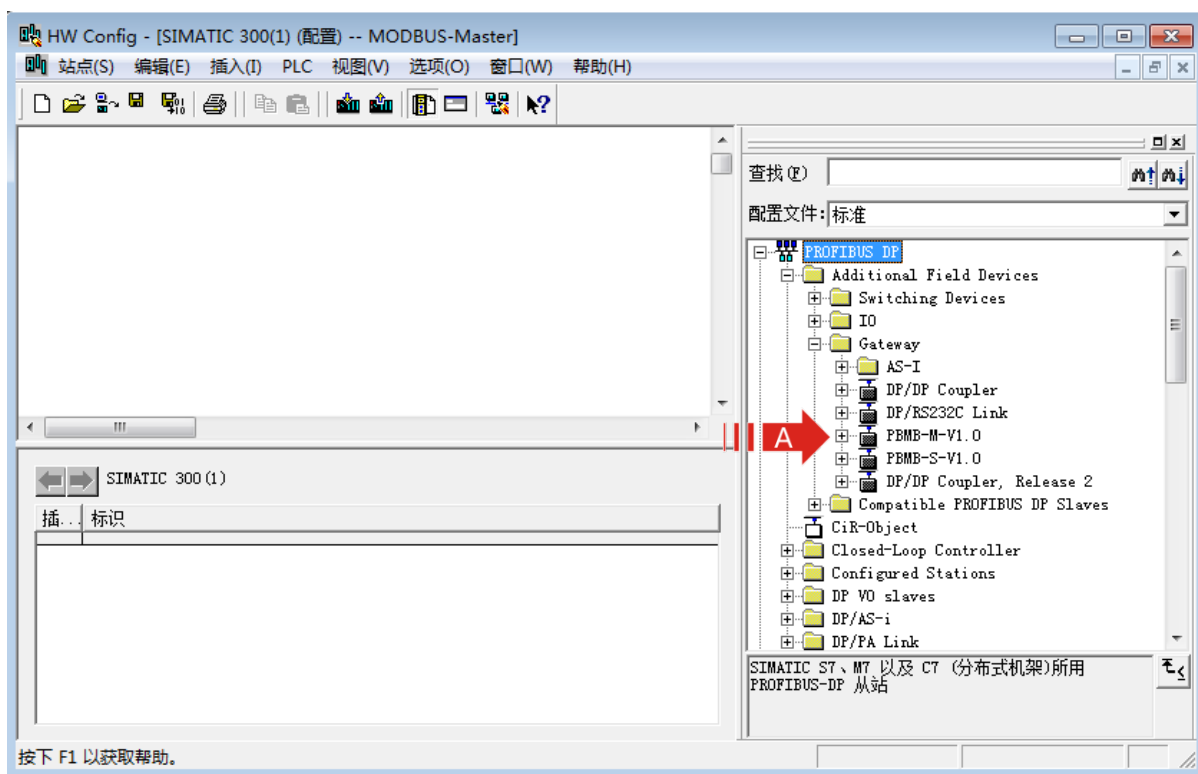


图 4-7

› 添加安装导轨,双击右侧目录栏中的 SIMATIC 300->RACK-300->Rail。如图 4-8 所示。

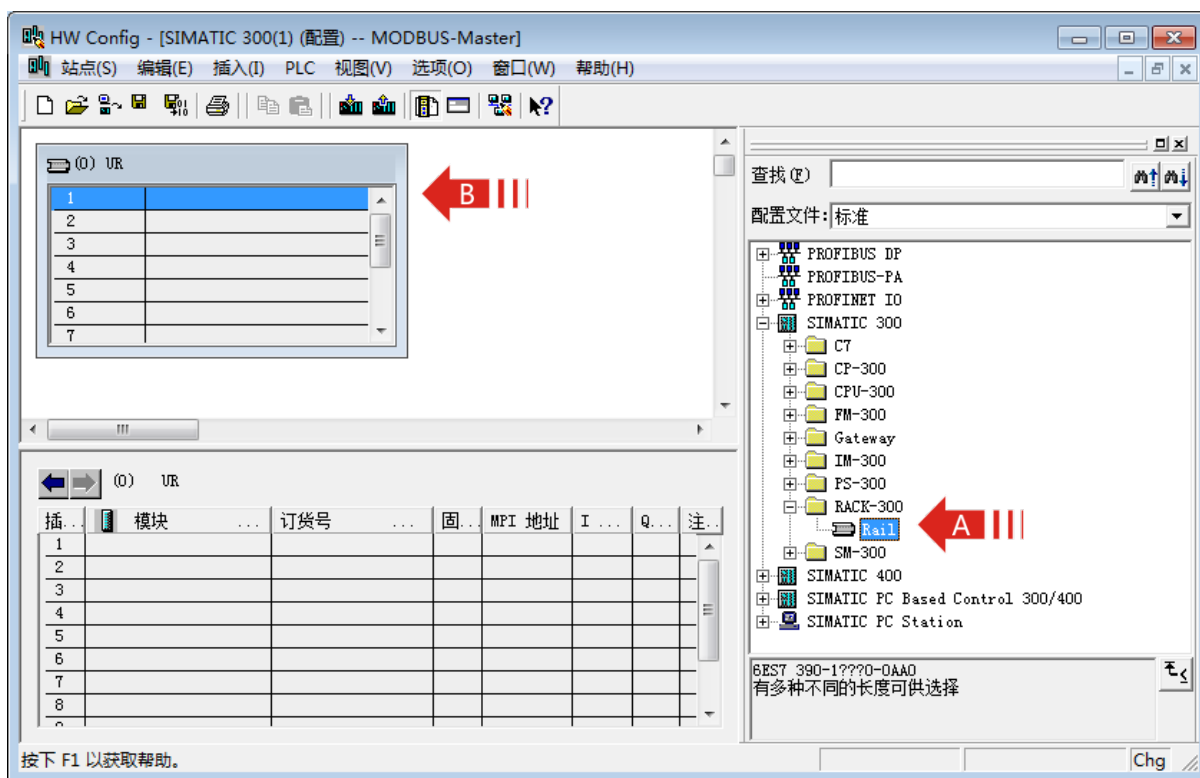


图 4-8

› 添加一个 CPU 模块。首先单击左栏“UR”中的 2 槽。然后双击右侧目录栏中的 SIMATIC 300->CPU-300->CPU 315-2 DP->6ES7 315-2AH14-0AB0->V3.0(本工程使用 CPU 315-2 DP, 请根据实际使用的 CPU 进行选取)。如图 4-9 所示。

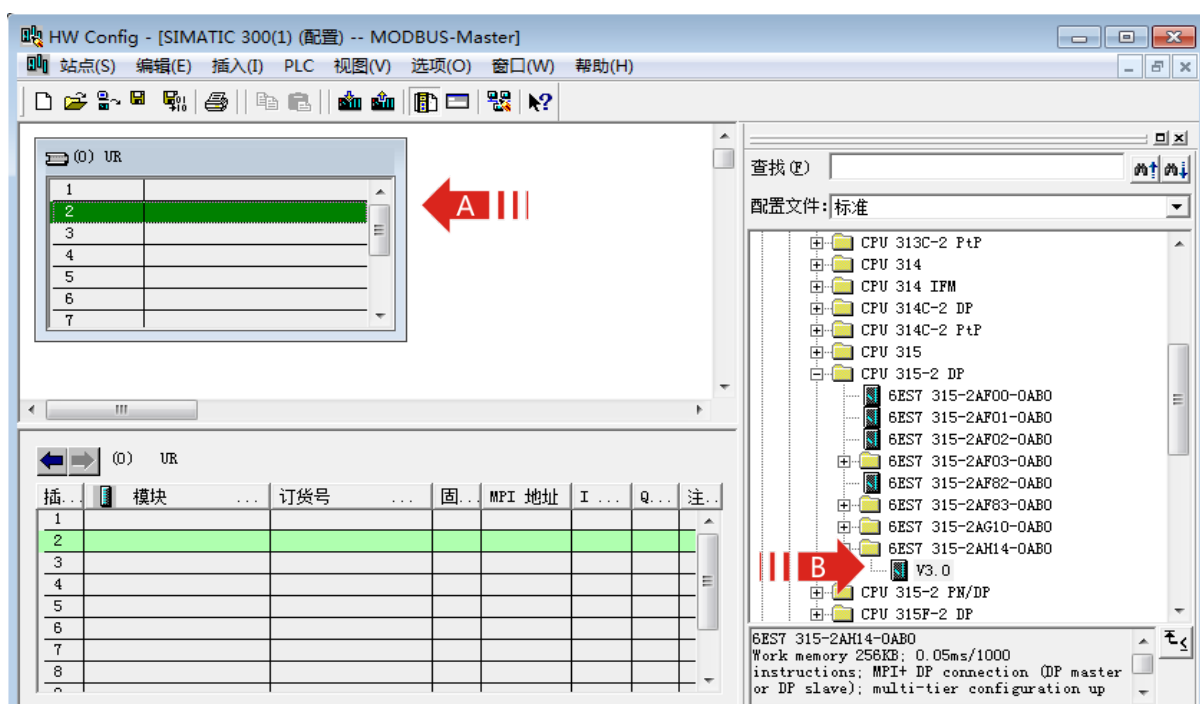


图 4-9

› 在出现的对话框中选择主站号 2 (默认), 如图 4-10 所示。

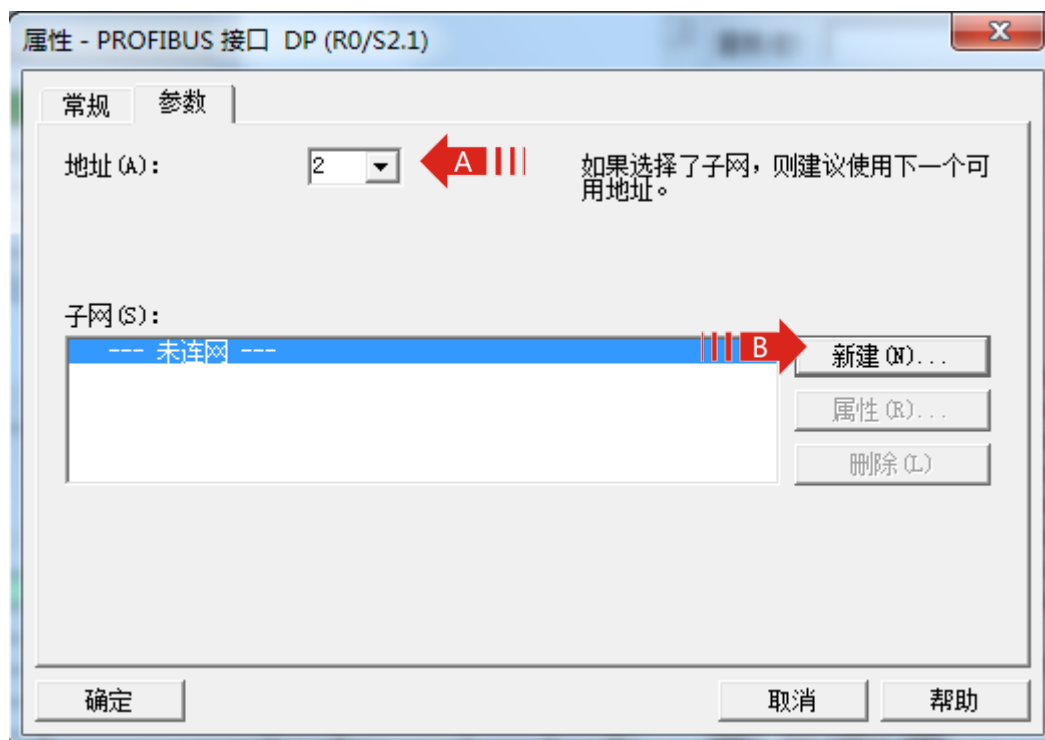


图 4-10

› 在图 4-10 中点击右侧的“新建(N)...”按钮, 出现如图 4-11 所示的“属性 - 新建子网 PROFIBUS”对话框, 选择“网络设置”选项卡, 并选择通信速率, 本例选择 1.5Mbps, 然后点击“确定”按钮。配置后的结果如图 4-12 所示。



图 4-11

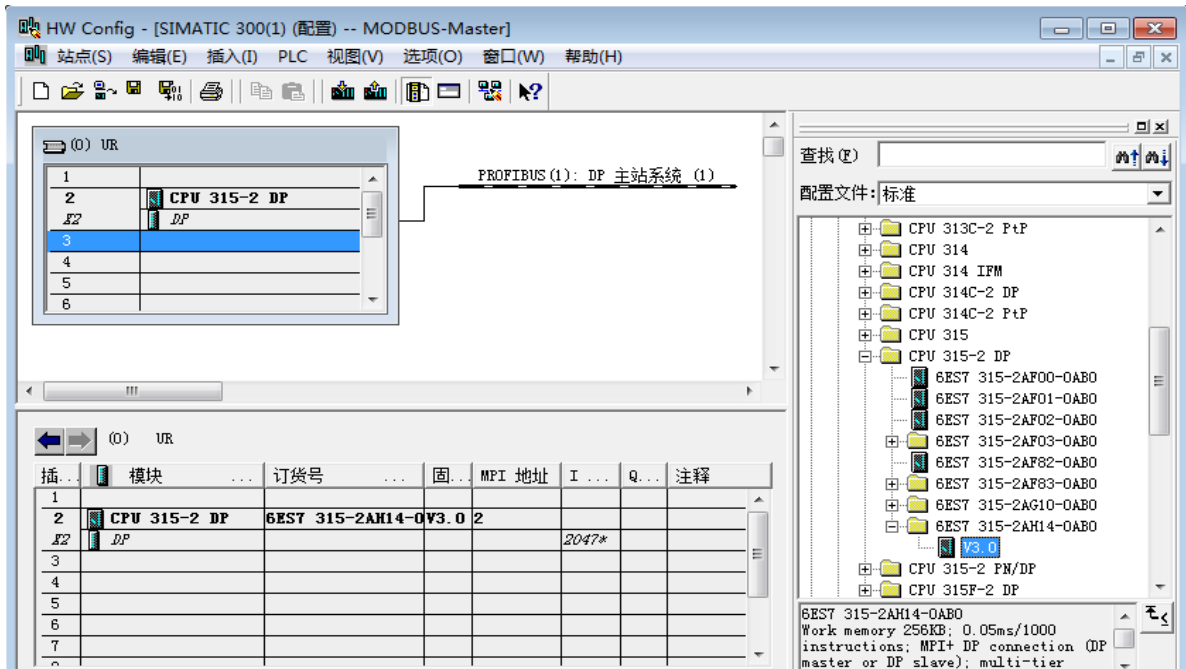


图 4-12

› 这样一个带 PROFIBUS 总线的 S7300 工程建立完成。

4.3 在项目中配置一个总线转换模块

› 点击图 4-13 中 “PROFIBUS(1): DP master system (1)” 下方的导轨，使其由黑白相间变为黑色实线。然后打开右侧目录栏中的 PROFIBUS DP->Additional Field Devices->Gateway->PBMB-M-V1.0, 双击 PBMB-M-V1.0, 出现 “属性 – PROFIBUS 接口 PBMB-M-V1.0” 对话框，选择从站地址，本例选择从站地址 6。如图 4-14 所示。然后点击确定。结果如图 4-15 所示。

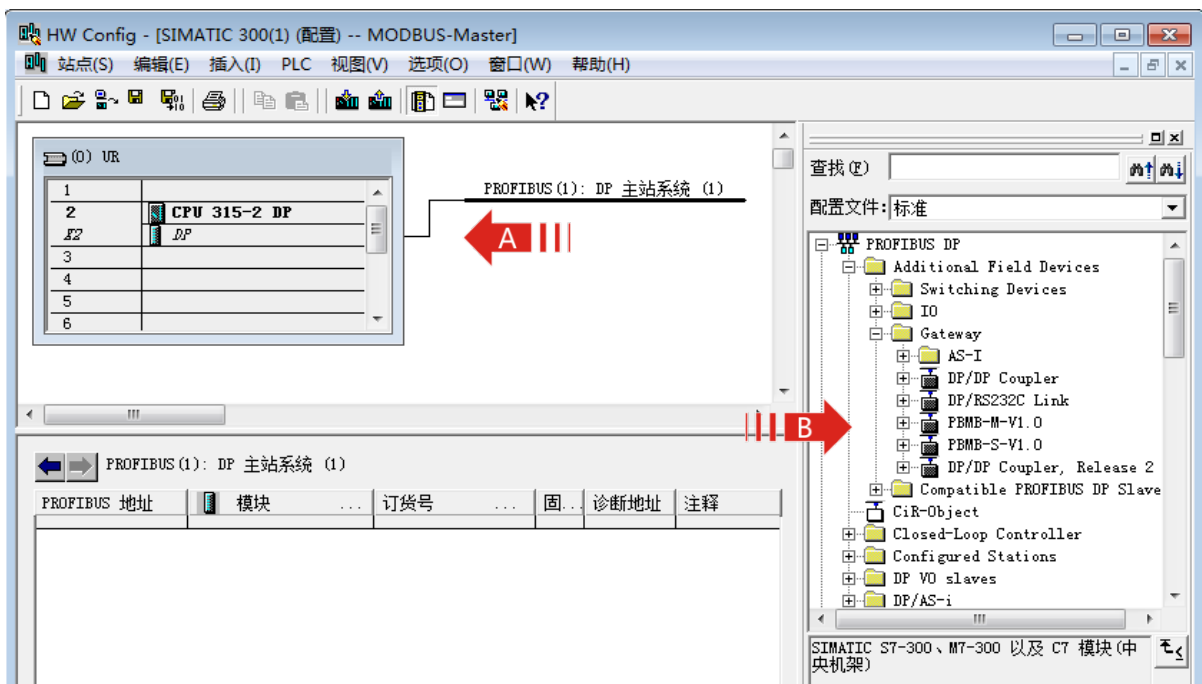


图 4-13

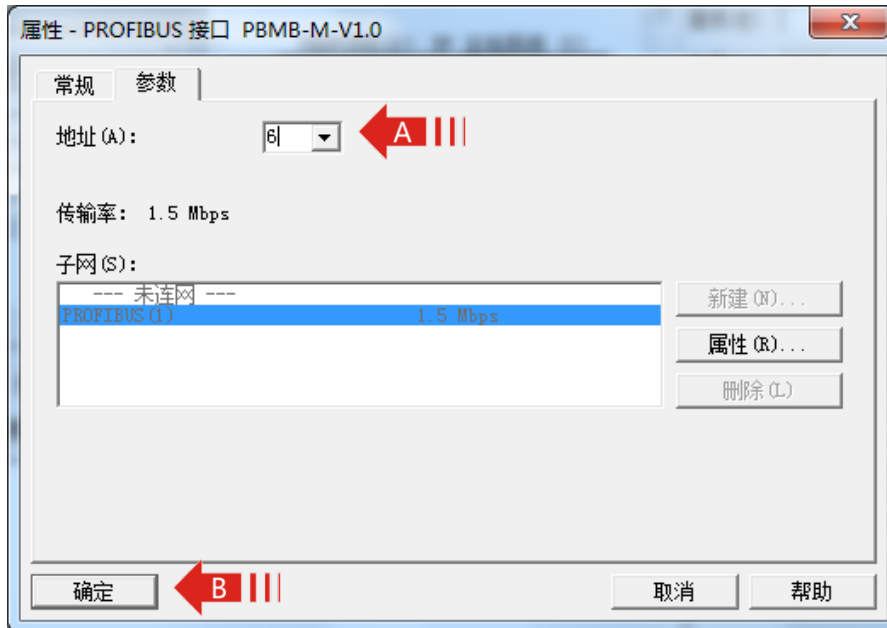


图 4-14

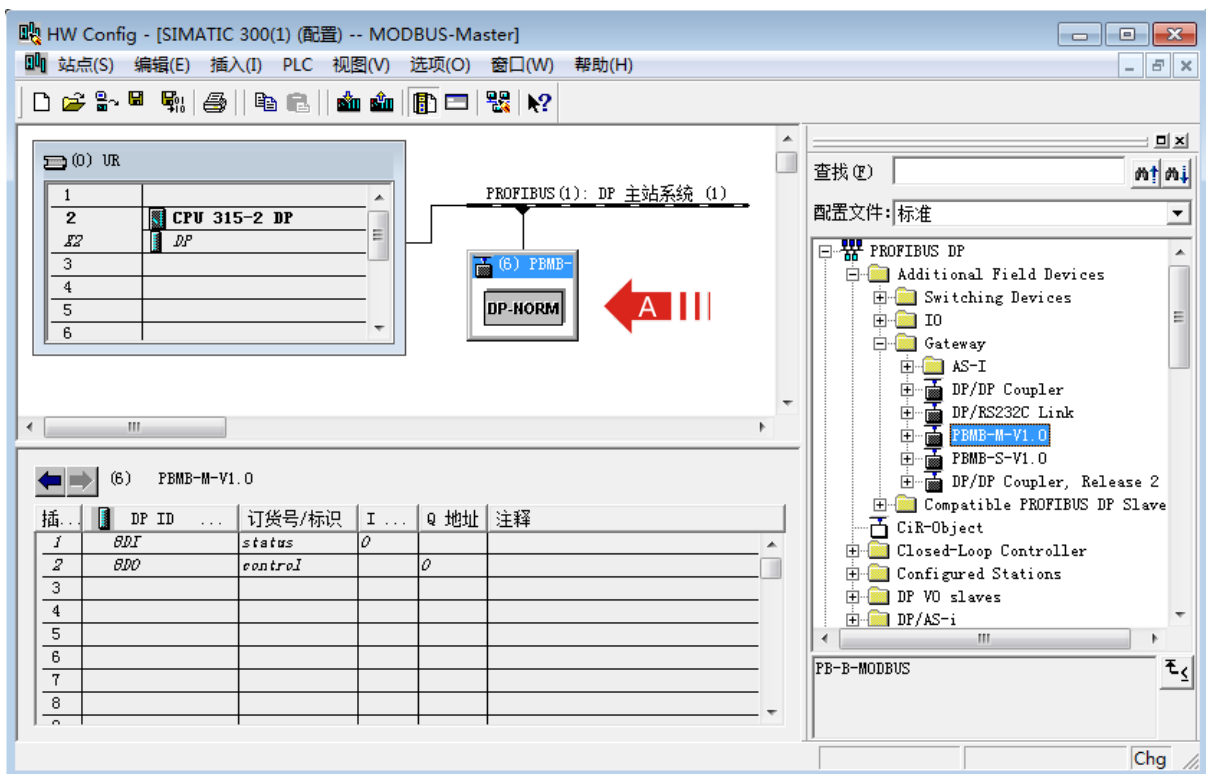


图 4-15

› 配置 MODBUS 接口属性：双击图中设备 PBMB-M-V1.0，出现“属性 - DP 从站”对话框，单击“分配参数”选项卡，这个选项卡主要配置了 MODBUS 接口的通讯参数，如图 4-16 所示。

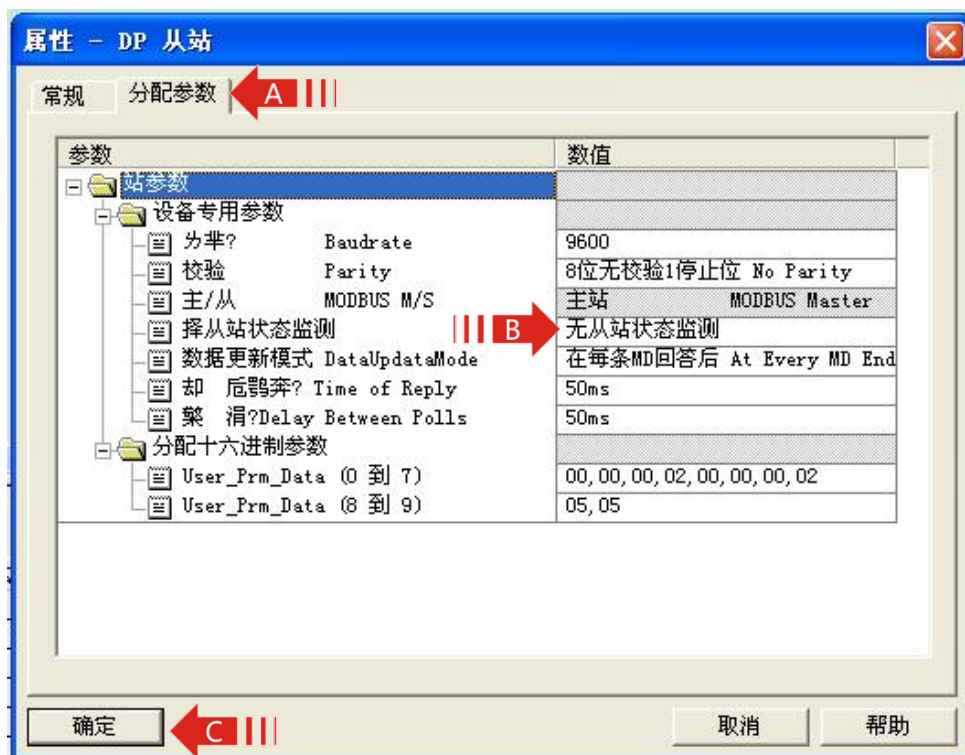


图 4-16

—选择波特率

单击“波特率 Baudrate”右侧的“数值”。

支持波特率范围：2400-115.2K。

本例中我们选择 9600。

—选择校验方式

单击“校验 Parity”右侧的“数值”。

支持“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”四种方式。

本例中我们选择“8位奇校验1停止位”。

—选择从站状态监测

单击“选择从站状态监测”右侧的“数值”。

可选项有“无从站状态监测”、“有从站状态监测（8位）”、“有从站状态监测（8字节）”、“有从站状态监测（16位）”、“有从站状态监测（16字节）”、“有从站状态监测（24位）”、“有从站状态监测（24字节）”、“有从站状态监测（32位）”、“有从站状态监测（32字节）”。

具体应用请参阅 4.7 对从站通讯状态检测。

—选择数据更新模式

更新模式由用户指定 PROFIBUS 数据区和 MODBUS 数据区之间何时进行数据交换。有两种方

式可选：

—在 MD 扫描结束后 At MD scan End：在 MODBUS 主站完成一次与所有 MODBUS 从站的通信之后进行 PROFIBUS 数据区和 MODBUS 数据区的数据更新。

—在每条 MD 回答后 At Every MD End：在 MODBUS 主站完成一次与一个 MODBUS 从站的通信之后进行 PROFIBUS 数据区和 MODBUS 数据区的数据更新。

本例中我们选择“在每条 MD 回答后 At Every MD End”。

—设置等待回答时间

单击“等待回答时间 Time of Reply”右侧的“数值”进行选择。

选择范围 10ms-1000ms 及无限期等待回答。这是总线转换模块发出 MODBUS 报文后等待 MODBUS 设备响应的的时间。若 MODBUS 设备在设定的等待回答时间内仍无响应，模块停止等待，继续发送下一条 MODBUS 报文。

