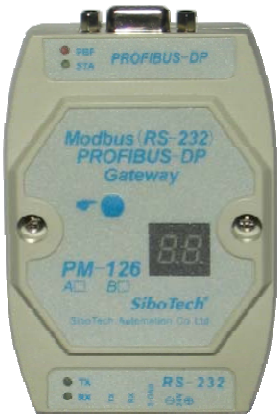
Modbus(RS232)/PROFIBUS-DP 网关

PM-126B

产品手册

REV 1.0

2010 年 7 月



上海泗博自动化技术有限公司

Sibotech Automation Co., Ltd

技术支持热线:021-5102 8348

E-mail: support@sibotech.net

目　录

一、引言 2
1.1 关于说明书 2
1.2 版权信息 2
1.3 相关产品 2
1.4 术语 2
二、产品概述 3
2.1 产品功能 3
2.2 产品特点 3
2.3 技术指标 3
2.4 电磁兼容性能 4
2.4.1 高频干扰试验(GB/T15153.1 classIII) 4
2.4.2 快速瞬变脉冲群试验(GB/T17626.4 classIII) 4
2.4.3 静电放电干扰(GB/T 17626.2 classIII) 4
2.4.4 辐射电磁场(GB/T 17626.3 classIII) 5
三、产品外观 6
3.1 产品外观 6
3.2 指示灯 6
3.3 按钮和数码管 7
3.4 通信端口 7
3.4.1 RS-485 端口 7
3.4.2 PROFIBUS-DP 端口 8
四、快速应用指南 9
五、Profibus-DP 主站组态界面参数设置 10
5.1 参数设置说明 10
5.2 参数设置步骤 10
5.2.1 创建新工程 10
5.2.2 注册 GSD 文件 13
5.2.3 组态设置 15
5.2.4 参数设置 19
六、Modbus 主、从站工作原理 26
6.1 Modbus 主站工作原理 26
6.2 Modbus 从站工作原理 26
七、Step7 如何读写网关数据 28
八、安装 29
8.1 机械尺寸 29
8.2 安装方法 29
九、运行维护及注意事项 31
附录：Modbus 协议 32

一、引言

1.1 关于说明书

本说明书描述了网关 PM-126B 的各项参数，具体使用方法和注意事项，方便工程人员的操作运用。在使用网关之前，请仔细阅读本说明书。

1.2 版权信息

本说明书中提及的数据和案例未经授权不可复制。泗博公司在产品的发展过程中，有可能在不通知用户的情况下对产品进行改版。

SiboTech是上海泗博自动化技术有限公司的注册商标。

该产品有许多应用，使用者必须确认所有的操作步骤和结果符合相应场合的安全性，包括法律方面，规章，编码和标准。

1.3 相关产品

本公司其它相关产品包括：

PM-125，PM-127，PM-126A，PM-160 等

获得以上几款产品的说明，请访问公司网站www.sibotech.net，或者拨打技术支持热线：021-5102 8348

1.4 术语

PROFIBUS-DP：PROFIBUS-DP 协议

RS232：一种串口的硬件规范

PM-126A：Modbus(RS232)/PROFIBUS-DP 网关，使用 GT-123 配置

PM-126B：Modbus(RS232)/PROFIBUS-DP 网关，使用 Step7 参数配置

二、产品概述

2.1 产品功能

网关 PM-126B 实现了串口和 PROFIBUS-DP 的数据通信。可连接具有 **Modbus RTU**（RS232）接口的设备到 PROFIBUS-DP，即将 Modbus/RS232 网络设备转换为 PROFIBUS-DP 网络设备。

2.2 产品特点

▼**应用广泛：**凡具有 RS232 接口的 Modbus RTU 协议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：**用户不必了解 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。

2.3 技术指标

[1] PM-126B 网关在 PROFIBUS 侧是一个 PROFIBUS-DP 从站，在 Modbus 一侧是 MODBUS 主、从站可设；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。

[2] PM-126B 网关作为 Modbus 主站，支持 01H、02H、03H、04H、05H、06H、0FH、10H 号功能码；**最多可配置 48 条 Modbus 命令**；

[3] PM-126B 网关作为 Modbus 从站，支持 Modbus 寄存器地址 3 区（3xxxx）、4 区（4xxxx）、0 区（0xxxx）和 1 区（1xxxx）；其中，3 区支持功能码 04H；4 区支持功能码 03H、06H、10H；0 区支持功能码 01H、05H、0FH；1 区支持功能码 02H；

[4] PROFIBUS-DP/V0 协议，符合；JB/T 10308.3-2001：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；

[5] PROFIBUS-DP 从站，波特率自适应，支持波特率范围：9600～12Mbps；

[6] PROFIBUS 输入/输出字节数可通过 Step7 自由设定，最大 PROFIBUS 输入/输出：

①Max Input Bytes ≤244Bytes

②Max Output Bytes ≤244 Bytes

③Max Data Bytes ≤488 Bytes

[7] 状态监视功能：作为 Modbus 主站，Profibus 端可以监视 Modbus 命令状态；作为 Modbus 从站，Profibus 端可以监视 Modbus 网络状态。

[8] MODBUS 协议接口是 RS-232 接口，半双工；波特率：300，600，1200，2400，9600，19200，38400，57600，115200bps 可选；8 位数据位；校验位(偶、奇、无、标记、空格)可选；停止位（1、2）可选；

[9] 供电：24VDC（11V-30V），80mA（24V DC）

[10] 工作环境温度：-20℃～60℃，相对湿度 5%～95%（无凝露）

[11] 外形尺寸：100mm（长）×70mm（宽）×25mm（深）

[12] 安装：35mm 导轨

[13] 防护等级：IP20

2.4 电磁兼容性能

2.4.1 高频干扰试验(GB/T15153.1 classⅢ)

施加场所	电源输入回路–对地 电源输入回路之间 交流输入回路–对地	
施加波形	第 1 波波高值 振荡频率 1/2 衰减时间 重复频度 试验设备输出阻抗	2.5～3kV 1.0～1.5MHz ≥6μs 50 回以上/s 150～200Ω

2.4.2 快速瞬变脉冲群试验(GB/T17626.4 classⅢ)

电压峰值	电源输入和交流加入回路：2kV 弱电回路：1kV
重复频率	5 kHz

2.4.3 静电放电干扰(GB/T 17626.2 classⅢ)

施加场所	通常运用时,操作者触及部分
电压、电流	6kV 接触放电，放电的第一个峰值电流 22.5A