在通常情况下选择典型值 100ms。

—查询间隔时间

单击“查询间隔 Delay Between Polls”右侧的“数值”进行选择。

选择范围 0ms-1500ms。这是总线转换模块接收到 MODBUS 从站回复的正确报文后，延时发送 MODBUS 主站报文的时间。若 MODBUS 从站设备响应主站报文较慢，如果总线转换模块发送 MODBUS 报文过快，那么会出现通信故障，可以适当增加发送报文间隔时间。

在通常情况下选择典型值 10ms。

4.4 配置 RBCM PBMB-04(02) 的 MODBUS 报文队列

› PBMB-M-V1.0 一共有 39 个槽,前两个槽分别作为状态字及控制字已被占用，剩下 37 个槽可供用户使用。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 个 MODBUS 通信模块(报文)。单击右侧目录栏中的 PROFIBUS DP->Additional Field Devices->Gateway->PBMB-M-V1.0 左侧的加号,使其目录展开。PBMB-M-V1.0 的每一个 MODBUS 模块对应一种功能的 MODBUS 报文,可先单击要使用的槽,然后双击右侧目录栏中 PBMB-M-V1.0 列出的目录中的一项,使其插入某一槽中。如图 4-17。模块的功能介绍如表 4-1。

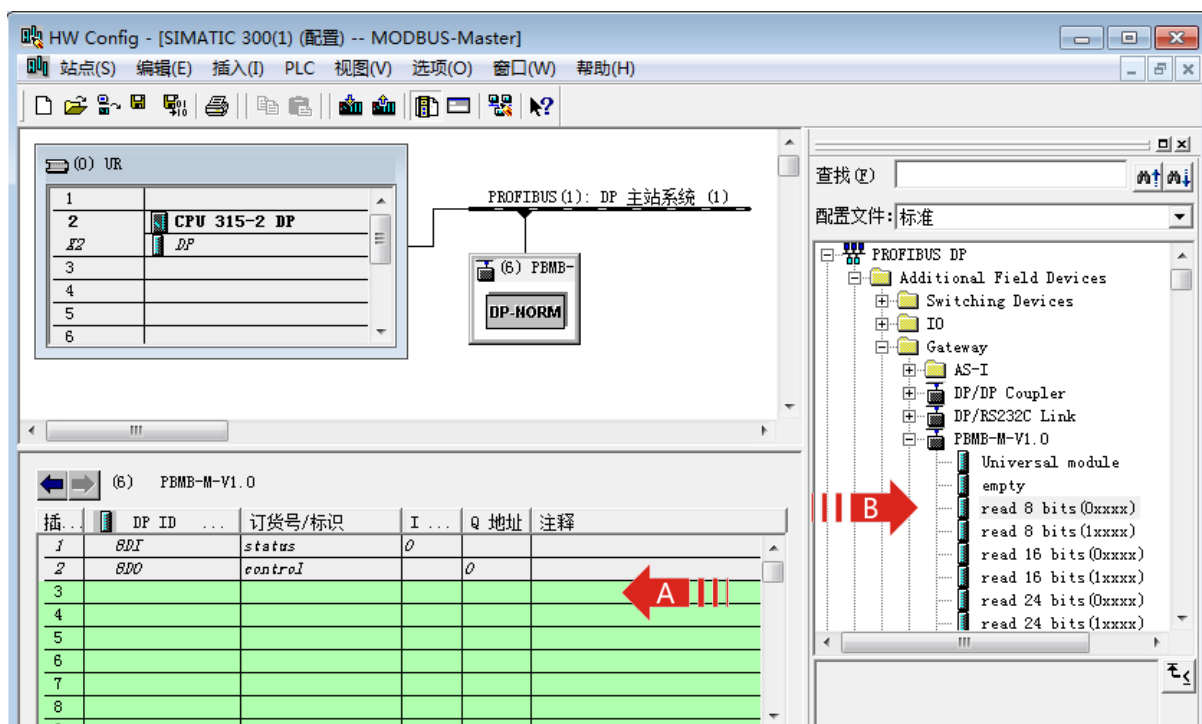


图 4-17

表 4-1 PBMB-M-V1.0 模块功能介绍

模块	对应 MODBUS 报文功能及存储区	可配置参数
read N bits (0xxxx) N=8~256	01H 功能 读取 N 个输出线圈 0xxxx 状态	1. MODBUS 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 N bits (1xxxx) N=8~256	02H 功能 读取 N 个输入线圈 1xxxx 状态	1. MODBUS 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 N Words (4xxxx) N=1~60	03H 功能 读 N 个保持寄存器 4xxxx 的值	1. MODBUS 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 N Words (3xxxx) N=1~60	04H 功能 读 N 个输入寄存器 3xxxx 的值	1. MODBUS 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 N bits (0xxxx) N=8~256	0FH 功能 将 N 个连续线圈 0xxxx 强置为 ON/OFF 状态。	1.MODBUS 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 N Words (4xxxx) N=1~60	10H 功能 预置从站 N 个保持寄存器 4xxxx 值。	1.MODBUS 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 Command)	05h 功能 强置单线圈 0xxxx 值。	1.MODBUS 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 Command)"	06h 功能 预置单保持寄存器 4xxxx 值。	1.MODBUS 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);

4.5 MODBUS 报文详解

› 本节举例说明总线转换模块所支持的 MODBUS 报文的配置方法

槽号	模块名称	PROFIBUS 地址	MODBUS 地址	MODBUS 命令
1	status	IB0		诊断 MODBUS 通讯的状态
2	control	QB0		控制 MODBUS 通讯
3	read 24 bits (0xxxx)	IB1 ~ IB3	站号:1 00020 ~ 00043	发 01H 命令读线圈 00020 ~ 00043 , 存入 IB1 ~ IB3
4	read 8 bits (1xxxx)	IB4	站号:2 10015 ~ 10022	发 02H 命令读输入线圈 10015 ~ 10022 , 存入 IB4
5	read 4words (4xxxx)	PIW256 ~ PIW262	站号:3 40001 ~ 40004	发 03H 命令读保持寄存器数据 40001 ~ 40004 , 存入 PIW256 ~ PIW262
6	read 6words(3xxxx)	PIW264 ~ PIW274	站号:4 30100 ~ 30105	发 04H 命令读输入寄存器数据 30100 ~ 30105 , 存入 PIW264 ~ PIW274
7	write8bits(0xxxx)	QB1	站号:5 00010 ~ 00017	发 0FH 命令 , 将 QB1 强置给线圈 00010 ~ 00017
8	write10 words (4xxxx)	PQW256 ~ PQW274	站号:6 40010 ~ 00019	发 10H 命令 , 将 PQW256 ~ PQW274 写入保持寄存器 40010 ~ 00019
9	force single bit(05h Command)	QB2	站号:7 00001	发 05H 命令 , 根据 Q2.0 置线圈 00001

10	set single word(06h Command)	PQW276	站号:8 40001	发06H 命令, 将PQW276置入保持寄存器40001
11	MODBUS 从站状态表 (8 字节)	IB5 ~ IB12		8 个 MODBUS 从站通讯状态字

4.5.1 功能 01H-读取 N 个输出线圈 0xxxx 状态

› 本例概述

读取站号为 1，MODBUS 设备地址为 00020 ~ 00043 的线圈状态，将读取的线圈状态存放到 plc 地址为 IB1、IB2、IB3 中，读取数量为 24 个 Bits。

› 插入模块。

单击 3 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “read 24 bits(0xxxx)”，如图 4-18。其中的 I 地址一栏中的 “1...3” 表示从站返回的 24bits 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中 “IB1、IB2、IB3” 地址。

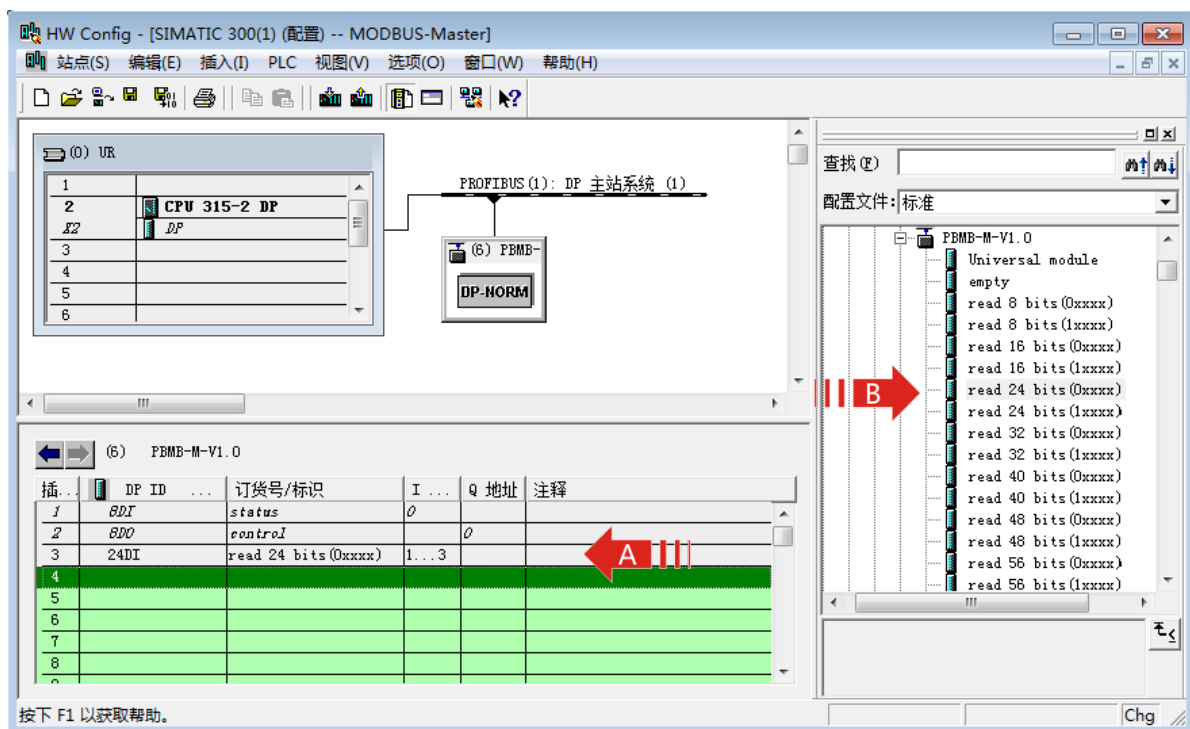


图 4-18

› 设定模块的详细参数。

双击 3 号槽中的模块 “24DIread 24 bits(0xxxx) 1...3”，打开 “属性 – DP 从站” 对话框。选择对话框中的 “分配参数” 选项卡。进行从站地址和起始地址的设置。如图 4-19 所示。

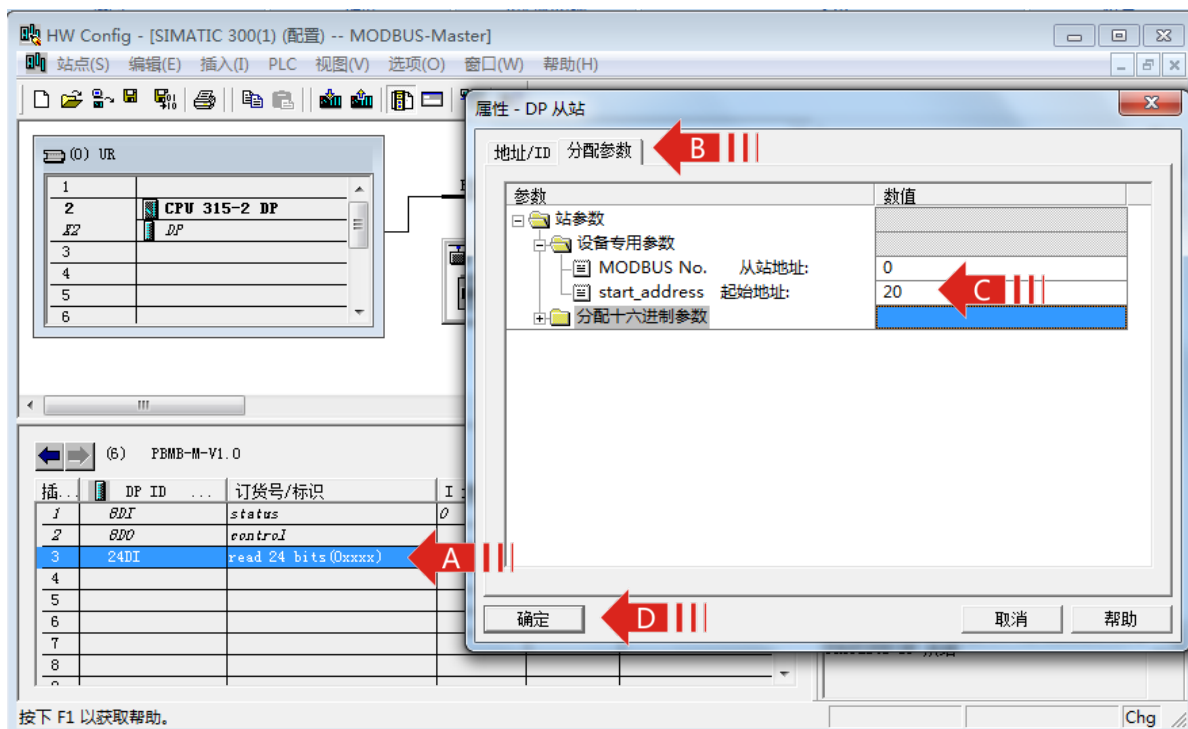


图 4-19

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 1。

注：从站地址不能设定为 0。

—起始地址：要读取的 00020 区的起始地址，终止地址为 00043，数量为 24 个。

› PROFIBUS 地址与 MODBUS 地址对应关系

IB1..IB3 是 PROFIBUS 主站分配给这个 MODBUS 模块的 PROFIBUS 输入地址 IB1~IB3，对应本 MODBUS 报文读到设备地址 00020~00043 共 24 bits，如图 4-20 所示。

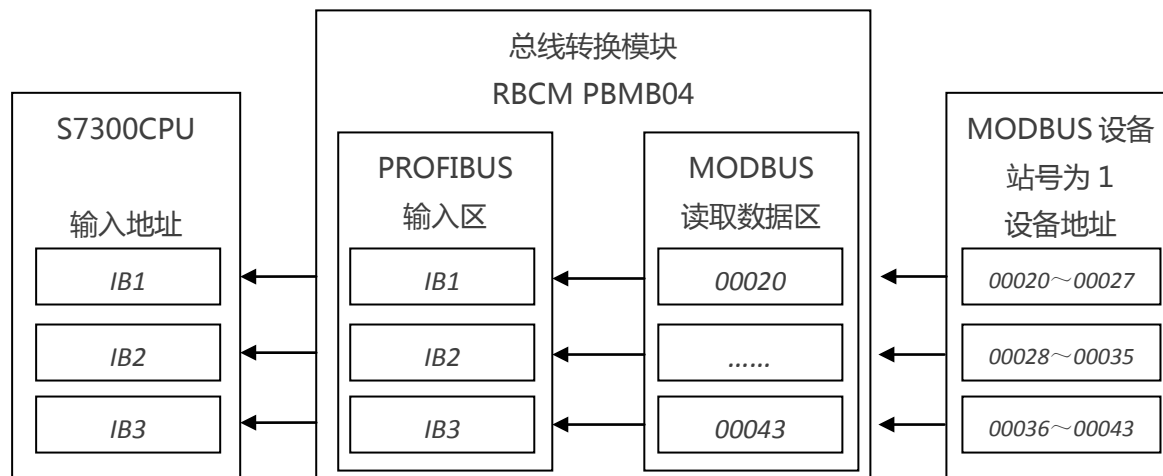


图 4-20

4.5.2 功能 02H-读取 N 个输入线圈 1xxxx 状态

› 本例概述

读取站号为 2，MODBUS 设备地址为 10015 ~ 10022 的线圈状态，将读取的线圈状态存放到 plc 地址为 IB4 中，读取数量为 8 个 Bits。

› 插入模块。

单击 4 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “read 8 bits(1xxxx)” ，如图 4-21。其中的 I 地址一栏中的 “4” 表示从站返回的 8bits 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中 “IB4” 地址。

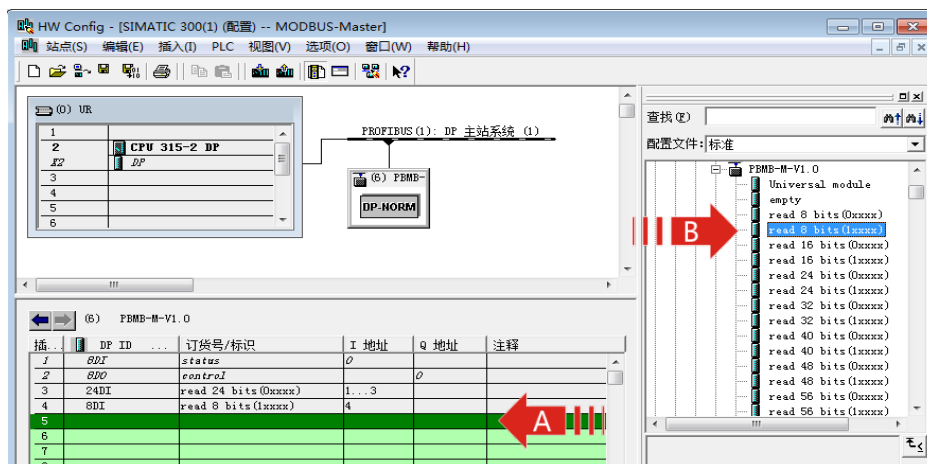


图 4-21

› 设定模块的详细参数。

双击 4 号槽中的模块 “8DI read 8 bits(1xxxx)4”，打开 “属性 - DP 从站” 对话框。选择对话框中的 “分配参数” 选项卡。进行从站地址和起始地址的设置。如图 4-22 所示。

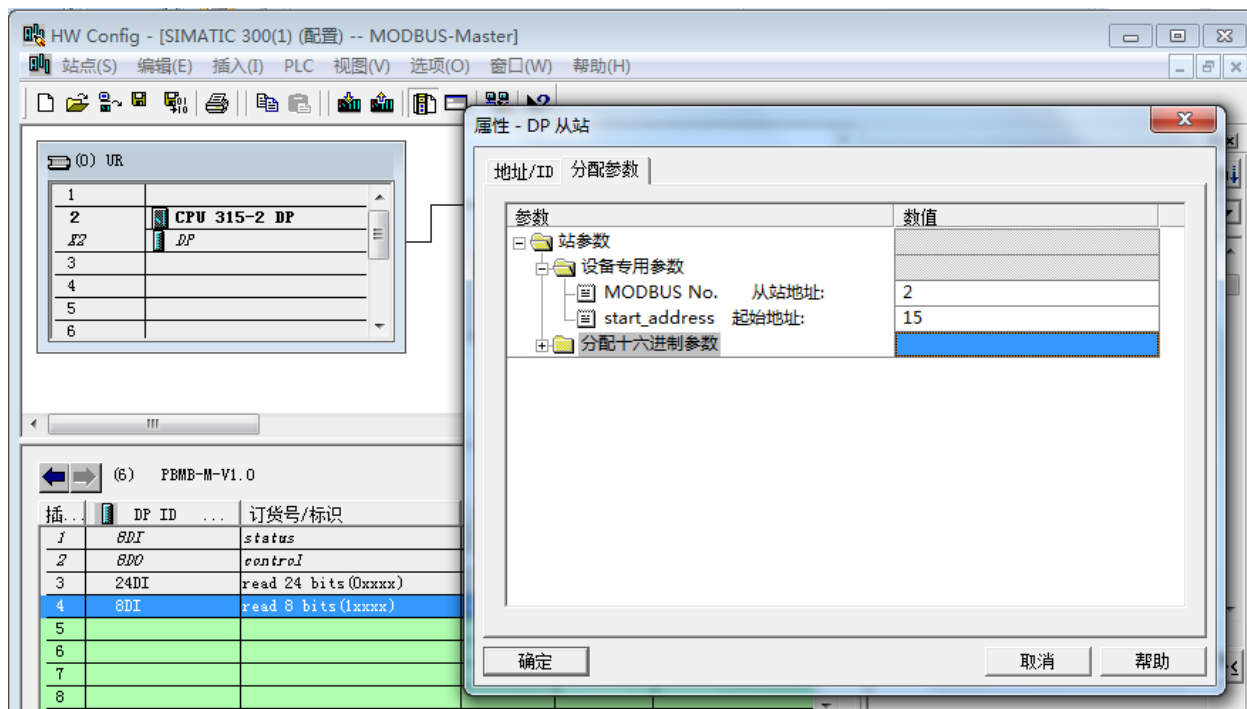


图 4-22

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 2。

注：从站地址不能设定为 0。

—起始地址：要读取的 10015 区的起始地址，终止地址为 10022，数量为 8 个。

› PROFIBUS 地址与 MODBUS 地址对应关系

IB4是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应本MODBUS 报文读到设备地址10015 ~ 10022共8bits，如图4-23所示。

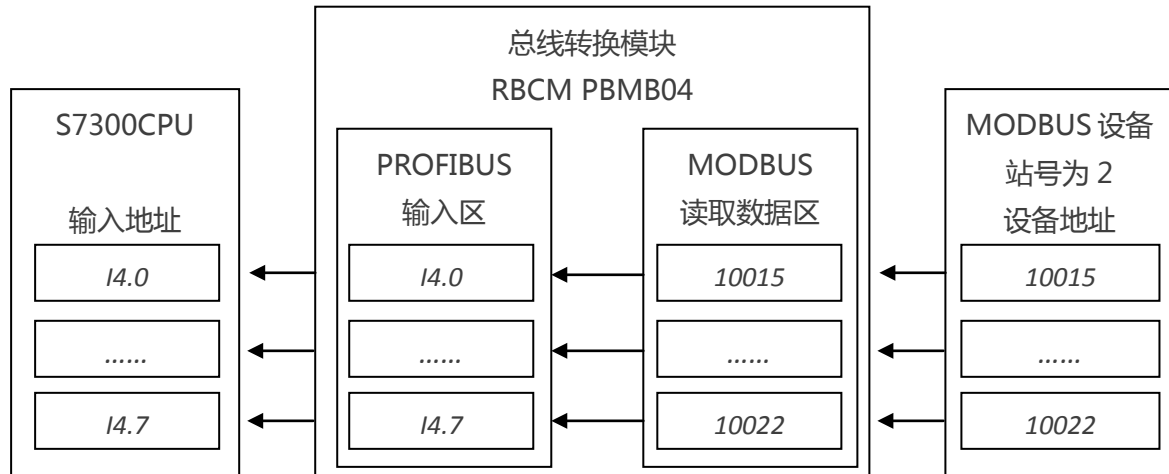


图4-23

4.5.3 功能 03H -读取 N 个保持寄存器 4xxxx 数据

› 本例概述

读取站号为 3，MODBUS 设备地址为 40001 ~ 40004 的保持寄存器数据，将读取的数据存放到 plc 地址为 PIW256 至 PIW262 中，读取数量为 4 个 Words。

› 插入模块。

单击 5 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “read 4words(4xxxx)”，如图 4-24。其中的 I 地址一栏中的 “256...263” 表示从站返回的 4 Words 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中 “PIW256 至 PIW262” 地址。

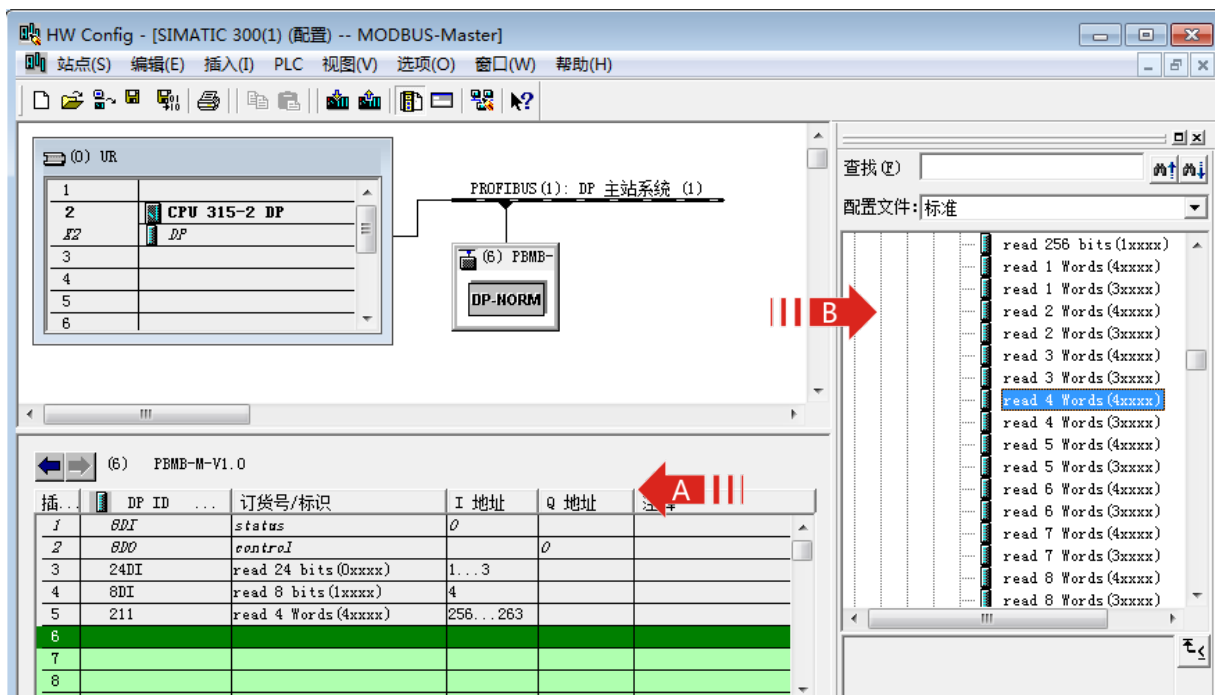


图 4-24

› 设定模块的详细参数。

双击 5 号槽中的模块 “211 read 4 Words(4xxxx) 256...263”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-25 所示。

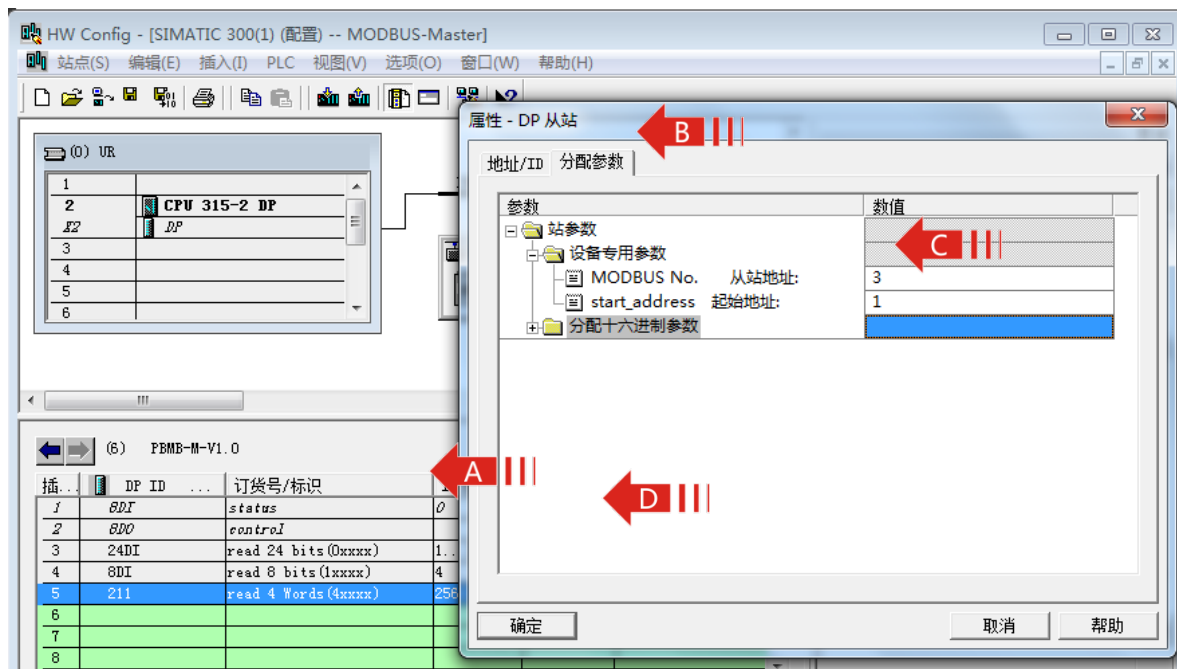


图 4-25

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 3。

注：从站地址不能设定为 0。

—起始地址：要读取的 40001 区的起始地址，终止地址为 40004，数量为 4 个。

› PROFIBUS 地址与 MODBUS 地址对应关系

IB256至IB263是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应本MODBUS 报文读到设备地址40001 ~ 40004共4words，如图4-26所示。

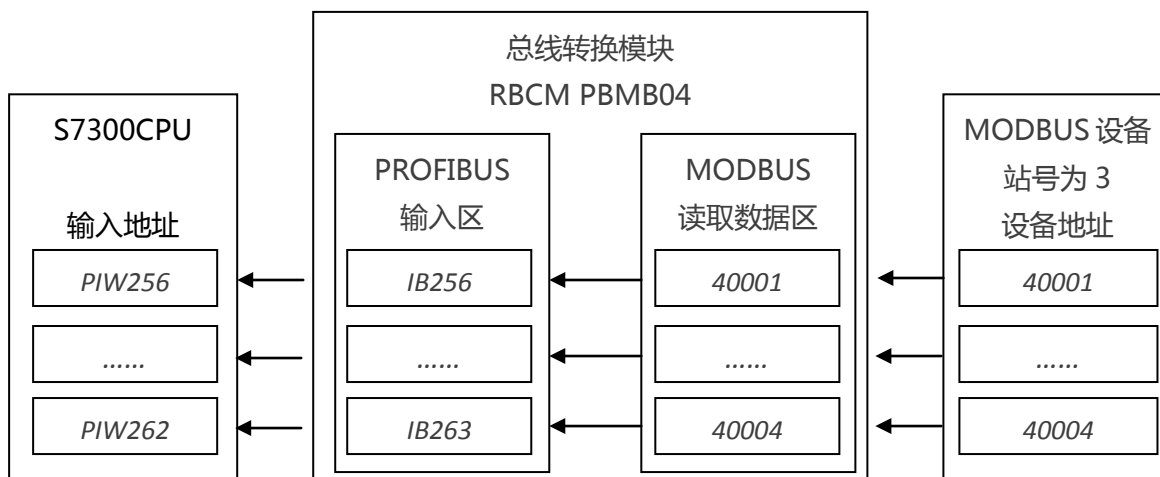


图4-26

4.5.4 04H 功能-读取 N 个输入寄存器 3xxxx 数据

› 本例概述

读取站号为 4，MODBUS 设备地址为 30100 ~ 30105 的输入寄存器数据，将读取的数据存放到 plc 地址为 PIW264 至 PIW274 中，读取数量为 6 个 Words。

› 插入模块。

单击 6 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “read 6words(3xxxx)”，如图 4-27。其中的 I 地址一栏中的 “264...275” 表示从站返回的 6 Words 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中 “PIW264 至 PIW274” 地址。

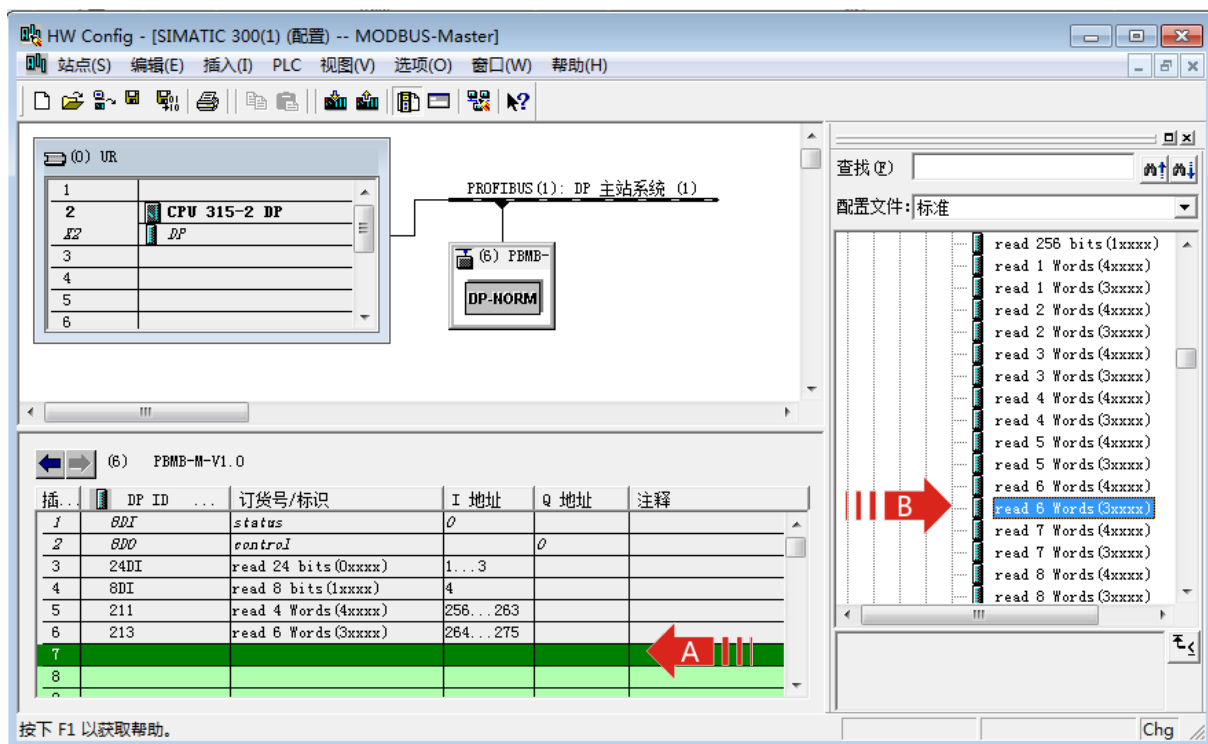


图 4-27

› 设定模块的详细参数。

双击 6 号槽中的模块 “213 read 6Words(3xxxx) 264...275”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-28 所示。

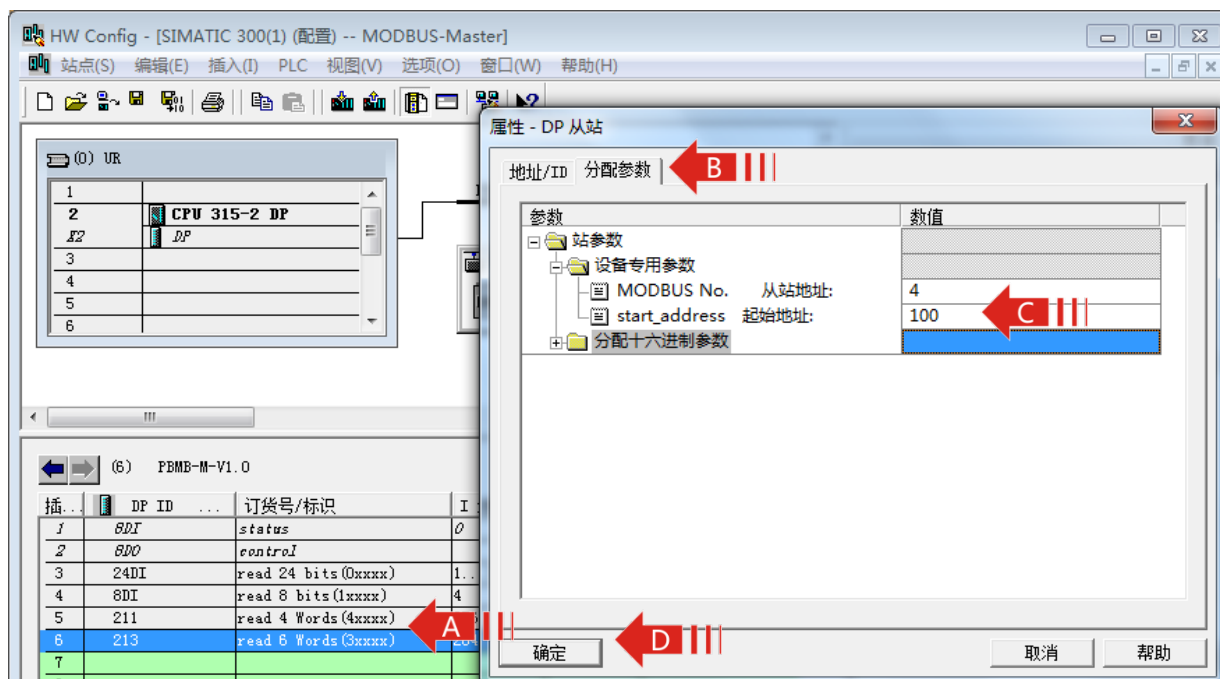


图 4-28

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 4。

注：从站地址不能设定为 0。

—起始地址：要读取的 30100 区的起始地址，终止地址为 30105，数量为 6 个。

› PROFIBUS 地址与 MODBUS 地址对应关系

IB264至IB275是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应本 MODBUS 报文读到设备地址30100 ~ 30105共6words，如图4-29所示。

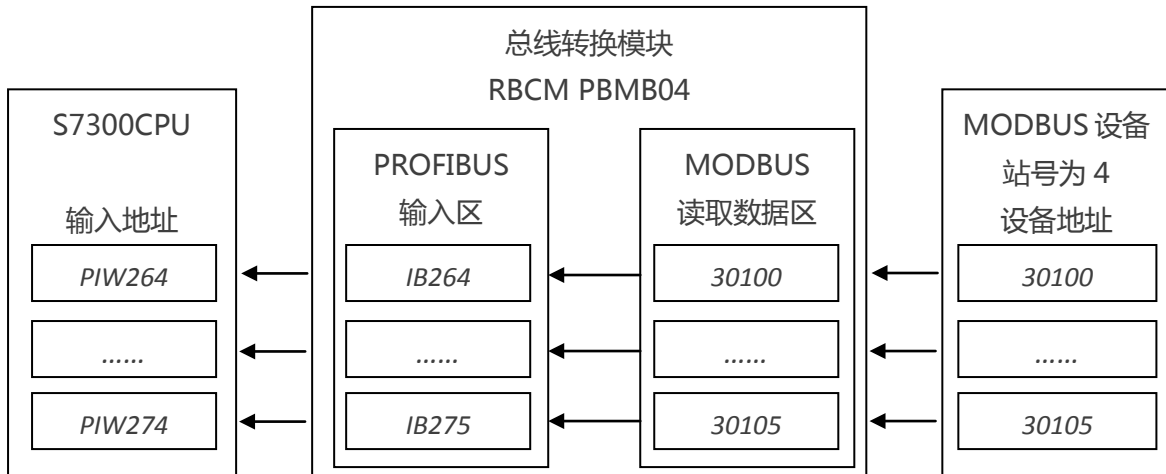


图4-29

4.5.5 0FH 功能-强置 N 个线圈 0xxxx 状态

› 本例概述

将 plc 地址为 QB1 中线圈状态强置给站号为 5 ,MODBUS 设备地址为 00010 ~ 00017 的线圈，强置数量为 8 个 Bits。

› 插入模块

单击 7 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “write8bits(0xxxx)”，如图 4-30。其中的 Q 地址一栏中的 “1” 表示从站强置数据，S7-300/CPU215-2DP 中 “Q1.0 至 Q1.7” 的线圈状态将会通过本总线转换模块发送至地址 00010 ~ 00017 中。

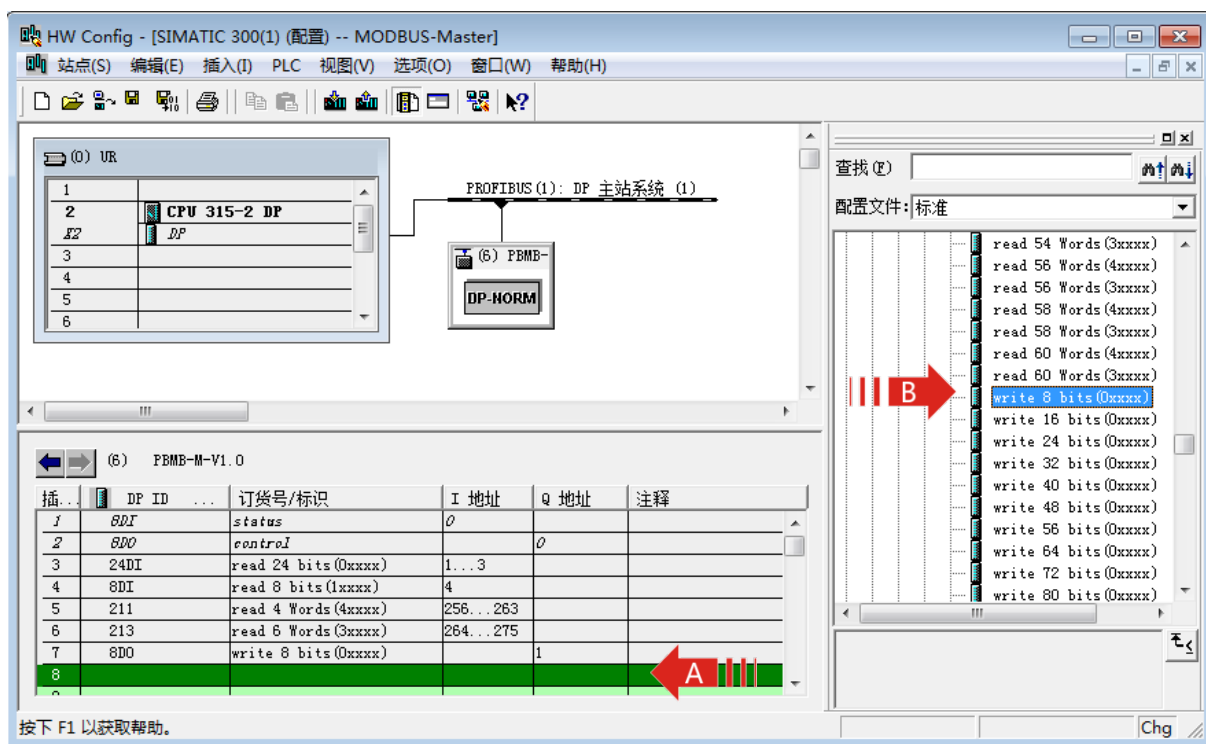


图 4-30

› 设定模块的详细参数。

双击 7 号槽中的模块 “8DO write 8 bits(0xxxx) 1”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-31 所示。

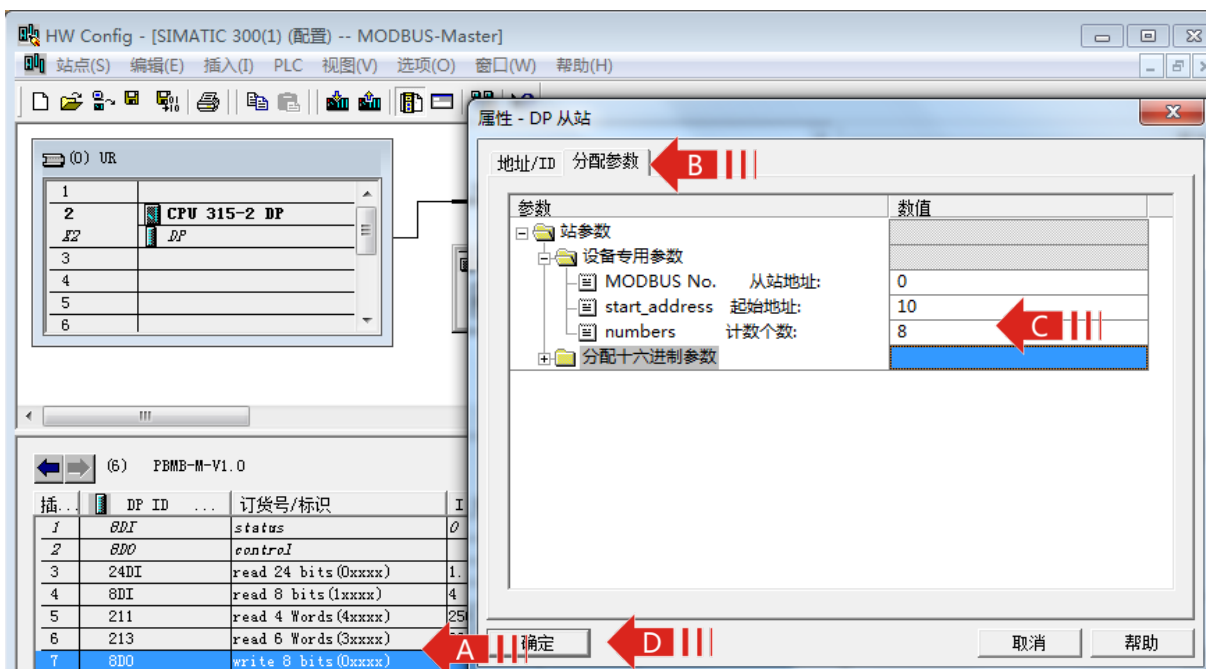


图 4-31

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 5。

注：从站地址不能设定为 0。

—起始地址：要读取的 00010 区的起始地址，终止地址为 00017，数量为 8 个。

—计数个数：写入 0XXXX 区中的 bit 个数。本例为 8。

› PROFIBUS 地址与 MODBUS 地址对应关系

QB1是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应本MODBUS 报文读到设备地址00010 ~ 00017共8bits，如图4-32所示。

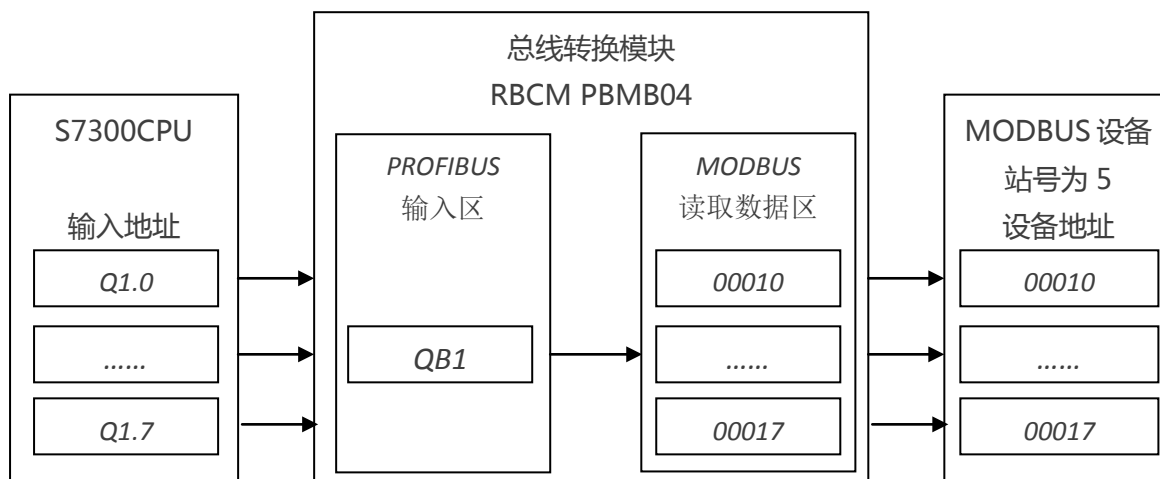


图4-32

4.5.7 功能 10H-预置 N 个保持寄存器 4xxxx 数据

› 本例概述

将 plc 地址为 PQW256 至 PQW274 中的数据写入站号为 6，MODBUS 设备地址为 40010 ~ 00019 的寄存器中，写入数量为 10 个 Words。

› 插入模块

单击 8 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “write10 words (4xxxx)”，如图 4-33。其中的 Q 地址一栏中的 “256...275” 表示 S7-300/CPU215-2DP 中 “QB256-QB275” 地址的数据，将会通过本总线转换模块发送至从站 40010 ~ 00019 地址中，共 10 个 Words。

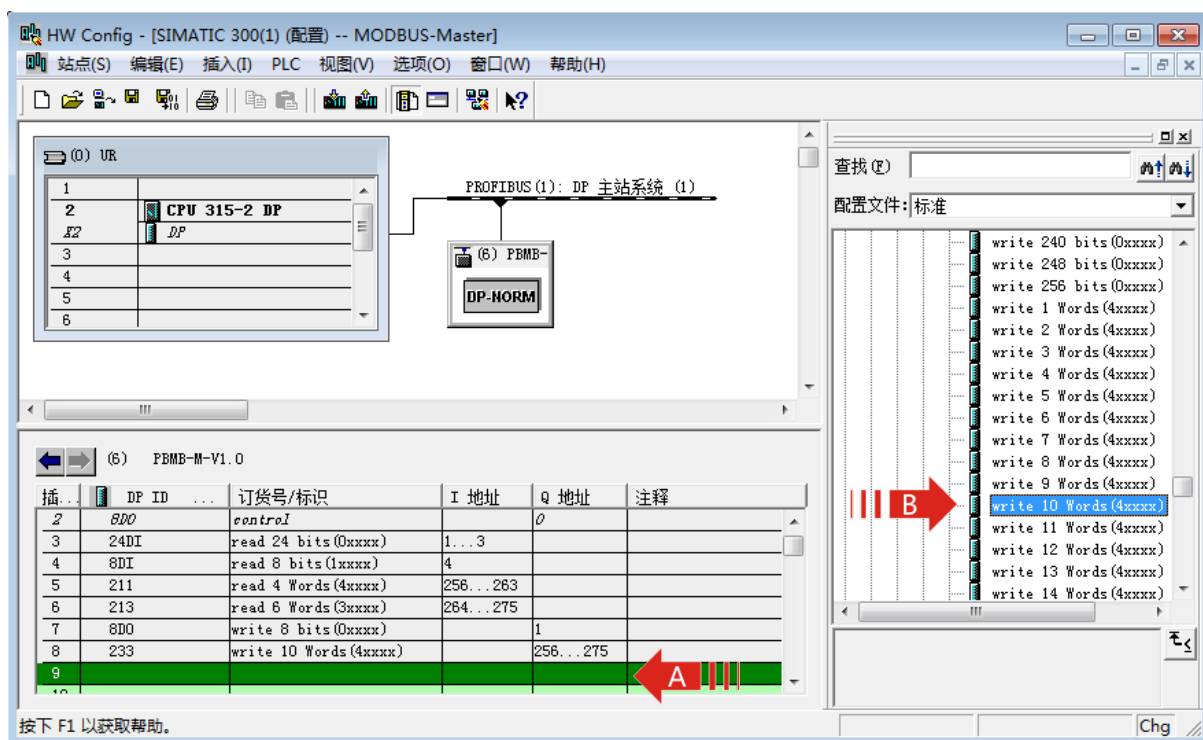


图 4-33

› 设定模块的详细参数。

双击 8 号槽中的模块 “233 write 10Words(4xxxx) 256...275”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-34 所示。

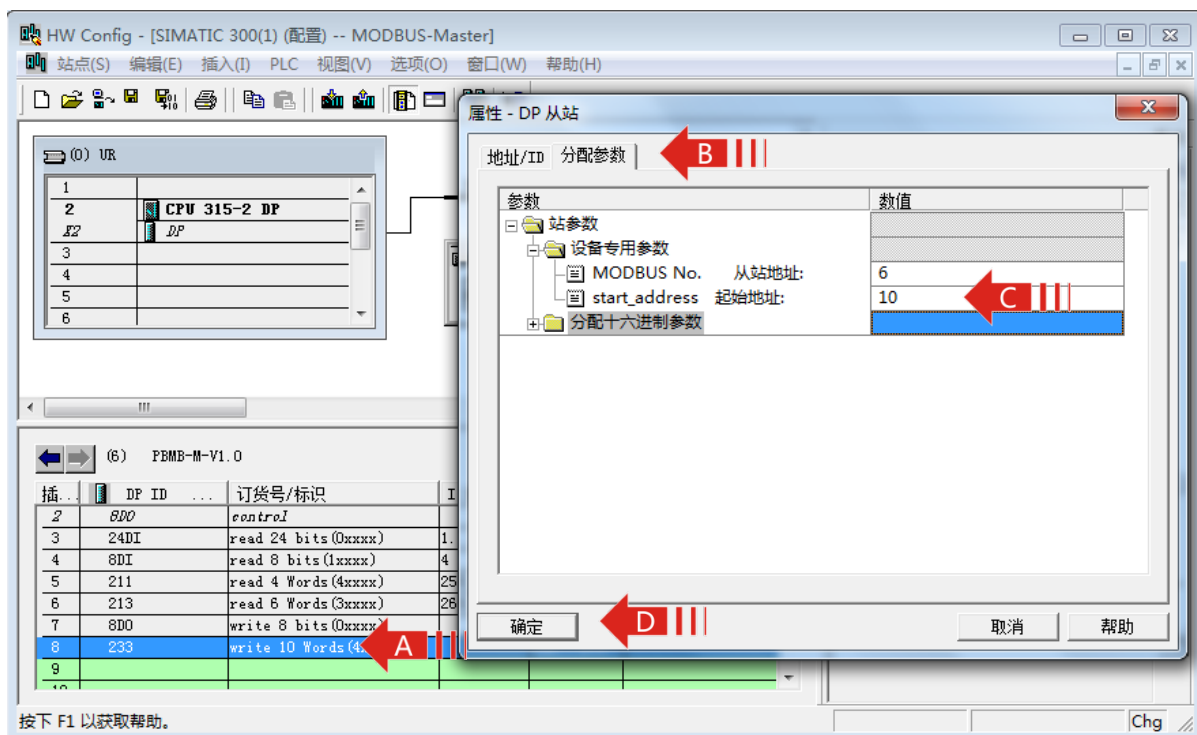


图 4-34

— 从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 6。

注：从站地址不能设定为 0。

— 起始地址：要读取的 40010 区的起始地址，终止地址为 00019，数量为 10 个。

› PROFIBUS 地址与 MODBUS 地址对应关系

QB256至QB275是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应本MODBUS 报文读到设备地址40010~40019共10Words，如图4-35所示。

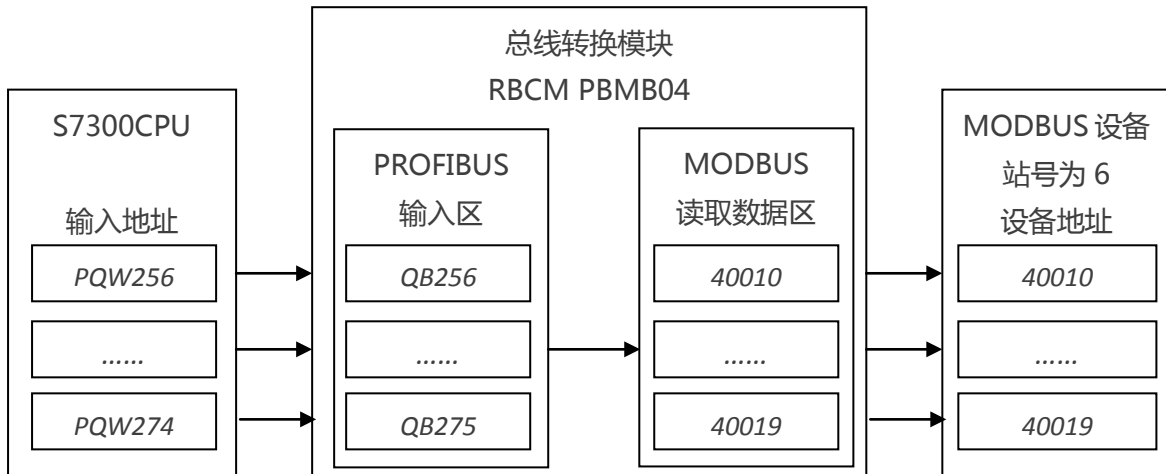


图4-35

4.5.8 05H 功能-强置单个线圈 0xxxx 状态

› 本例概述

将 plc 地址为 QB2 中线圈状态强置给站号为 7，MODBUS 设备地址为 00001 的线圈，强置数量为 1 个 Bits。

› 插入模块

单击 9 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “force single bit(05h Command)”，如图 4-36。其中的 Q 地址一栏中的 “2” 表示从站强置数据，S7-300/CPU215-2DP 中 “Q2.0 至 Q2.7” 的线圈状态将会通过本总线转换模块发送至线圈地址为 00001 中。

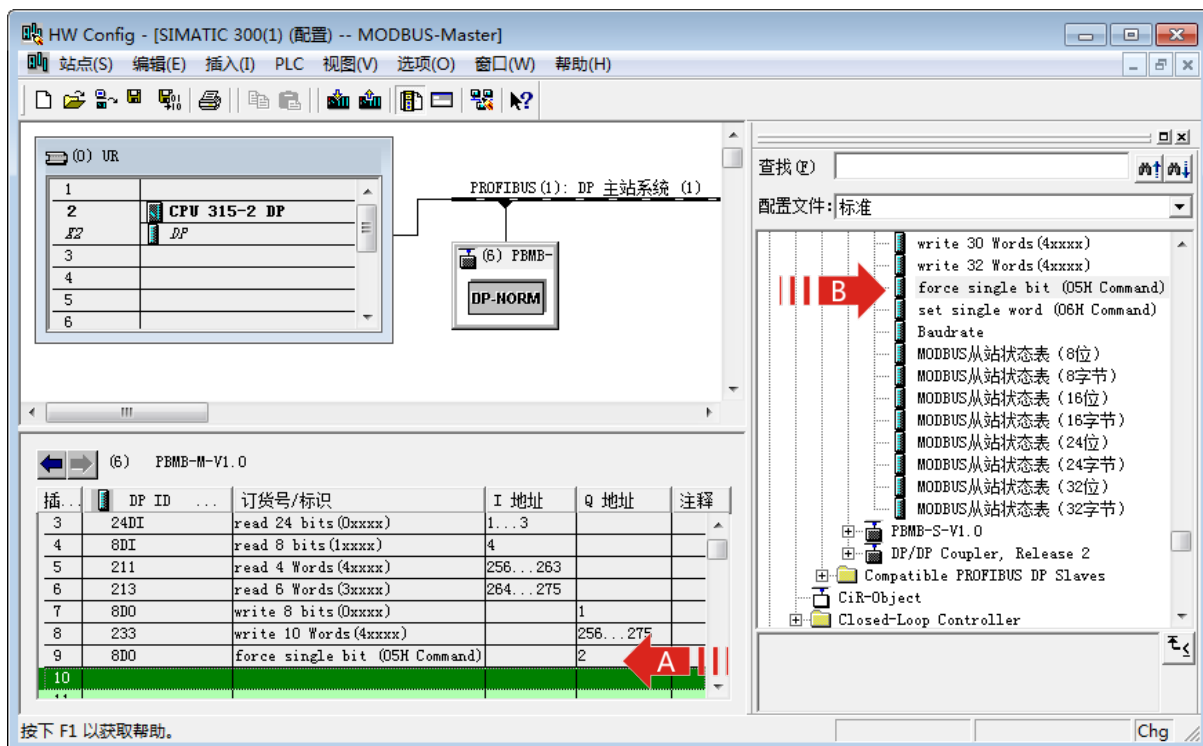


图 4-36

› 设定模块的详细参数。

双击 9 号槽中的模块 “8DO force single bit(05H Command) 2”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-37 所示。

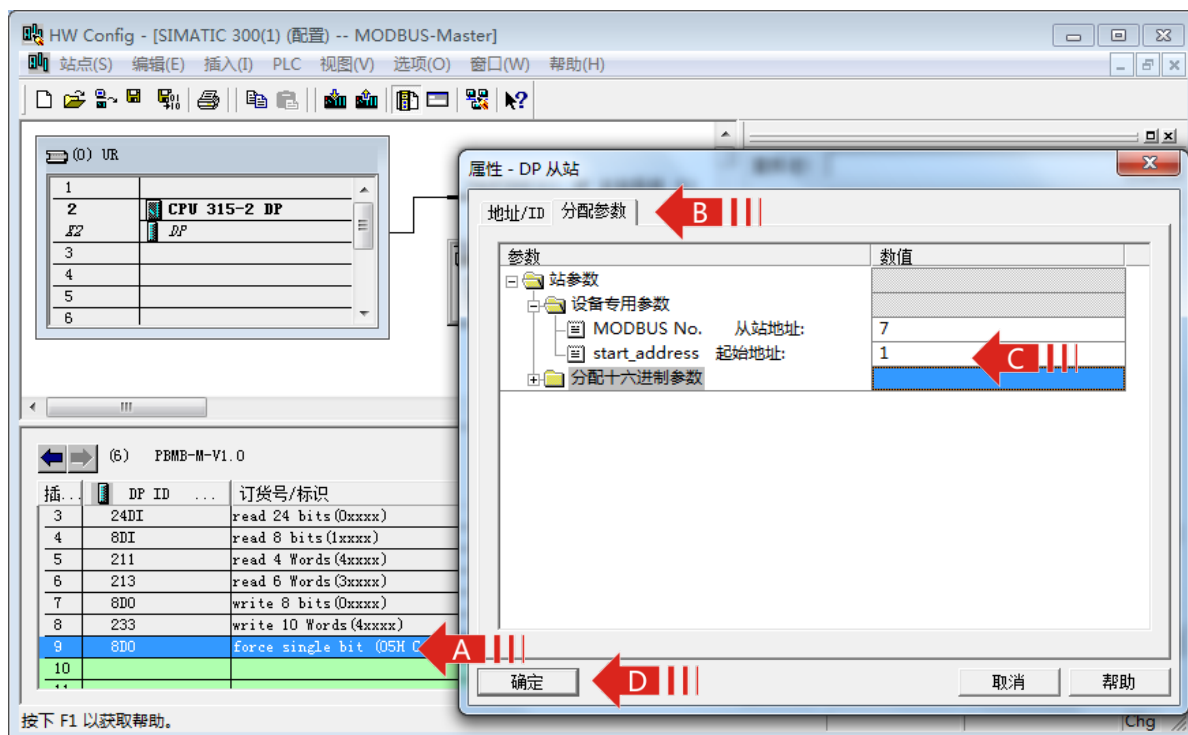


图 4-37

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 7。

注：从站地址不能设定为 0。

— 起始地址：要强置的 00001 地址。

› PROFIBUS 地址与 MODBUS 地址对应关系

QB2是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，当Q2.0=1时，设备地址00001强置为1，当Q2.0=0时，设备地址00001强置为0，如图4-38所示。

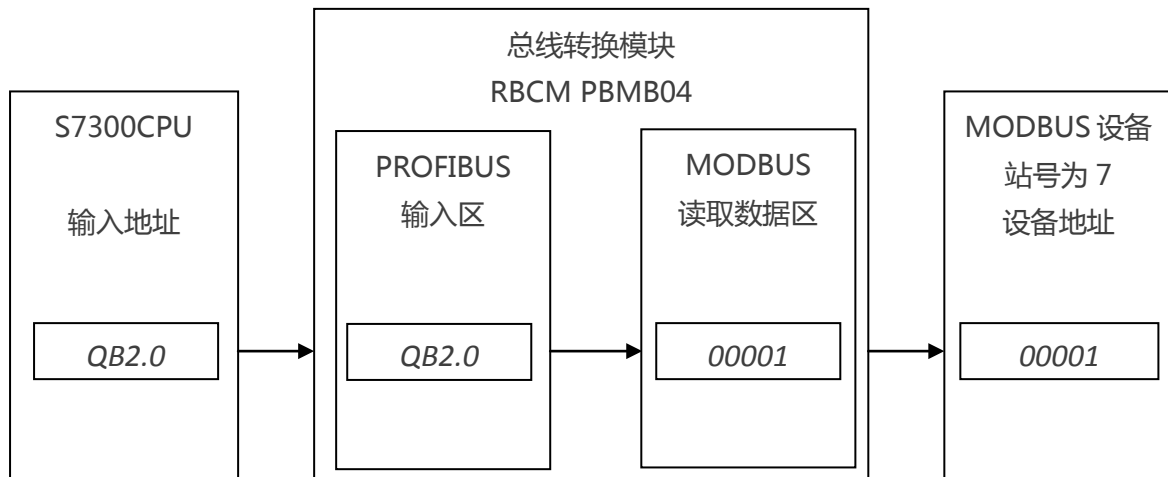


图4-38

4.5.7 功能 06H-预置单个保持寄存器 4xxxx 数据

› 本例概述

将 plc 地址为 PQW276 中的数据写入站号为 8，MODBUS 设备地址为 40001 的寄存器中，写入数量为 1 个 Words。

› 插入模块

单击 10 号槽，然后双击目录栏中 PBMB-M-V1.0 下的 “set single word(06h Command)”，如图 4-39。其中的 Q 地址一栏中的 “276...277” 表示 S7-300/CPU215-2DP 中 “QB276-QB277” 地址的数据，将会通过本总线转换模块发送至从站 40001 地址中，共 1 个 Words。

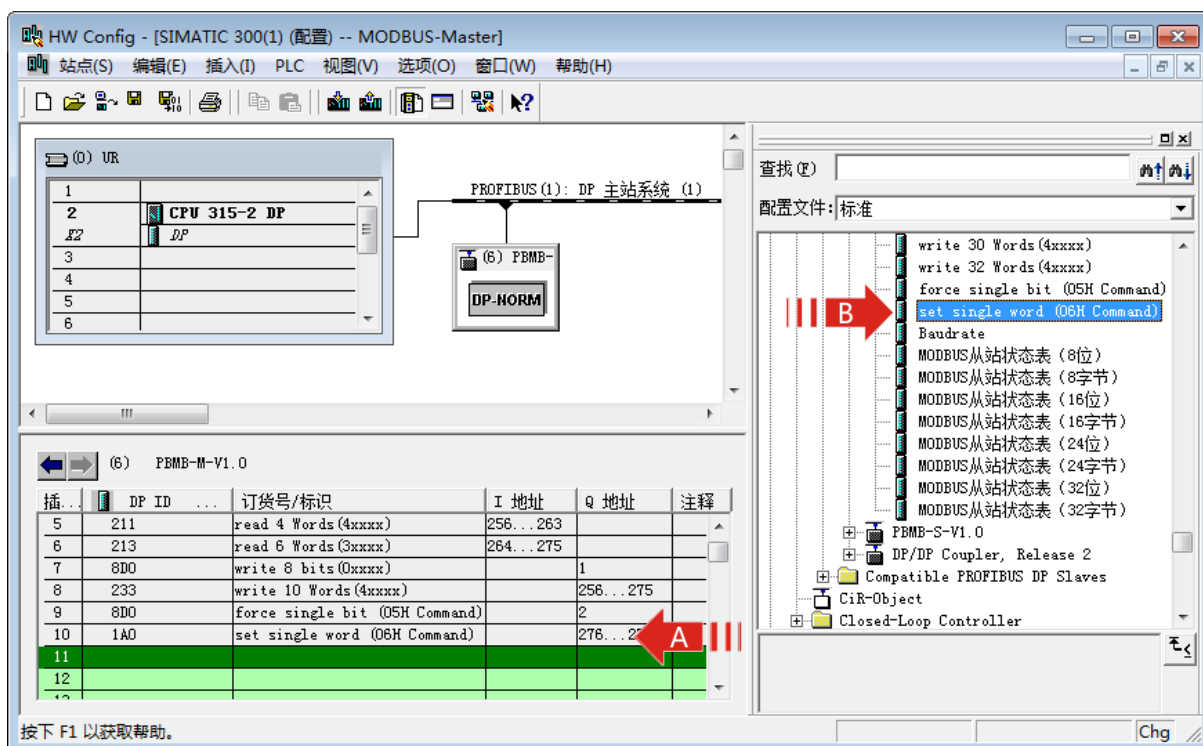


图 4-39

› 设定模块的详细参数。

双击 10 号槽中的模块 “1A0 set single word(06h Command) 276...277”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。进行从站地址和起始地址的设置。如图 4-40 所示。

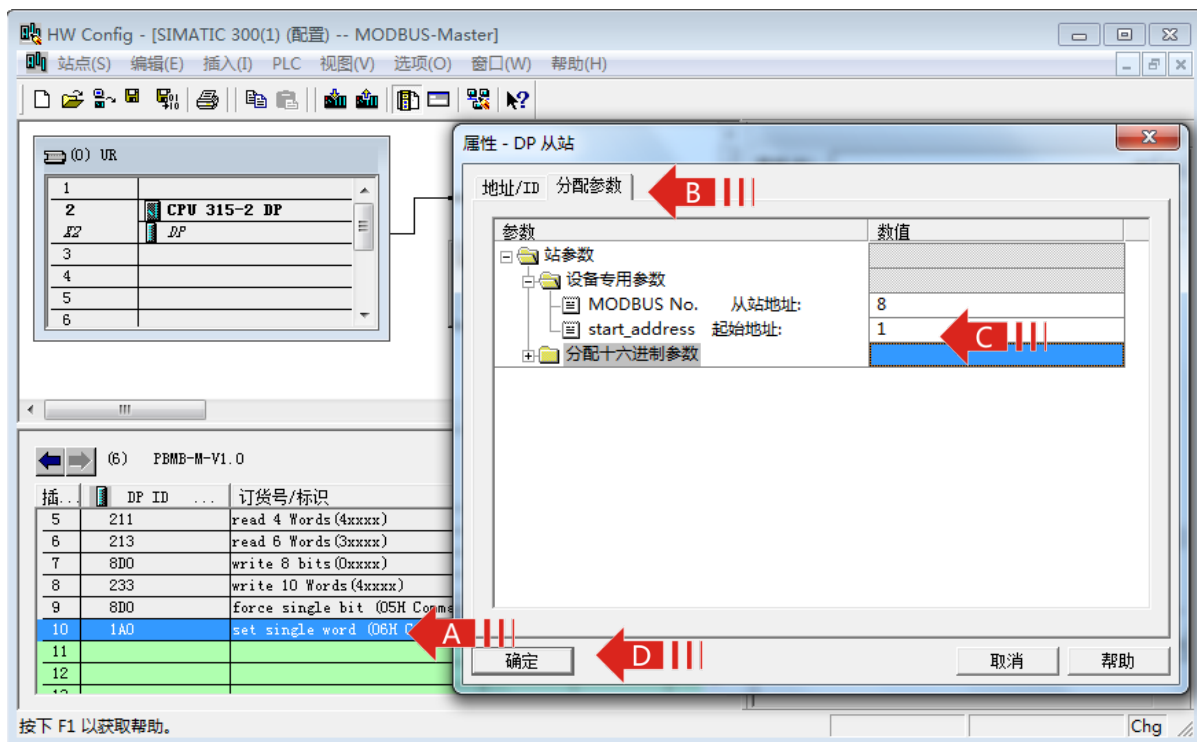


图 4-40

—从站地址：连接到该模块的 MODBUS 从设备的地址。本例地址为 8。

注：从站地址不能设定为 0。

—起始地址：要写入的地址为 40001。

› PROFIBUS 地址与 MODBUS 地址对应关系

QB276至QB277是PROFIBUS 主站分配给这个MODBUS 模块的PROFIBUS 输入地址，对应MODBUS设备地址40001共1Word，如图4-41所示。

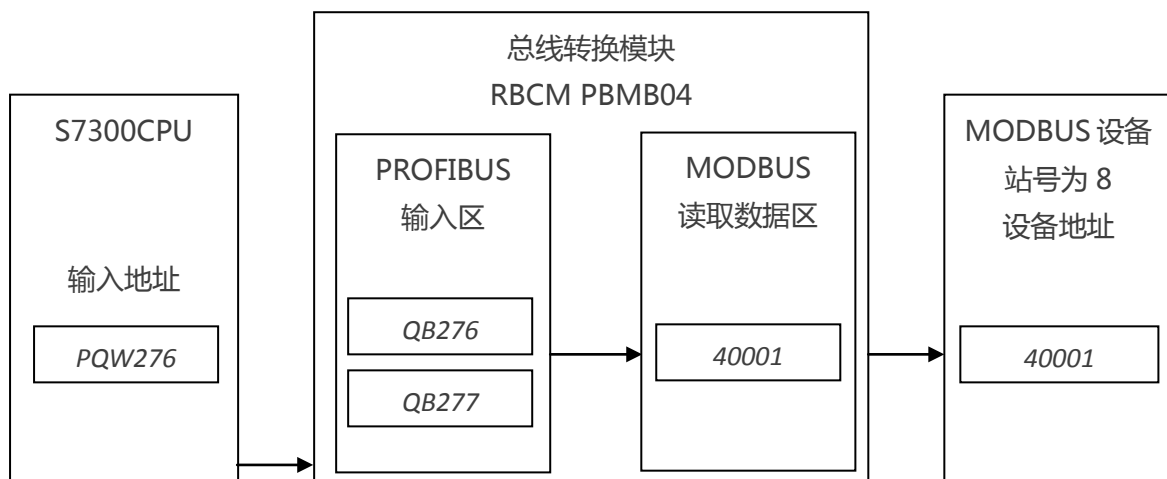


图4-41

4.5.7 保存并编译

此时，系统已配置完毕。点击菜单栏中的“站点->保存并编译(M)”保存并编译。如图 4-42 所示。

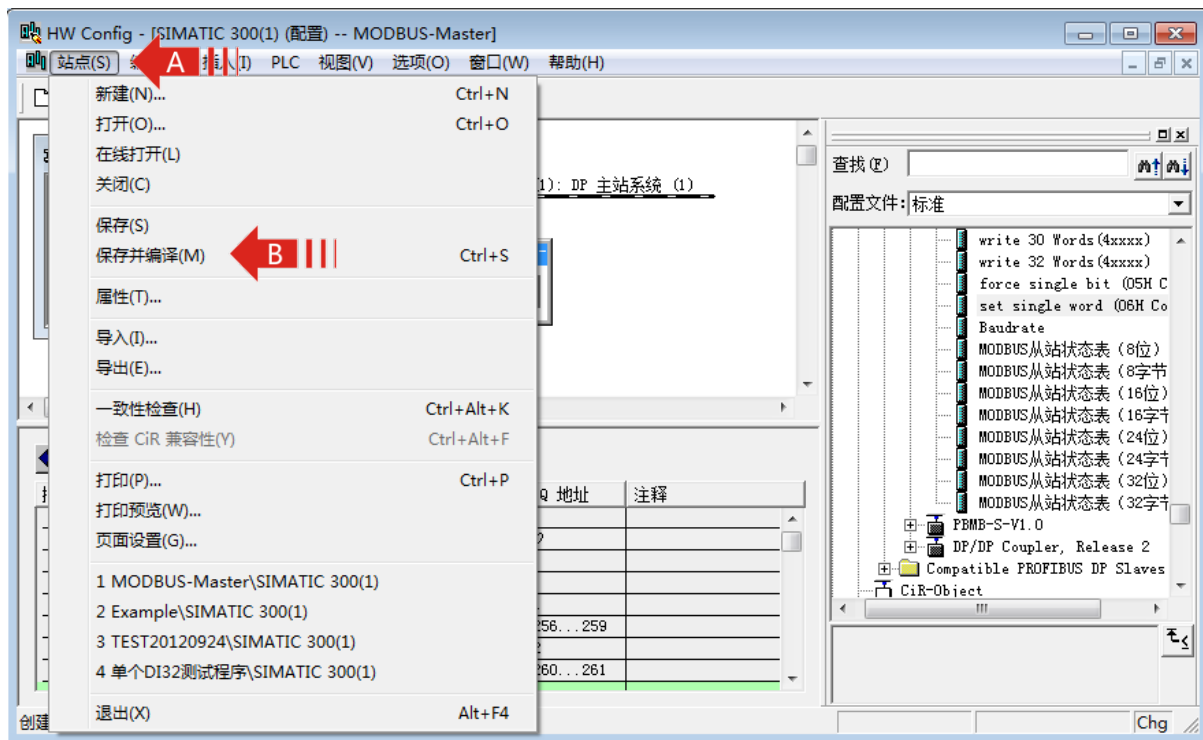


图 4-42

4.6 通信状态字与通信控制字

4.6.1 通信状态字与通信控制字

从系统配置中可以看到 1 槽和 2 槽已被占用，其中 1 槽为一字节输入，对应的 PROFIBUS 输入地址 IB0，作为本总线转换模块的通信状态字（status）。2 槽为一字节输出，对应的 PROFIBUS 输入地址 QB0，作为本总线转换模块的通信控制字（control）。如图 4-43 所示。

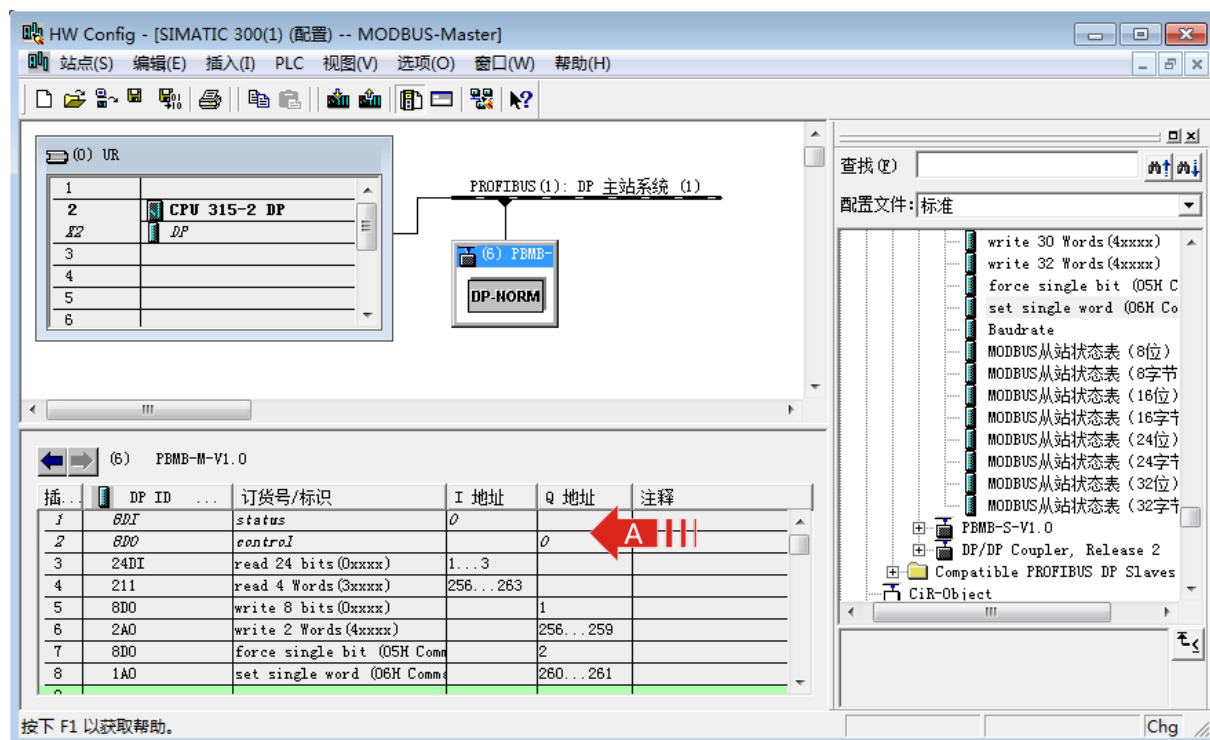


图 4-43

4.6.2 通信状态字格式

Bit7	Bit 6	Bit 5	Bit 4- Bit 1	Bit 0
奇偶校验错指示	CRC 校验错指示	等待应答超时	异常应答码	接收或发送状态指示

注：当通信正常之后，即使所有的报文都可以正常应答，且无错误发生。Bit5 ~ Bit7 置位后并不会自动清零，需要使用通信控制字中的清除错误标记位才能将这些位清零。

Bit 0 :

- 1：本协议转换模块处在发送报文或等待接收状态。
- 0：本协议转换模块在接收报文或处理接收到的报文状态。

Bit 4- Bit 1 :

MODBUS 从机无法正确执行 MODBUS 主机发送的命令时，将返回的异常应答码。详见 MODBUS 技术简介。整个报文队列最多可以有 37 条 MODBUS 报文，但是只有一个状态字所以当有新的异常

应答出现时，之前的异常应答状态码会被覆盖。

Bit 5 :

本总线转换模块发出 MODBUS 报文后，按配置的“等待回答时间 Time of Reply”等待 MODBUS 设备的应答，如果等待时间已到，仍未收到设备应答，本位置，协议转换模块继续发送下一条 MODBUS 报文。

Bit 6 :

接口收到的 MODBUS 报文 CRC 校验出现错误，本位置 1，并将收到的报文丢弃。

Bit 7 :

接口收到的字节奇偶校验错误，本位置 1，并将收到的报文丢弃。

4.6.3 通信控制字格式

Bit7	Bit 6	Bit 5	Bit 4	Bit 3	Bit2	Bit 1	Bit 0
强制 MODBUS 扫描复位	停止等待	清除错误标记	写入命令执行选择	通信故障数据清零	启用 USB 监视诊断	保留	启动/停止 MODBUS 扫描

Bit 0 :

1：启动总线转换模块，开始 MODBUS 扫描。

0：关闭总线转换模块，停止 MODBUS 扫描。

注：需要在程序中把该位置 1 后，MODBUS 开始扫描。

Bit 1 :

保留

Bit 2 :

1：启用 USB 监视诊断功能。

0：关闭 USB 监视诊断功能。

具体 USB 监视诊断功能见 4.7.5 利用 USB 监测测模块通信状态章节。

Bit 3 :

1：当 modbus 从站无应答或者是校验等通信故障时，将 Profibus 数据清零。

0：当 modbus 从站无应答或者是校验等通信故障时，将 Profibus 数据保持故障前的通信数据。

V0.5 以上版本的模块有效。

Bit 4 :

1：当发送 MODBUS 报文队列中的写类命令：05H、06H、0FH、10h 时，写的的数据无变化，模块不执行 MODBUS 报文。这样可以不执行无用的报文，提高 MODBUS 刷新速度。V2.0 版本的模块有效。

0：当发送 MODBUS 报文队列中的写类命令：05H、06H、0FH、10h 时，写的的数据无变化，模块

仍然执行 MODBUS 报文。

Bit 5 :

置 1 的时候将通信状态字中的 Bit7-Bit1 清零。

Bit 6 :

当配置系统的等待回答时间为“无限期等待回答 Waiting...”的时候。若总线转换模块发送一条报文后无 MODBUS 应答，本总线转换模块会无限期等待。此时，设置本位为 1，则可以停止等待，进入下一条报文的发送。

注 若此位保持为 1，当下一条报文发送之后，同样不会等待，通常本位配合 Bit0 启动停止 MODBUS 扫描使用。示例如下：

...

总线转换模块正无限期等待应答；

设置“Bit0 启动/停止 MODBUS 扫描”为 0 停止 MODBUS 扫描；

设置“Bit6 停止等待”为 1，关闭无限期等待应答；

设置“Bit6 停止等待”为 0，启用无限期等待应答；

设置“Bit0 启动/停止 MODBUS 扫描”为 1 重新开始 MODBUS 扫描；

总线转换模块停止等待，发送下一条 MODBUS 报文。

...

Bit 7 :

1：强制 MODBUS 扫描回到第一条 MODBUS 报文位置。

0：强制 MODBUS 扫描复位无效

注：若要重新开始发送，需要将此位设置为 0；

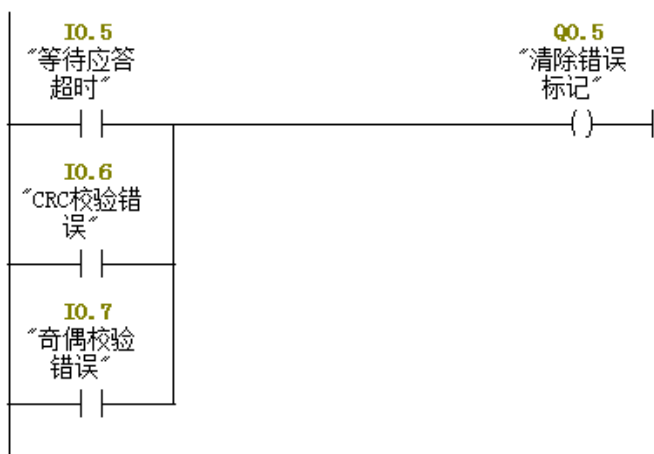
4.6.4 通信状态字及通信控制字 PROFIBUS 对应关系

通信状态字	PROFIBUS地址	通信控制字	PROFIBUS地址
D0：接收或发送状态	I0.0	D0:启动/停止 MODBUS 扫描	Q0.0
D1 ~ D4：异常应答码	I0.1 ~ I0.4	D1:保留	Q0.1
		D2: 启用 USB 监视诊断功能	Q0.2
		D3: 通信故障数据清零	Q0.3
		D4: 写入命令执行选择	Q0.4
D5：等待应答超时	I0.5	D5:清除错误标记	Q0.5
D6：CRC 校验错误	I0.6	D6:停止等待	Q0.6
D7：奇偶校验错误	I0.7	D7:强制 MODBUS 扫描复位	Q0.7

4.6.5 PLC 程序对 MODBUS 通讯的控制

程序段 1：标题：

总线转换模块出现应答超时、CRC或者奇偶校验错误时，相应的状态字D5、D6、D7置1，程序中自动把控制字“D5：清除错误标记”置，清除错误。

**程序段 2：标题：**

MO.0可以控制MODBUS通讯口的启动和停止。如果通讯发生错误，那么程序会立刻停止MODBUS通讯，待错误复位后，MODBUS通讯自动恢复运行



注：在 PLC 程序中一定要把控制字“D0:启动/停止 MODBUS 扫描”置 1，MODBUS 通讯才能启动。

4.7 对从站通讯状态监测

- › 当总线转换模块MODBUS作主站，带有多个MODBUS 从站时，可以使用PROFIBUS 主站监测MODBUS 从站的通信状态。从站的通讯状态或者通讯错误码直接对应PLC输入地址，PLC可以利用这些地址进行逻辑控制，也可以利用人机界面或者组态软件对这些地址的监控。
- › 本总线转换模块提供两种检测模式，位监测模式和字节监测模式。位检测模式，一位对应一个从站。字节监测模式，一个字节对应一个主站。字节监测模式相对于位检测模式提供更多的从站状态信息。下面对两种不同的检测模式分别进行介绍。

4.7.1 对 MODBUS 从站通讯状态检测（位）

- › 在前面的里章节中我们列举了MODBUS功能码01H、02H、03H、04H、05H、06H、0FH、10H的设定和地址的转换关系，同时也定义了8个从站，从站号为1至8。下面我们以1至8号从站为例介绍对MODBUS从站通讯状态检测（位）。

在硬件配置窗口中，左键双击总线上的转换模块，弹出“属性-DP从站”对话框，选择分配参数，选择“有从站状态监测（8位）”，8位对应例程中的8个从站。如图4-44。

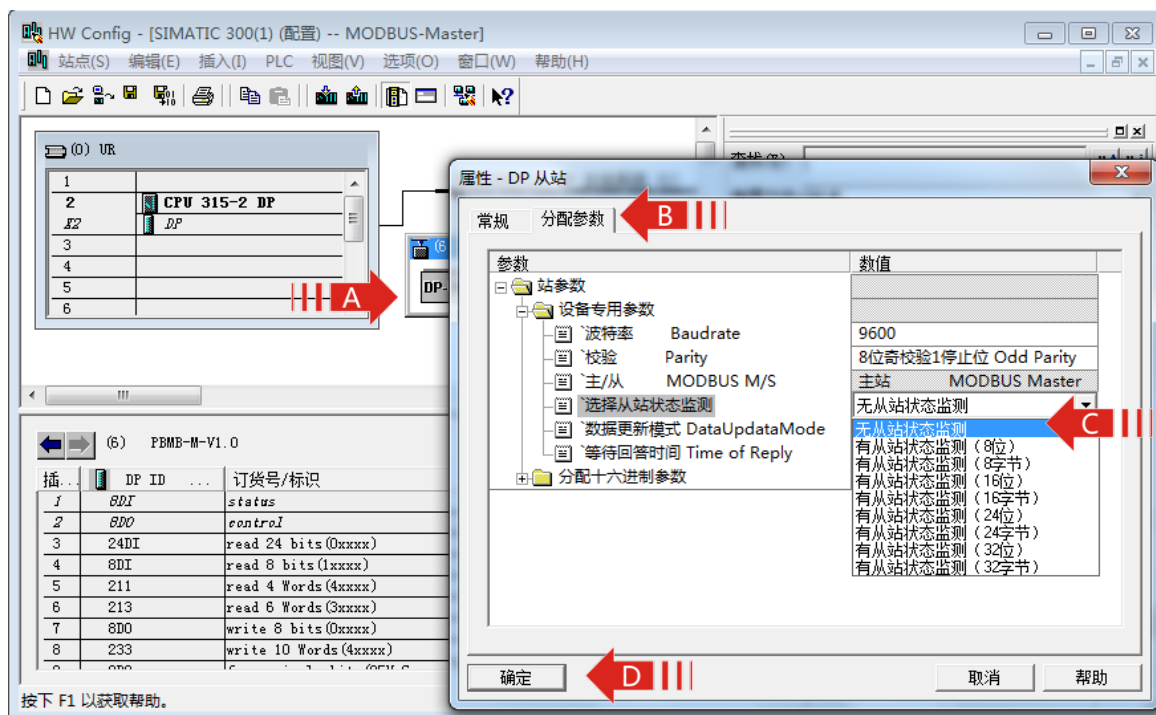


图 4-44

在报文列表中插入选择“MODBUS 从站状态表（8位）”。

单击 11 号槽，然后双击目录栏中 PBMB-M-V1.0 下的“MODBUS 从站状态表（8位）”，如图 4-45。其中的 I 地址一栏中的“5”表示从站返回的 8bits 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中“IB5”地址。

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

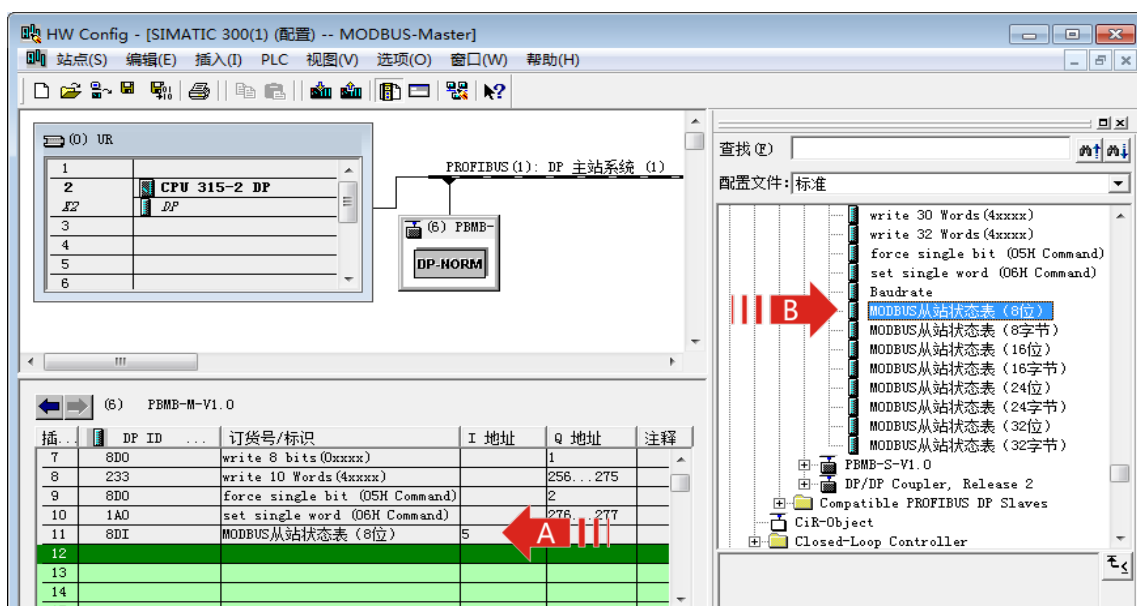


图 4-45

› 设定模块的详细参数。

双击 11 号槽中的模块“8DI MODBUS 从站状态表（8 位）”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。在输入框内输入 01 至 08，中间用逗号分开。如图 4-46 所示。

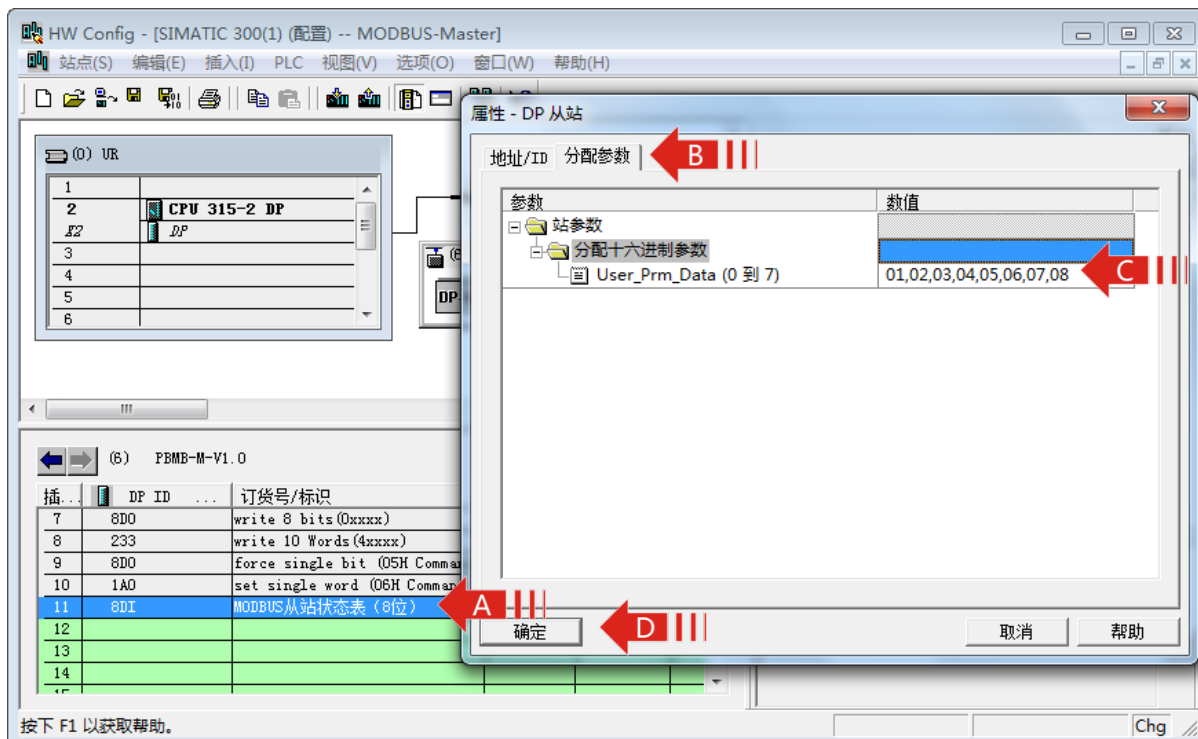


图 4-46

› 程序运行后，可在 PROFIBUS 地址 IB5 中检测到 MODBUS 从站 01 至 08 的通信状态的显示：

IB5：

D7 : I5.7	D6 : I5.6	D5 : I5.5	D4 : I5.4	D3 : I5.3	D2 : I5.2	D1 : I5.1	D0 : I5.0
从站08H	从站07H	从站06H	从站05H	从站04H	从站03H	从站02H	从站01H
通讯状态	通讯状态	通讯状态	通讯状态	通讯状态	通讯状态	通讯状态	通讯状态

D0 = 01H 从站通信状态：

Dn(n=0...7)=0：从站通讯故障。MODBUS 主站向 01H 从站发送报文，超过等待时间之后没有收到从站回答或 01H 从站根本没有接到可使其回答的 MODBUS 主站报文。超时等待时间设定见 4.3 章节。

Dn(n=0...7)=1：从站通讯正确。01H 站在接收到 MODBUS 主站报文后在规定的时间内作出了回答，并且 MODBUS 主站接收到的回答报文正确。

4.7.2 对 MODBUS 从站通讯状态检测（字节）

› 在前面的章节中我们列举了 MODBUS 功能码 01H、02H、03H、04H、05H、06H、0FH、10H 的设定和地址的转换关系，同时也定义了 8 个从站，从站号为 1 至 8。下面我们以 1 至 8 号从站为例介绍对 MODBUS 从站通讯状态检测（字节）。

› 在硬件配置窗口中，左键双击总线上的转换模块，弹出“属性-DP 从站”对话框，选择分配参数，选择“有从站状态监测（8 字节）”，因为我们例程中有 8 个从站。如图 4-47。

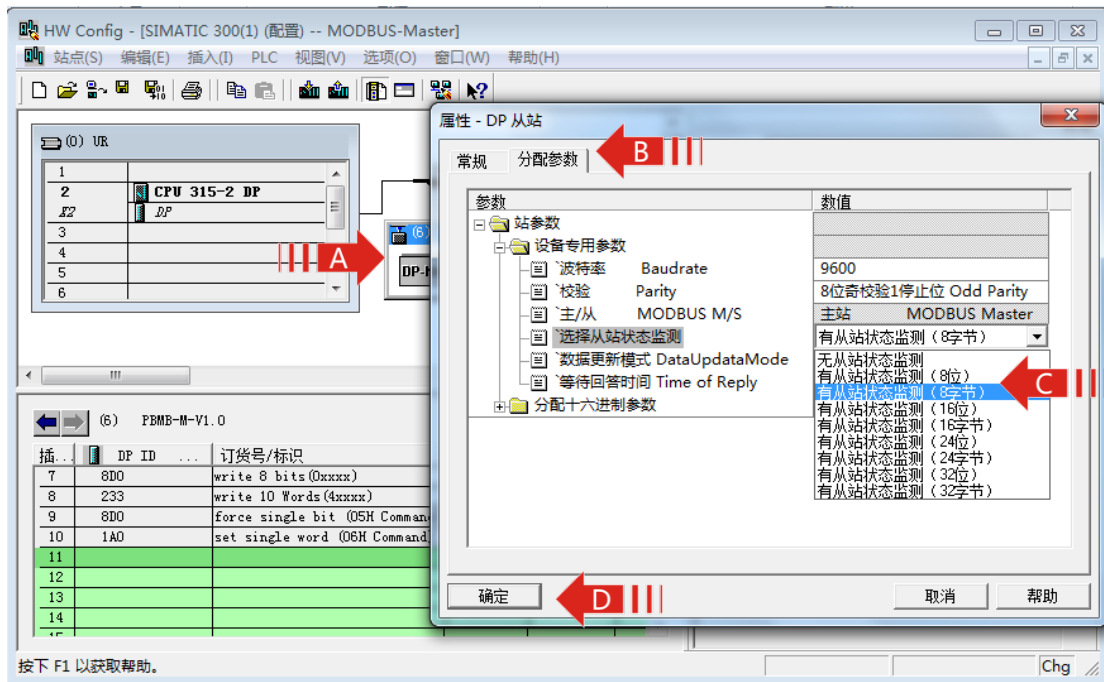


图 4-47

› 在报文列表中插入选择“MODBUS 从站状态表（8 字节）”。

单击 11 号槽，然后双击目录栏中 PBMB-M-V1.0 下的“MODBUS 从站状态表（8 字节）”，如图 4-48。其中的 I 地址一栏中的“5~12”表示从站返回的 8byte 的数据，将会通过本总线转换模块发送至 S7-300/CPU215-2DP 中“IB5~IB12”地址。

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

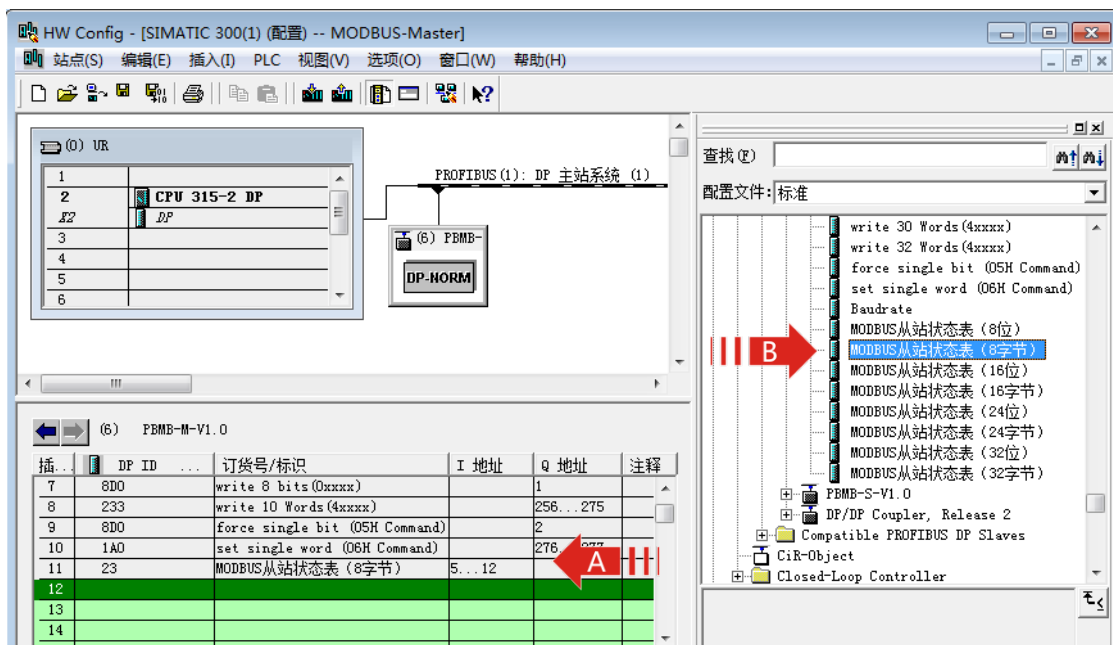


图 4-48

› 设定模块的详细参数。

双击 11 号槽中的模块“23 MODBUS 从站状态表 (8 字节)”，打开“属性 - DP 从站”对话框。选择对话框中的“分配参数”选项卡。在输入框内输入 01 至 08，中间用逗号分开。如图 4-49 所示。

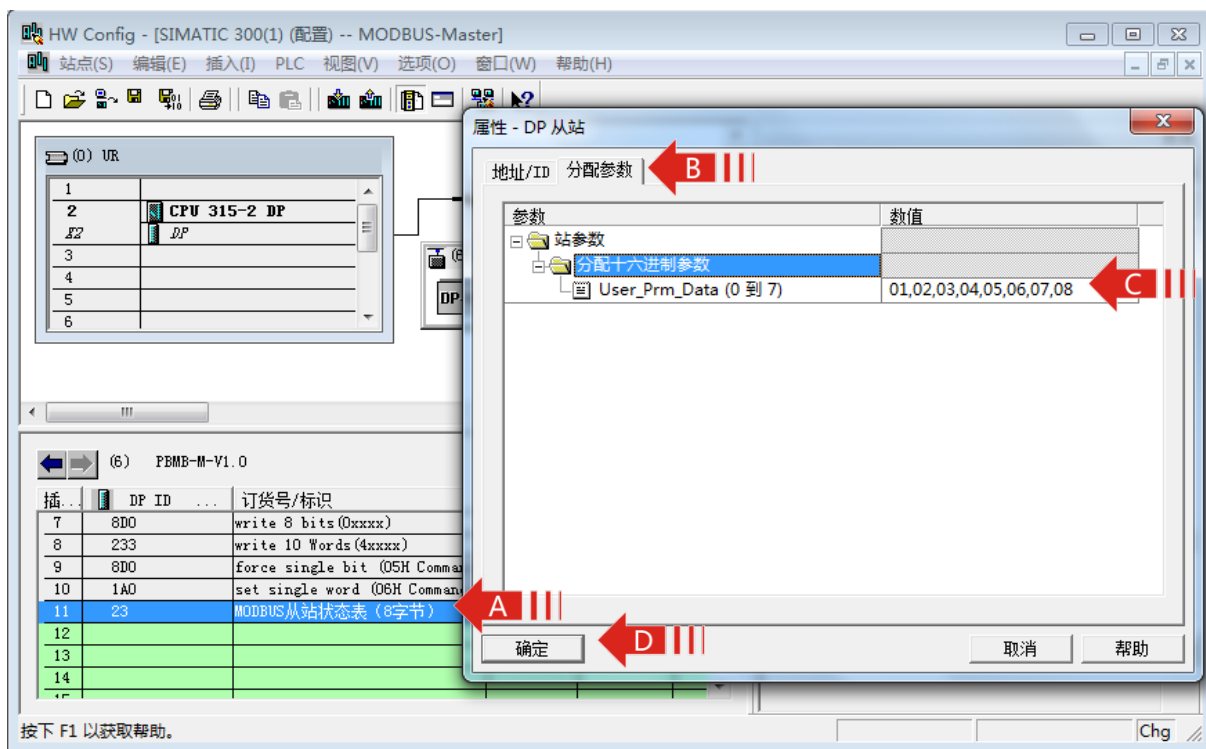


图 4-49

› 运行程序后，在 PROFIBUS 主站地址 IB5 ~ IB12 中，可显示对应 MODBUS 从站号 01H 至 08H 的通信状态字节。

IB5：对应 01H 号 MODBUS 从站的状态字节

D7：	D6：	D5	D4~D1：	D0:
奇偶校验错误	CRC 校验错误	不用	MODBUS 异常应答码	主站等待回答超时

其中：

— **D0 (I5.0) : 主站等待回答超时**

D0=0：MODBUS 主站向 01H 从站发送报文，超过等待时间之后没有收到从站回答或 01H 从站根本没有接到可使其回答的 MODBUS 主站报文。超时等待时间设定见 4.3 章节。

D0=1：01H 号从站接收到 MODBUS 主站报文后在超时时间之内作出了回答，并且 MODBUS 主站接收到的回答报文是正确的。

— **D4 ~ D1 (I5.1 ~ I5.4)：MODBUS 异常应答码**

当 MODBUS 主站发送一条 MODBUS 报文后，01H 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“附录B MODBUS技术简介-B.3.异常应答”。

—D6：CRC效验错

D6=1：MODBUS 主站接收到一条MODBUS 回答报文时CRC 校验错误，此时，MODBUS 主站认为MODBUS 回答数据不可靠、废弃不用，不与PROFIBUS对应数据区交换。

—D7：奇偶校验错

D7=1：MODBUS 主站接收字符中发现字符奇偶校验错。此时，MODBUS 主站认为MODBUS 回答数据不可靠、废弃不用，不与PROFIBUS 对应数据区交换。

）其他站号02H~08H分别对应IB6~IB12,功能与IB5相同。

4.7.3 对 MODBUS 从站通讯状态检测异常状态

› 如果在MODBUS 报文配置中配置了01H 号从站的报文，而在键入MODBUS从站地址表中（见图4-46或图4-49）没有键入01H 地址；当MODBUS 主站发出01H 从站报文后，如果接收（或没有接收）到回答，但MODBUS 主站在从站地址表中找不到01H，此时，MODBUS 主站将总状态字（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。

IB0：总状态字

Bit7	Bit 6	Bit 5	Bit 4- Bit 1	Bit 0
奇偶校验错指示	CRC 校验错指示	等待应答超时	异常应答码	接收或发送状态指示
			1111	

› 如果MODBUS 主站接收到01H 号从站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01H，将收到的异常应答码存入相应的

“MODBUS 从站通信状态字节”中（IB5的D4~D1）。但如果：在MODBUS 从站地址表中没有找到该报文MODBUS 地址（见图4-46或图4-49），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。

› 如果MODBUS 主站接收到01H 号从站的报文有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01H，对相应的“MODBUS 从站通信状态字节”置标志位（IB5的D6或D7。但如果：在MODBUS 从站地址表中没有找到该报文的MODBUS 地址（见图4-46或图4-49），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。

4.7.4 对 MODBUS 从站通讯状态检测注意事项

由于从站通讯检测表要占用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。所以总线转换模块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	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

4.7.5 利用 USB 监测测模块通信状态

› USB 口监测功能

- 监测 PROFIBUS 总线通信状态。
- 监测模块通信状态，提示操作信息。
- 显示通信串口收发报文的数据信息。

› 对 USB 口操作

- 用 USB 线连接模块与计算机。模块 USB 接口为 micro 型。
- 安装 USB 口驱动程序，驱动程序名称“监视 USB 驱动程序 CH341SER”可以向厂商索取。
- 安装串口调试助手软件，可以向厂商索取。



图 4-24

-串口调试助手软件的设置

串口号：在计算机硬件列表中可以查询到 340USB 串口的串口号。

串口设置：波特率 115.2K；数据位 8 位；停止位 1 位；无校验位；无流控制。不可设置其他参数

HEX 显示：不选择 HEX 显示

打开串口，即可监视到模块数据。关闭串口。即可查询前面的数据信息。

-启用 USB 监测模块通信状态功能

将控制字第三位 QX.2=1，启用 USB 监测模块通信状态功能。硬件 V2.2 以上版本需要启用，硬件 V2.2 以下版本默认已经启用。

注：在模块断电前要关闭串口调试软件的串口，否则会造成串口调试软件死机。

4.8 MODBUS 通讯故障及排除

在检测MODBUS通讯故障之前首先要确定总线转换模块要与PROFIBUS主站通讯正常，也就是说 PROFIBUS故障指示灯BF不亮，正确指示灯BC常亮。如果与PROFIBUS主站通讯不正常，那么 MODBUS是不能进行通讯的。

4.8.1 MODBUS 接口不工作

产生原因

MODBUS接口无数据发送和接收。

故障现象

—检查 MODBUS 通讯发送灯 TD 和接收灯 RD 无闪烁。

› 解决方法

—PROFIBUS 通讯接口是否正常。

—控制字 D0：启动 MODBUS 扫描位是否置 1，见 4.6.3 控制字。

—控制字 D1：读允许和控制字 D2：写允许是否同时置 1 或同时置 0。

4.8.2 MODBUS 通讯超时等待错误

› 产生原因

如果在总线转换模块配置“等待回答时间Time of Replay”中选择一个的等待时间，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 扫描时间到后将发出下一条 MODBUS 报文。

› 故障现象

—总的状态字“D5: 等待应答超时”=1。

—如果应用了从站检测功能，那么从站相对应的状态字“D5: 等待应答超时”=1。

—MODBUS 通讯状态灯正常是发送灯 TD 闪烁一次，接收灯 RD 闪烁一次。如果出现通讯超时等待错误，那么就会出现连续两次 TD 闪烁，而中间没有 RD 灯闪烁。

—MODBUS 通讯报警灯 ALM 闪烁一次，表示没有接收到回答的报文，出现通讯超时等待故障。

› 解决方法

—MODBUS 总线连接是否可靠。

—MODBUS 从站配置是否和主站软件配置一致，包括地址站号、波特率。

4.8.3 CRC 校验错误

› 产生原因

总线转换模块接收到的 MODBUS 回答报文有字符 CRC 校验错。

› 故障现象

—如果总线转换模块接收到的MODBUS回答报文有字符CRC 校验错，总线转换模块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“D6: CRC校验错误”置1。

—如果应用了从站检测功能，那么从站相对应的状态字“D6: CRC 校验错误”=1。

› 解决方法

—字符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“D5：清错误标记”=1 将错误标记清除。“D5：清错误标记”=1 不影响MODBUS 扫描器。“D5：清错误标记”保持为1，将保持清除错误标记功能有效。

—减少外部环境对总线的电磁干扰。

4.8.4 奇偶校验错误

› 产生原因

总线转换模块接收到的 MODBUS 回答报文有字符奇偶校验错误。

› 故障现象

—如果总线转换模块接收到的MODBUS回答报文有字符奇偶校验错,总线转换模块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“D7: 奇偶校验错误”置1。

—如果应用了从站检测功能,那么从站相对应的状态字“D7: 奇偶校验错误”=1。

› 解决方法

—检查总线转换模块的奇偶校验设置是否与从站的设置相同。

—字符奇偶校验错误不影响MODBUS扫描进行,但错误标志将保留。可以使用控制字“D5: 清错误标记”=1 将错误标记清除。“D5: 清错误标记”=1 不影响MODBUS 扫描器。“D5: 清错误标记”保持为1,将保持清除错误标记功能有效。

—减少外部环境对总线的电磁干扰。

4.8.5 MODBUS 扫描在无限期等待回答

› 产生原因

如果在总线桥配置“等待回答时间Time of Replay”中选择了“无限期等待Waiting.....”,当总线转换模块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 扫描处在无限期等待回答中。

› 故障现象

—状态字“D0: 接收完毕/发送允许”=0, MODBUS 扫描等待回答。

—MODBUS 通讯发送灯 TD 和接收灯 RD 无闪烁。

› 解决方法

—第一种方法

使用控制字“D6: 停止等待”,使MODBUS 扫描器停止等待,转向发送下一条MODBUS 报文。

↓

↓

MODBUS 扫描器处在无限期等待回答中.....

D0: 启动MODBUS 扫描=0;

D6: 停止等待=1;

D6: 停止等待=0;

D0: 启动MODBUS 扫描=1;

MODBUS 扫描器停止等待，转向发送下一条MODBUS 报文.....

↓

↓

—第二种方法

使用控制字“D7：强置MODBUS 扫描复位”，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.....

D0：启动MODBUS 扫描=0；

D7：强置MODBUS 扫描复位=1；

D7：强置MODBUS 扫描复位=0；

D0：启动MODBUS 扫描=1；

MODBUS 扫描器停止等待、复位、发送第一条MODBUS 报文.....

↓

↓

4.8.6 MODBUS 扫描器反复回到起始位置

› 故障现象

—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。

› 解决方法

—使用正确的启动方法，启动时控制字“D7：强制 MODBUS 扫描复位”=0 和“D6：停止等待”=0。

4.8.7 MODBUS 扫描器没有等待而跳到下一个位置

› 故障现象

—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。

› 解决方法

—使用正确的启动方法，启动时控制字“D7：强制 MODBUS 扫描复位”=0 和“D6：停止等待”=0。

4.8.8 MODBUS 异常应答

› 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。

› 故障现象

—从机将以“异常应答”回答之。见“附录B MODBUS 技术简介 B.3异常应答”。通信状态字D4~D1 是MODBUS 异常码。

注: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。

› 解决方法

—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。可以使用控制字“D5：清错误标记” =1 将错误标记清除。

MODBUS 为从站工作模式的应用

5

引言

本章使用 S7300 作为 PROFIBUS 主站，STEP7 为配置和调试软件详细的介绍了 PBCM PBMB-04(02)模块的 MODBUS 为从站工作模式的应用方法，包括：

- › S7300工程的建立
- › MODBUS通讯接口的设定
- › 实例列举了01H、02H、03H、04H、0FH、10H、05H、06H MODBUS功能码的配置
- › PBCM PBMB-04(02)模块的状态字和控制字介绍

5.1 建立一个项目

› 建立一个 S7300 为 PROFIBUS 主站的工程项目，工程的名字为 MODBUS-Slave。建立的说明请参阅第 4 章的 4-1 和 4-2 部分。

5.2 在项目中配置一个总线转换模块

› 单击图 5-1 中“PROFIBUS(1): DP 主站系统 (1)”下方的总线，使其由黑白相间变为黑色实线。然后打开右侧目录栏中的 PROFIBUS DP->Additional Field Devices->Gateway->PBMB-S-V1.0，双击 PBMB-S-V1.0，出现“Properties – PROFIBUS 接口 PBMB-S-V1.0”对话框，选择从站地址，本例选择从站地址 7。如图 5-2 所示。然后点击确定。结果如图 5-3 所示。

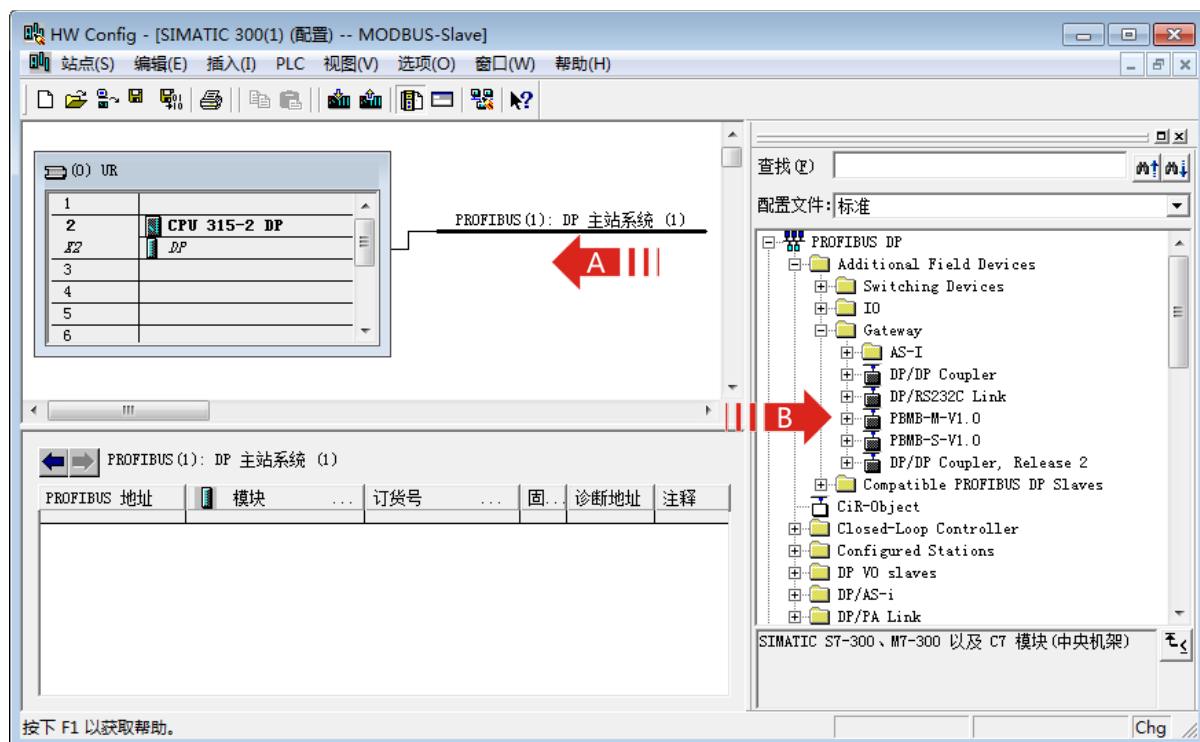


图 5-1



图 5-2

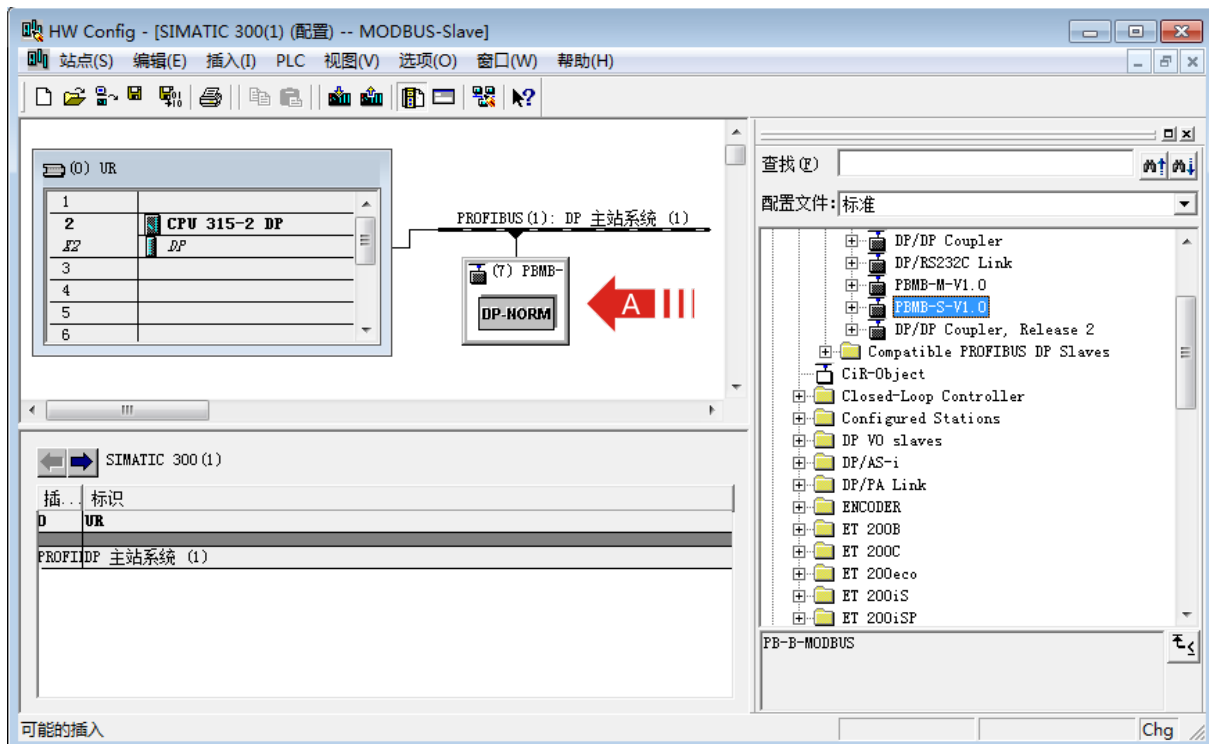


图 5-3

› 配置 DP 从站属性：双击图中位置导轨下的(7)PBMB-S-V1.0，出现“属性 - DP 从站”对话框，单击“分配参数”选项卡，如图 5-4 所示。

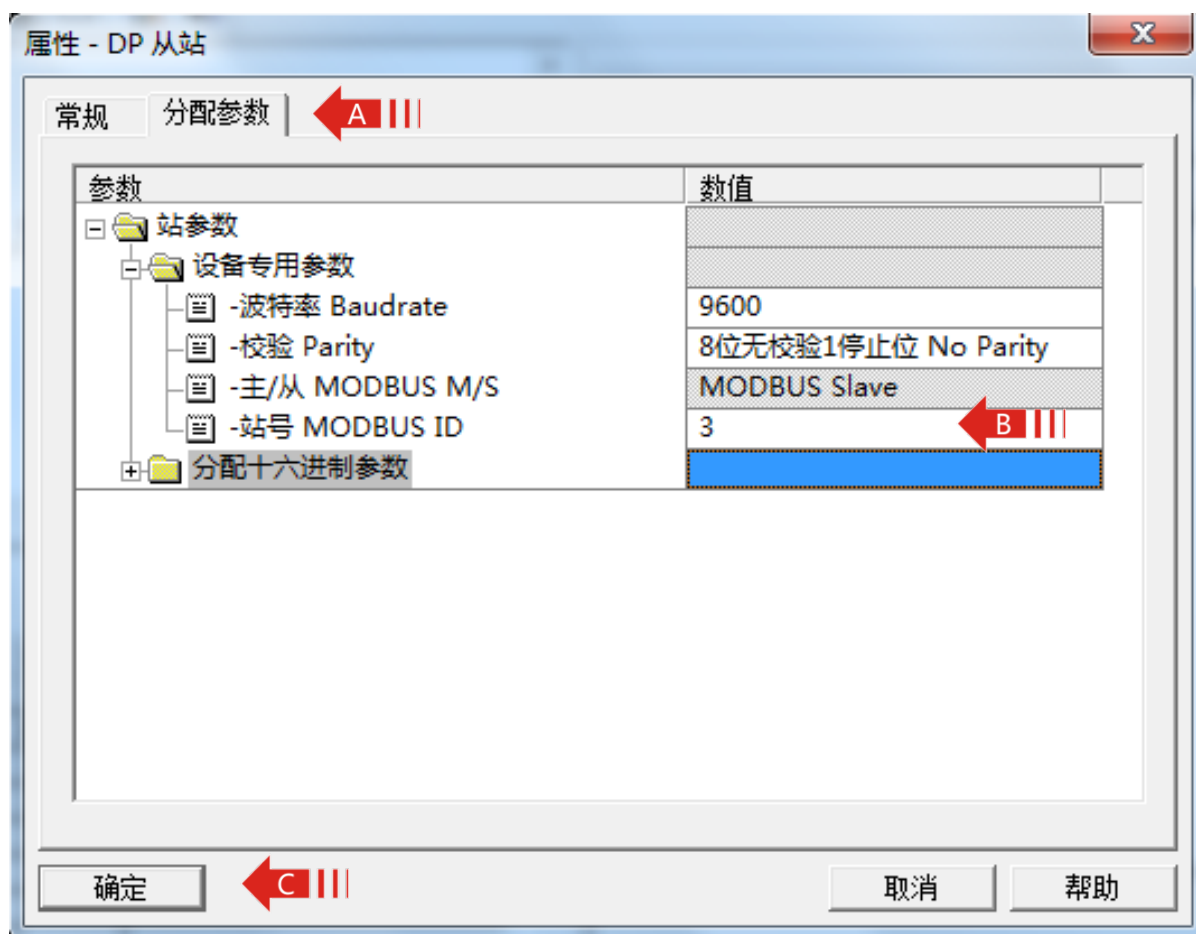


图 5-4

—选择波特率

单击“波特率 Baudrate”右侧的“数值”。

支持波特率范围：2400-115.2K。

本例中选择 9600。

—选择校验方式

单击“校验 Parity”右侧的“数值”。支持“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”四种方式。

—设置从站站号

本例中作为 MODBUS 从站，此处设置协议桥的站号为 3。

5.3 配置 RBCM PBMB-04(02) 的 MODBUS 报文队列

› PBMB-S-V1.0 一共有 20 个槽,前两个槽分别作为状态字及控制字已被占用，剩下 18 个槽可供用户使用。每个槽可以用来插入一条 PROFIBUS 输入输出与 MODBUS 存储区的对应关系。所以一

共可以插入 18 项。单击右侧目录栏中的 PROFIBUS DP->Additional Field

Devices->Gateway->PBMB-S-V1.0 左侧的加号，使其目录展开。PBMB-S-V1.0 的每一个 MODBUS 模块对应一种功能的 MODBUS 报文，可先单击要使用的槽，然后双击右侧目录栏中 PBMB-S-V1.0 列出的目录中的一项，使其插入某一槽中。如图 5-5。模块与 MODBUS 报文类型对应关系介绍如下表。

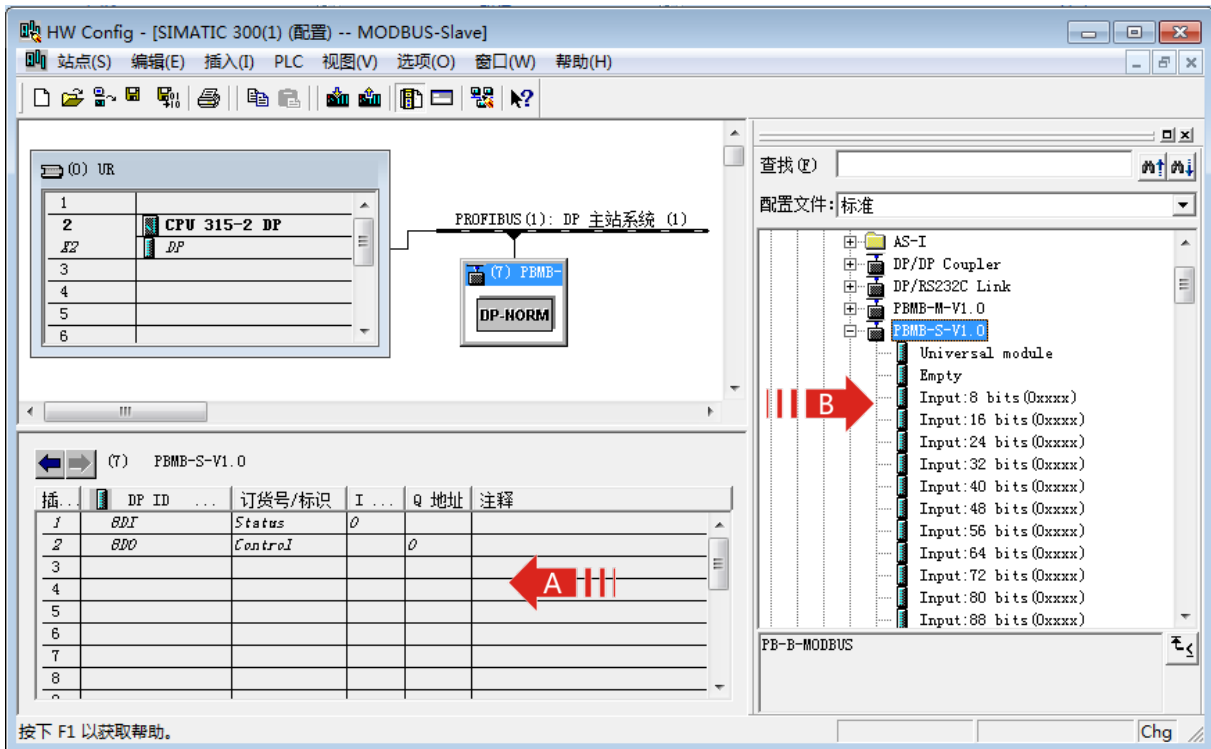


图 5-5

表 PBMB-S-V1.0 模块功能介绍

模块	PROFIBUS I/O	对应 MODBUS 存储区	建立的关系（数据交换）
Input: N bits(0xxxx)	Bit 输入区：Ix.y 地址范围：S7-300(0-255) S7-400(0-511)	线圈 0xxxx 地址范围：0~1791	PROFIBUS (BIT) 输入与 MODBUS 线圈存储区 0xxxx 间
Input: N Word(4xxxx)	Word 输入区：IWx 地址范围：S7-300(≥ 256) S7-400(≥ 512)	保持寄存器 4xxxx 地址范围：0~111	PROFIBUS (WORD) 输入与 MODBUS 保持寄存器 4xxxx 间
Output: N bits(0xxxx)	Bit 输出区：Qx.y 地址范围：S7-300(0-255) S7-400(0-511)	线圈 0xxxx 地址范围：0~1791	PROFIBUS (BIT) 输出与 MODBUS 线圈存储区 0xxxx 间
Output: N bits(1xxxx)	Bit 输出区：Qx.y 地址范围：S7-300(0-255) S7-400(0-511)	输入线圈 1xxxx 地址范围：0~1791	PROFIBUS (BIT) 输出与 MODBUS 输入线圈 1xxxx 间

Output: N Words(3xxxx)	Word 输出区 : QWx 地址范围 : S7-300(≥ 256) S7-400(≥512)	输入寄存器 3xxxx 地址范围 : 0~111	PROFIBUS (WORD) 输出与 MODBUS 输入寄存器 3xxxx 间
Output: N Words(4xxxx)	Word 输出区 : QWx 地址范围 : S7-300(≥ 256) S7-400(≥512)	保持寄存器 4xxxx 地址范围 : 0~111	PROFIBUS (WORD) 输出与 MODBUS 保持寄存器 4xxxx 间

5.4 MODBUS 报文详解

› 本节举例说明总线转换模块所支持的 MODBUS 报文的配置方法

槽号	PROFIBUS 主站读/写	PROFIBUS 地址	MODBUS 地址	MODBUS 主站读/写
1	status	IB0		诊断 MODBUS 通讯的状态
2	control	QB0		控制 MODBUS 通讯
3	PROFIBUS 主站只读	IB1 ~ IB3	00001 ~ 00024	执行 05H 或者 0FH 命令写线圈 00020 ~ 00043 , 存入 IB1 ~ IB3
4	PROFIBUS 主站只读	PIW256 ~ PIW263	40001 ~ 40004	执行 06H 或者 10H 写命令 写保持寄存器 40001 ~ 40004 , 存入 PIW256 ~ PIW263
5	PROFIBUS 主站只写	QB1	00025 ~ 00032	发 01H 命令读线圈 00025 ~ 00032
6	PROFIBUS 主站只写	QB2	10001 ~ 10008	发 02H 命令读线圈 10001 ~ 10008
7	PROFIBUS 主站只写	QB256 ~ QB265	30001 ~ 30005	发 04H 命令读输入寄存器 30001 ~ 30005
8	PROFIBUS 主站只写	QB266 ~ QB271	40005 ~ 40007	发 03H 命令读保持寄存器 40005 ~ 40007
9	force single bit(05hCommand)	QB2	站号:7 00001	发 05H 命令, 根据 Q2.0 置线 圈 00001
10	set single word(06hCommand)	PQW276	站号:8 40001	发 06H 命令, 将 PQW276 置入 保持寄存器 40001
11	MODBUS 从站状态表 (8 字节)	IB5 ~ IB12		8 个 MODBUS 从站通讯状态字

5.4.1 PROFIBUS 主站读取 MODBUS 主站 N 个输出线圈 0xxxx 状态

› 本例概述

MODBUS 主站向总线转换模块写入地址为 00001 ~ 00024 的线圈状态，总线转换模块将写入的线圈状态存放到 plc 地址为 IB1、IB2、IB3 中，PLC 读取数量为 24 个 Bits。

› 插入模块。

单击 3 号槽，然后双击目录栏中 PBMB-S-V1.0 下的 “Input:24 bits(0xxxx)” ，如图 5-6。其中的 I 地址一栏中的 “1...3” 表示本 MODBUS 从站的内部的数据，将会发送至 S7-300/CPU215-2DP 中 “IB1、IB2、IB3” 地址。

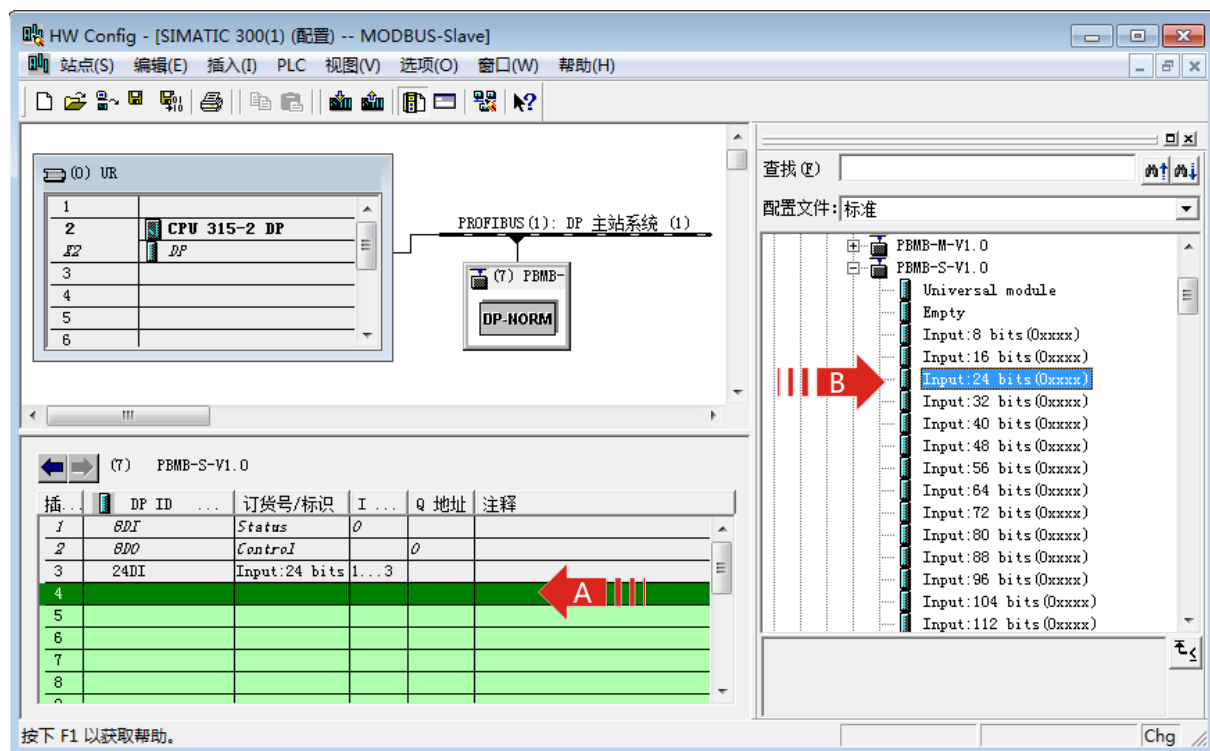


图 5-6

› PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS I1.0 ~ I3.7 (共 3x8=24bits) 与 MODBUS 线圈 00001 ~ 00024 间的对应关系，即从 PROFIBUS I1.0 ~ I3.7 可以读到本总线转换模块中的 MODBUS 线圈 00001~00024 地址的状态数据。关系如图 5-7。

注：MODBUS 一侧的地址是从 00001 开始依次分配的，如果再插入有一项 “24 bits in (0xxxx)” ，则 MODBUS 线圈地址顺序连续分配，即从 00025~00048，以此类推。

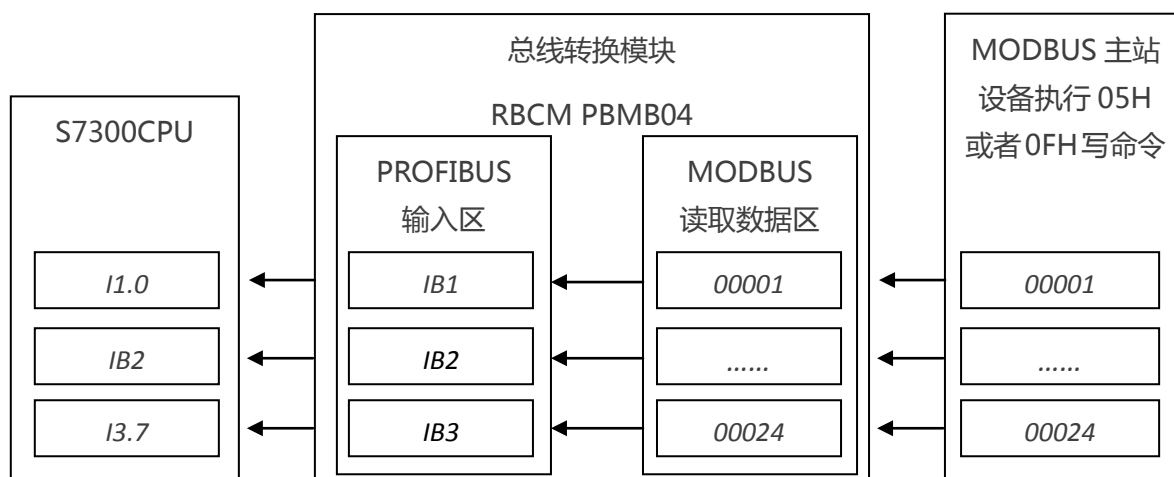


图 5-7

5.4.2 PROFIBUS 主站读取 MODBUS 主站 N 个保持寄存器 4xxxx 数据

› 本例概述

MODBUS 主站向总线转换模块写入保持寄存器地址为 40001 ~ 40004 的数据，总线转换模块将写入的数据存放到 plc 地址为 PIW256 ~ PIW263 中，PLC 读取数量为 4 个 Words。

› 插入模块。

单击 4 号槽，然后双击目录栏中 PBMB-S-V1.0 下的 “Input:4 Words(4xxxx)” ，如图 5-8。其中的 I 地址一栏中的 “256...263” 表示本 MODBUS 从站的内部的数据，将会发送至 S7-300/CPU215-2DP 中 “PIW256 ~ PIW263” 地址。

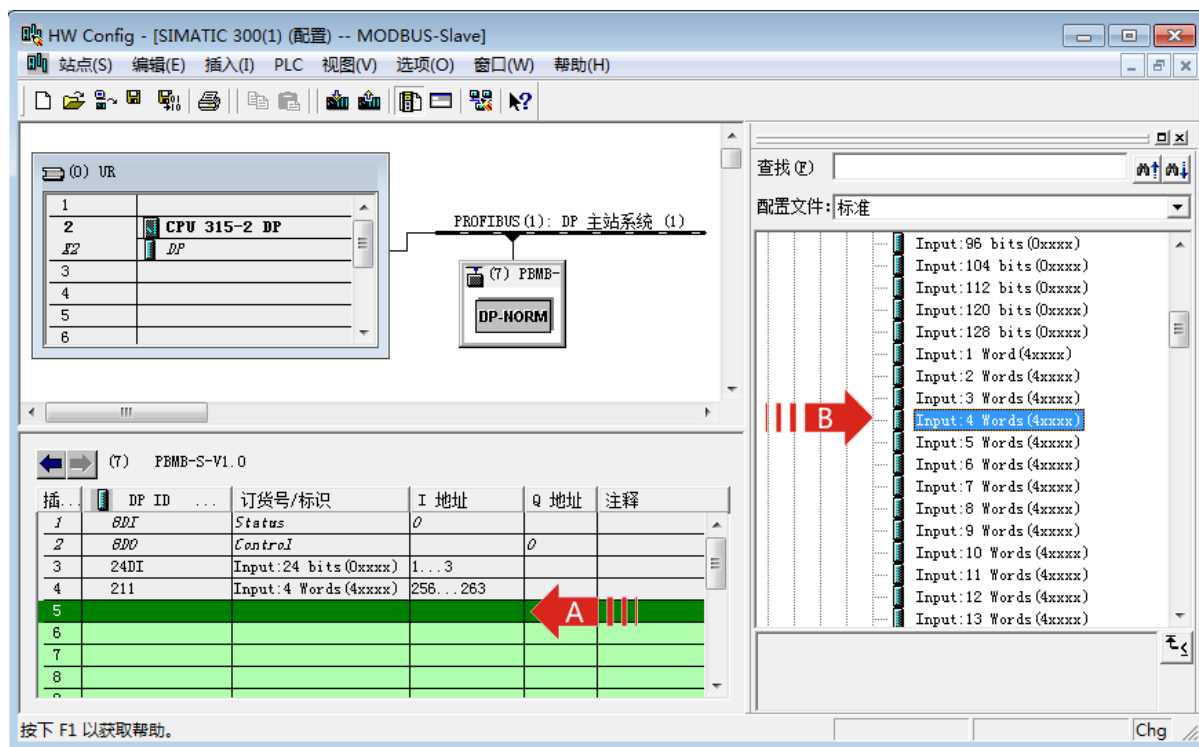


图 5-8

› PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS PIW256 ~ PIW263 (共 4Words) 与 MODBUS 线圈 40001 ~ 40004 间的对应关系，即从 PROFIBUS PIW256 ~ PIW263 可以读到本总线转换模块中的 MODBUS 线圈 40001 ~ 40004 地址的状态数据。关系如图 5-9。

注 :MODBUS 一侧的地址是从 40001 开始依次分配的 ,如果再插入有一项“Input:4 Words(4xxxx)” , 则 MODBUS 线圈地址顺序连续分配，即从 40005~40008，以此类推。

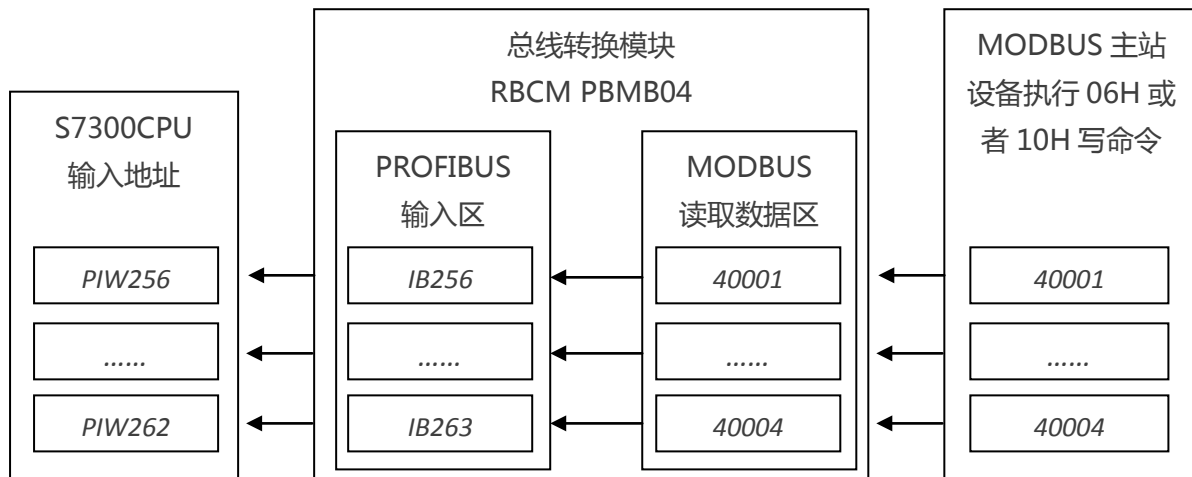


图 5-9

5.4.3 PROFIBUS 主站写入 MODBUS 主站 N 个线圈 0xxxx 状态

› 本例概述

PROFIBUS 主站向总线转换模块写入地址为 QB1 的线圈状态 ,总线转换模块将写入的线圈状态存放到 MODBUS 地址为 00025 ~ 00032 中供 MODBUS 主站读取 ,PLC 输出数量为 8 个 Bits。

› 插入模块。

单击 5 号槽，然后双击目录栏中 PBMB-S-V1.0 下的“Output:8 bits(0xxxx)”，如图 5-10。其中的 Q 地址一栏中的“1”表示 S7-300/CPU215-2DP 中“QB1”地址的数据，将会发送至本总线转换模块从站，共 1 个 Byte。

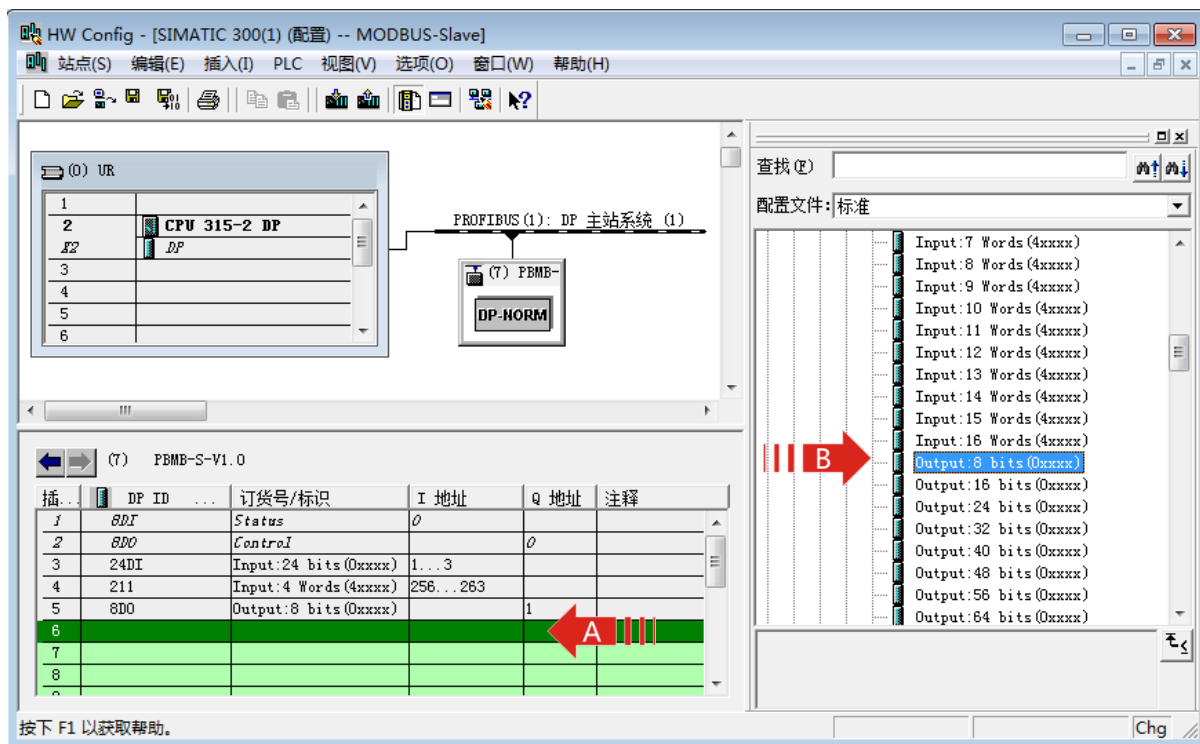


图 5-10

> PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS QB1 与 MODBUS 线圈 00025 ~ 00032 间的对应关系，即可以把数据写入 PROFIBUS 的 QB1，通过总线转换模块的数据交换，更新模块中的 MODBUS 线圈 00025 ~ 00032 地址的数据。关系如图 5-11。

注：因为在 3 号槽中已经插入 “Input:24 bits(0xxxx)”，占用了 00001 ~ 00024 所以 MODBUS 一侧的地址是从 00025 开始依次分配的。

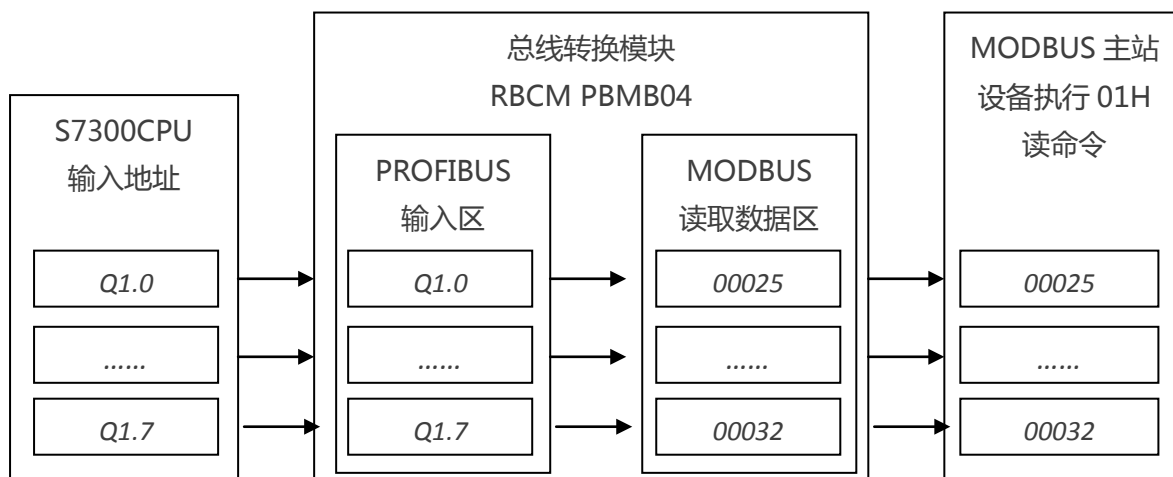


图 5-11

5.4.4 PROFIBUS 主站写入 MODBUS 主站 N 个输入线圈 1xxxx 状态

> 本例概述

PROFIBUS 主站向总线转换模块写入地址为 QB2 的输入线圈状态,总线转换模块将写入的线圈状态存放到 MODBUS 地址为 10001 ~ 10008 中供 MODBUS 主站读取,PLC 输出数量为 8 个 Bits。

› 插入模块。

单击 6 号槽,然后双击目录栏中 PBMB-S-V1.0 下的“Output:8 bits(1xxxx)”,如图 5-12。其中的 Q 地址一栏中的“2”表示 S7-300/CPU215-2DP 中“QB2”地址的数据,将会发送至本总线转换模块从站,共 1 个 Byte。

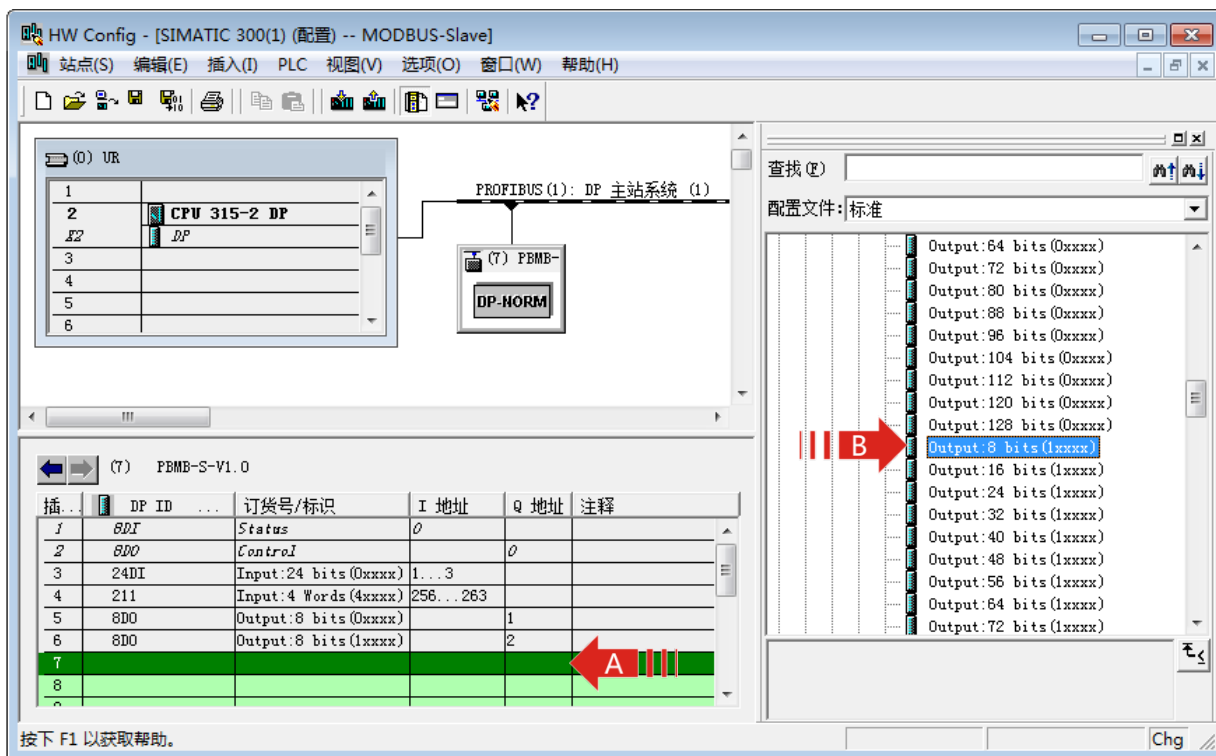


图 5-12

› PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS QB2 与 MODBUS 输入线圈 10001 ~ 10008 间的对应关系,即可以把数据写入 PROFIBUS 的 QB2,通过总线转换模块的数据交换,更新模块中的 MODBUS 线圈 10001 ~ 10008 地址的数据。关系如图 5-13。

注:MODBUS 一侧的地址是从 10001 开始依次分配的,如果再插入有一项“Output:8 bits(1xxxx)”,则 MODBUS 线圈地址顺序连续分配,即从 10009 ~ 10016,以此类推。

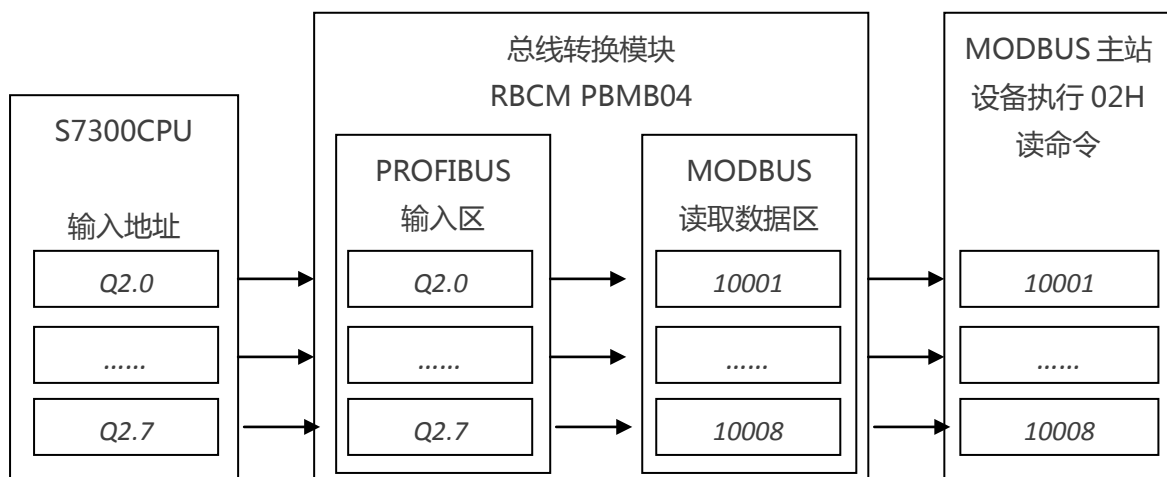


图 5-13

5.4.5 PROFIBUS 主站写入 MODBUS 主站 N 个输出寄存器 3xxxx 数据

› 本例概述

PROFIBUS 主站向总线转换模块写入地址为 QB256 ~ QB265 的输出寄存器数据，总线转换模块将写入的输出寄存器存放到 MODBUS 地址为 30001 ~ 30005 中供 MODBUS 主站读取，PLC 输出数量为 5 个 Words。

› 插入模块。

单击 7 号槽，然后双击目录栏中 PBMB-S-V1.0 下的 “Output:5Words(3xxxx)” ，如图 5-14。其中的 Q 地址一栏中的 “256...265” 表示 S7-300/CPU215-2DP 中 “QB256 ~ QB265” 地址的数据，将会发送至本总线转换模块从站，共 8 个 Byte，即 5 个 Words。

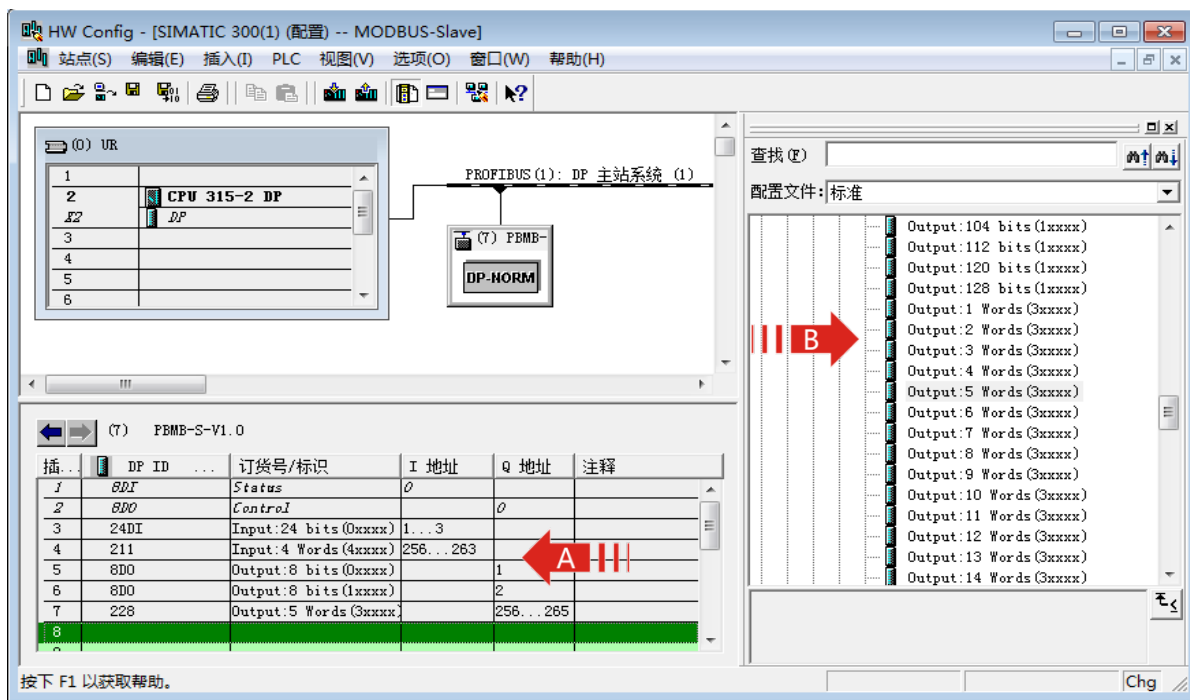


图 5-14

› PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS QB256 ~ QB265 与 MODBUS 输入寄存器 30001 ~ 30005 间的对应关系，即可以把数据写入 PROFIBUS 的 QB256 ~ QB265，通过总线转换模块的数据交换，更新模块中的 MODBUS 输入寄存器 30001 ~ 30005 地址的数据。关系如图 5-15。

注：MODBUS 一侧的地址是从 30001 开始依次分配的。如果再插入有一项“Output:5Words(3xxxx)”，则 MODBUS 输入寄存器地址顺序连续分配，即从 30006 ~ 30010，以此类推。

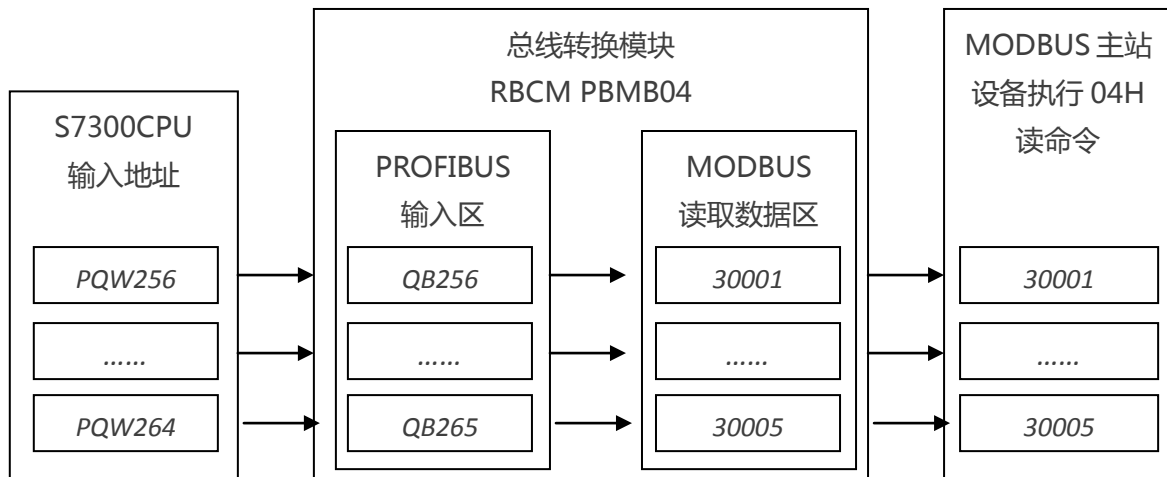


图 5-15

5.4.5 PROFIBUS 主站写入 MODBUS 主站 N 个保持寄存器 4xxxx 数据

› 本例概述

PROFIBUS 主站向总线转换模块写入地址为 QB266 ~ QB271 的保持寄存器数据，总线转换模块将写入的保持寄存器存放到 MODBUS 地址为 40005 ~ 40007 中供 MODBUS 主站读取，PLC 输出数量为 3 个 Words。

› 插入模块。

单击 8 号槽，然后双击目录栏中 PBMB-S-V1.0 下的“Output:3Words(4xxxx)”，如图 5-16。其中的 Q 地址一栏中的“266...271”表示 S7-300/CPU215-2DP 中“QB266 ~ QB271”地址的数据，将会发送至本总线转换模块从站，共 6 个 Byte，即 3 个 Words。

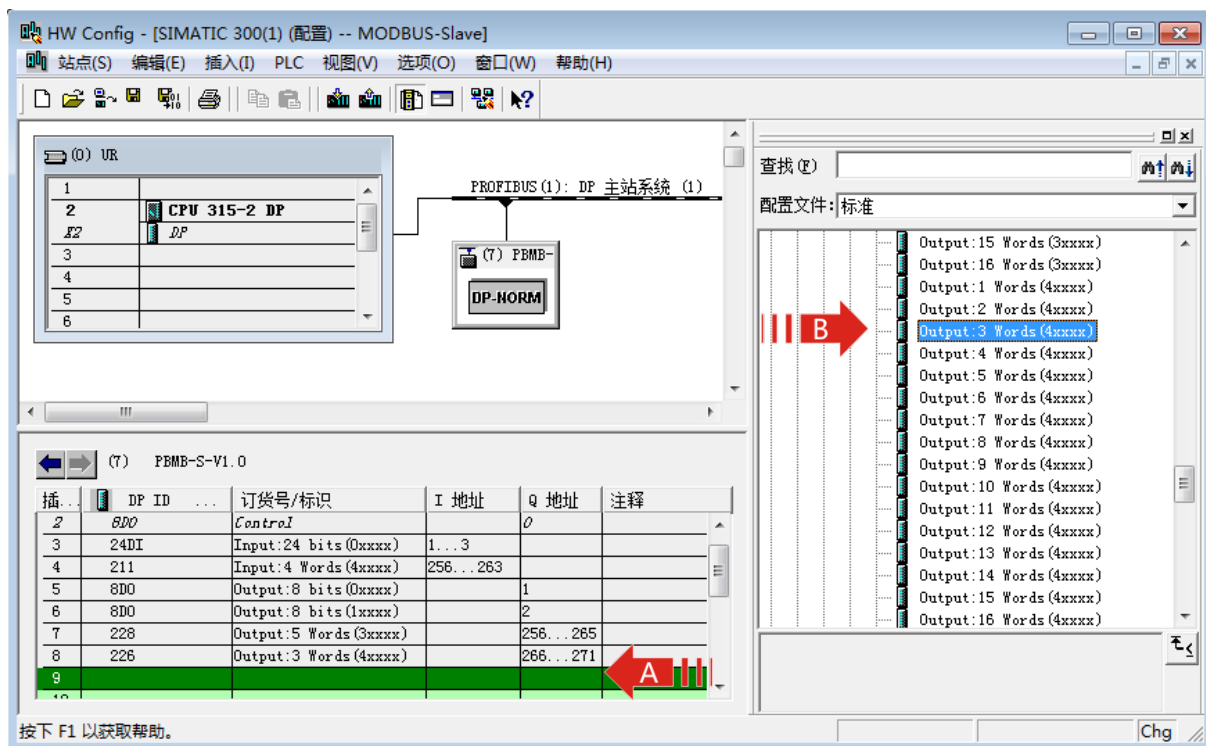


图 5-16

› PROFIBUS 地址与 MODBUS 地址对应关系

本 MODBUS 模块建立了 PROFIBUS QB266 ~ QB271 与 MODBUS 保持寄存器 40005 ~ 40007 间的对应关系，即可以把数据写入 PROFIBUS 的 QB266 ~ QB271，通过总线转换模块的数据交换，更新模块中的 MODBUS 保持寄存器 40005 ~ 40007 地址的数据。关系如图 5-17。

注：因为在 4 号槽中已经插入 “Input: 4 Words(4xxxx)”，占用了 40001 ~ 40004 所以 MODBUS 一侧的地址是从 40005 开始依次分配的。

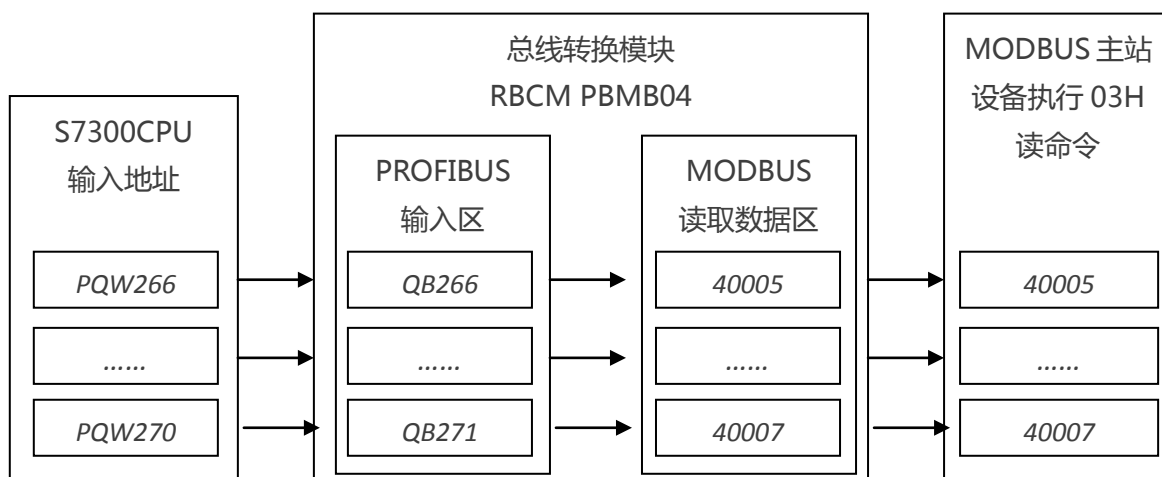


图 5-17

5.4.7 保存并编译

› 此时，系统已配置完毕。点击菜单栏中的“站点->保存并编译(M)”保存并编译。如图 5-19 所示。

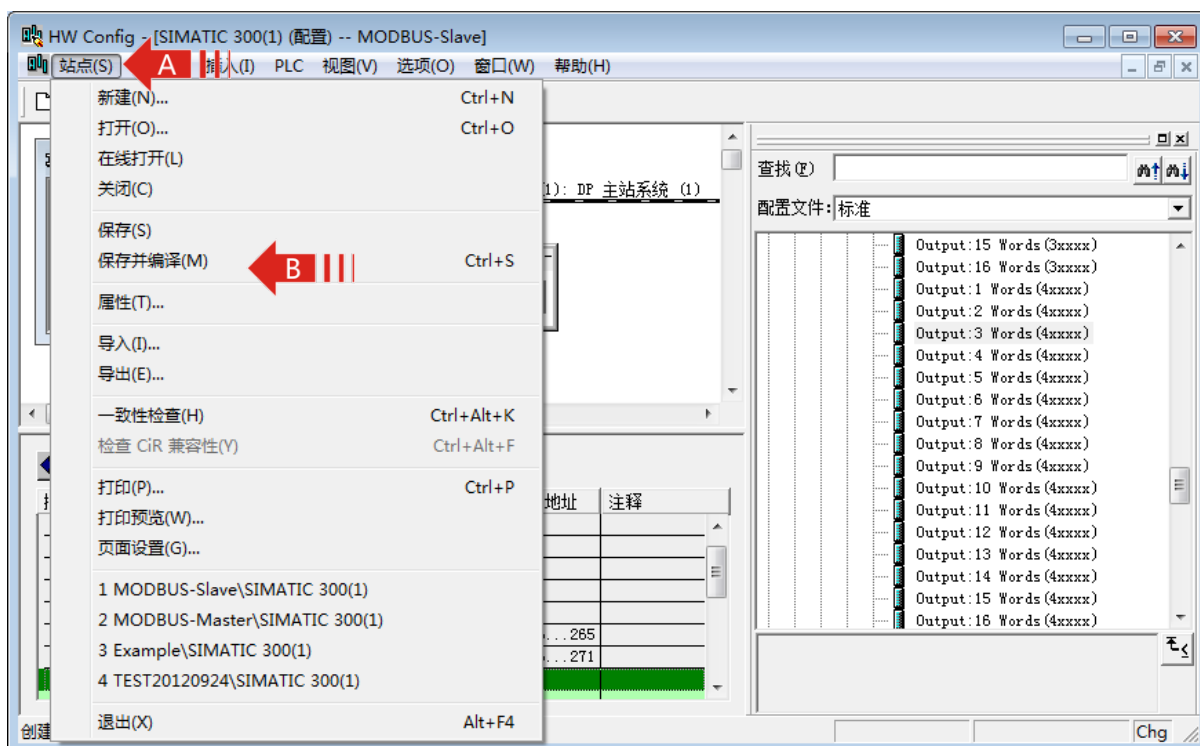


图 5-19

5.5 通信状态字与通信控制字

5.5.1 通信状态字与通信控制字

从系统配置中可以看到 1 槽和 2 槽已被占用，其中 1 槽为一字节输入，对应的 PROFIBUS 输入地址 IB0，作为本协议桥的通信状态字 (status)。2 槽为一字节输出，对应的 PROFIBUS 输入地址 QB0，作为本协议桥的通信控制字 (control)。如图 5-19 所示。

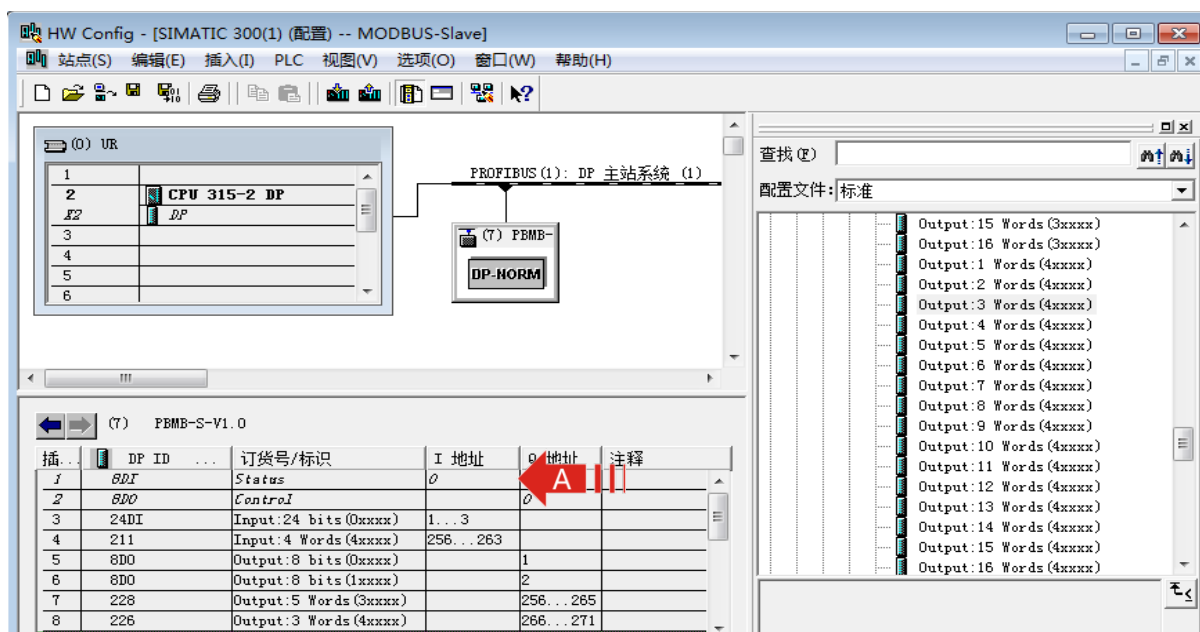


图 5-19

5.5.2 通信状态字格式

Bit7	Bit 6	Bit 5	Bit 4- Bit 1	Bit 0
奇偶校验错误	CRC 校验错误	保留功能	异常应答码	接收或发送状态指示

注：当通信正常之后，即使所有的报文都可以正常应答，且无错误发生，这些位并不会自动清零，需要使用通信控制字中的清除错误标记位才能将这些位清零。

Bit 0

1：本总线转换模块处在发送报文或等待接收状态。

0：本总线转换模块处在接收报文或处理接收到的报文状态。

Bit 4- Bit 1

MODBUS 从机无法正确执行 MODBUS 主机发送的命令时，将返回 4bit 的异常应答码。详见 MODBUS 技术简介。整个报文队列最多可以有 37 条 MODBUS 报文，但是只有一个状态字所以当有新的异常应答出现时，之前的异常应答状态码会被覆盖。

Bit 5

保留功能。

Bit 6

接口收到的 MODBUS 报文 CRC 校验出现错误，本位置 1，并将收到的报文丢弃。

Bit 7

接口收到的字节奇偶校验错误，本位置 1，并将收到的报文丢弃。

5.5.3 通信控制字格式

Bit7-Bit 6	Bit 5	Bit 4-Bit 1	Bit 0
保留功能	清除错误	保留功能	PRIFIBUS 输出有效

Bit 0

1：PRIFIBUS 输出有效，启动总线转换模块内部数据交换。

0：PRIFIBUS 输出无效，关闭总线转换模块内部数据交换。

Bit 4- Bit 1

保留未用。

Bit 5

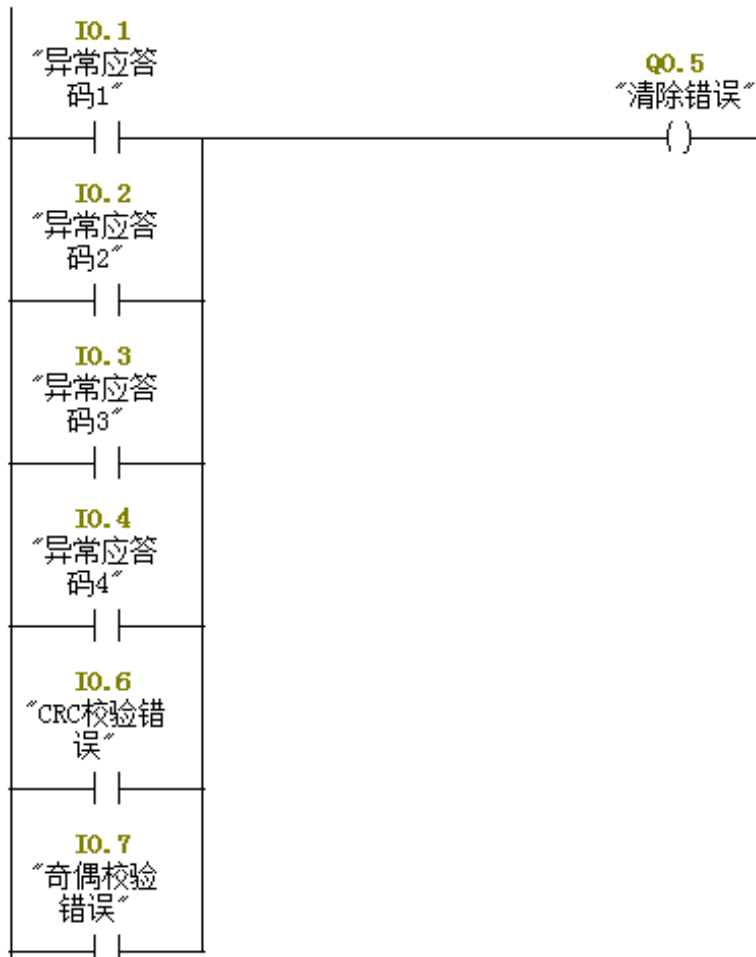
置 1 的时候将通信状态字中的 Bit7-Bit1 清零。

Bit 7- Bit 6

保留未用。

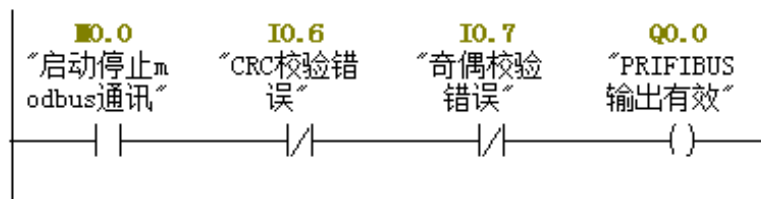
程序段 1: 标题:

当用modbus有通讯错误发生时，状态字相对应的错误位置1，程序自动清除错误位。



程序段 2: 标题:

M0.0可以控制总线转换模块的工作启动停止，当无CRC校验错误和奇偶校验错误时，模块开始工作。



5.5.3 利用 USB 监测测模块通信状态

> USB 口监测功能

- 监测 PROFIBUS 总线通信状态。
- 监测模块通信状态，提示操作信息。
- 显示通信串口收发报文的数据信息。

› 对 USB 口操作

- 用 USB 线连接模块与计算机。模块 USB 接口为 micro 型。
- 安装 USB 口驱动程序，驱动程序名称“监视 USB 驱动程序 CH341SER”可以向厂商索取。
- 安装串口调试助手软件，可以向厂商索取。



图 5-20

-串口调试助手软件的设置

串口号：在计算机硬件列表中可以查询到 340USB 串口的串口号。

串口设置：波特率 115.2K；数据位 8 位；停止位 1 位；无校验位；无流控制。不可设置其他参数

HEX 显示：不选择 HEX 显示

打开串口，即可监视到模块数据。关闭串口。即可查询前面的数据信息。

注：在模块断电前要关闭串口调试软件的串口，否则会造成串口调试软件死机。

5.6 MODBUS 通讯故障及排除

› 在检测MODBUS通讯故障之前首先要确定总线转换模块要与PROFIBUS主站通讯正常，也就是说 PROFIBUS故障指示灯BF不亮，正确指示灯BC常亮。如果与PROFIBUS主站通讯不正常，那么 MODBUS是不能进行通讯的。

5.6.1 MODBUS 接口不工作

› 产生原因

MODBUS接口无数据发送和接收。

› 故障现象

—MODBUS 通讯发送灯 TD 和接收灯 RD 无闪烁。

› 解决方法

—PROFIBUS 通讯接口是否正常。

—控制字“D0：PRIFIBUS 输出有效”是否置 1，见 5.5.2 控制字。

—MODBUS 通讯地址是否与主站读取的地址一致。

—MODBUS 通讯波特率是否与主站一致。

5.6.2 CRC 校验错误

› 产生原因

总线转换模块接收到的 MODBUS 主站报文有字符 CRC 校验错。

› 故障现象

—如果总线转换模块收到的MODBUS主站报文有字符CRC校验错，总线转换模块认为此发送报文数据不可靠，将拒绝回答MODBUS报文，视为此次通信无效，继续等待下一条主站报文。同时将通信状态字“D6: CRC校验错误”置1。

› 解决方法

—字符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“D5：清错误标记”=1 将错误标记清除。“D5：清错误标记”保持为1，将保持清除错误标记功能有效。

—减少外部环境对总线的电磁干扰。

5.6.3 奇偶校验错误

› 产生原因

总线转换模块收到的 MODBUS 主站报文有字符奇偶校验错误。

› 故障现象

—如果总线转换模块收到的MODBUS主站报文有字符奇偶校验错，总线转换模块认为此回答报文数据不可靠，拒绝将回答MODBUS报文，视为此次通信无效，继续等待下一条主站报文。同时将通信状态字“D7: 奇偶校验错误”置1。

› 解决方法

—字符奇偶校验错误不影响MODBUS扫描进行，但错误标志将保留。可以使用控制字“D5：清错误标记”=1 将错误标记清除。“D5：清错误标记”=1 不影响MODBUS 扫描器。“D5：清错误标记”保持为1，将保持清除错误标记功能有效。

—减少外部环境对总线的电磁干扰。

5.6.4 MODBUS 异常应答

› 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。

› 故障现象

—从机将以“异常应答”回答之。见“附录B MODBUS 技术简介 B.3异常应答”。同时将异常码存放通信状态字D4 ~ D1。

注: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。

› 解决方法

—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。可以使用控制字“D5：清错误标记” =1 将错误标记清除。

引言

本章阐述了产品常见的故障及排除的方法。

6.1 电源及 PROFIBUS 故障及排除方法

6.1.1 总线转换模块的电源指示灯 P 不亮

- › 正常状态：总线转换模块在正常供电情况下，电源指示灯P常亮。
- › 排除方法：
 - 检测供电是否正常，额定供电电压为DC24V。
 - 内部硬件故障，返回厂家维修。

6.1.2 总线转换模块与 PROFIBUS 主站通信故障

- › 排除方法：
 - PROFIBUS通讯接口是否连接正确，是否连接可靠。
 - PROFIBUS通讯总线的两端是否接入终端电阻。
 - 是否正确的在PLC主站中配置了该接口模块。
 - 总线转换模块的设定地址是否与PROFIBUS主站软件配置的地址相同。
 - 内部硬件故障，返回厂家维修。

6.1.3 总线转换模块的 PROFIBUS 的通讯指示灯 BF 亮，BC 不亮

- › 正常状态：如果与PROFIBUS主站正常通讯，红色BF通讯故障指示灯不亮，绿色BC通讯正确指示灯亮
- › 排除方法：与6.1.2接口模块与PROFIBUS主站通信故障的处理方法相同

6.2 MODBUS 通讯故障及排除方法

6.2.1 MODBUS 通讯接口在主站工作模式下的故障及排除方法

- › 见“4.8 MODBUS通讯故障及排除”章节。

6.2.2 MODBUS 通讯接口在从站工作模式下的故障及排除方法

- › 见“5.6MODBUS 通讯故障及排除”章节。

附录

A 产品订货一览表

B MODBUS 协议简介

使用本产品不必了解MODBUS 的技术细节，如果读者仅从使用产品角度出发，可以只阅B.4以后的部分。

B.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；

应用层	-----→	MODBUS 报文格式规范
表示层		
会话层		
传输层		
网络层		
数据链路层	-----→	MODBUS 主/从
物理层	-----→	RS232/485

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。

B.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；

注：本产品只能用于 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	

B.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。

B.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	0001 ~ 0XXXX
1XXXX	输入线圈	位	只读	1001 ~ 1XXXX
3XXXX	输入寄存器	字	只读	3001 ~ 3XXXX

4XXXX	保持/输出寄存器	字	读/写	40001 ~ 4XXXX
-------	----------	---	-----	---------------

B.5 MODBUS功能

即MODBUS 应用层，规定了MODBUS 报文格式和服务功能。

B.5.1主要功能码

功能码	功能	操作地址区域	操作类型
01H	读取多个线圈输出状态	0XXXX	读
02H	读取多个输入线圈状态	1XXXX	读
03H	读取多个保持寄存器	4XXXX	读
04H	读取输入寄存器	3XXXX	读
05H	强置单个线圈	0XXXX	写
06H	预置单个保持寄存器	4XXXX	写
0FH	强置多线圈	0XXXX	写
10H	预置多个保持寄存器	4XXXX	写

B.5.2功能码详解

(1) 读取多个线圈输出状态

功能码：01H

主站询问报文格式

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
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，报文起始地址=0013H=19，对应MODBUS设备地址00020；线圈数=0025H=37；MODBUS设备末地址=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= 00011011，前面三位填0，后五位对应00052-00056；

(2) 读取多个输入线圈状态

功能码：02H

主站询问报文格式：

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
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，报文起始地址=00C4H=196，对应MODBUS设备地址10197；线圈数=0016H=22，MODBUS设备末地址=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，报文起始地址=006BH=107，对应MODBUS设备地址40108；寄存器数=0003；MODBUS设备末地址=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，报文起始地=0008H=0008，对应MODBUS设备地址30009；寄存器数=0001；MODBUS设备末地址=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30009 高位	输入寄存器30009 低位	CRC
11	04	02	01	01	XXXX

功能：从站返回输入寄存器30009 的值；（30009）=0101H

(5) 强置单个线圈

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。

注意：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：报文起始地址=00AC(H)=172，对应MODBUS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) 预置单个保持寄存器

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。

注意：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(135)	03	9E	XXXX

功能：预置17 号从机保持寄存器40136值=0x039E后原文返回。

(7) 读取异常状态

功能码：07H

本产品暂不支持这一功能。

(8) 回送校验

功能码：08H

本产品暂不支持这一功能。

(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

本产品暂不支持这一功能。

(11) 强置多个线圈

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，报文线圈起始地址=0013H=19，对应MODBUS设备地址00020；线圈数=000AH=10；MODBUS设备末地址=00020+10-1=00029；

因此，本询问报文功能是：强置17 (11H) 号从站MODBUS设备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) 预置多个寄存器

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，报文寄存器起始地址=0087H=135，对应MODBUS设备地址40136，线圈数=0002H=2，MODBUS设备末地址=40135+2-1=40137；

因此，本询问报文功能是：预置17 (11H) 号从站，MODBUS设备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

REDTECH 瑞德泰科

www.redtech.cn

沈阳瑞德泰科电气有限公司 SHENYANG REDTECH ELECTRIC CO., LTD.

> 电话：024-64691655 024-64691665 > 传真：024-64691675
> 地址：沈阳市铁西区云峰北街4-1号12A-2 > 邮编：110025
> 邮箱：service@redtech.cn



• 宣传册中涉及的所有名称可能是瑞德泰科公司或其供应商的商标或产品名称，如果第三方擅自使用，可能会侵犯所有者的权利。
• 最新的产品信息请关注瑞德泰科公司网站。

如有变动，恕不事先通知。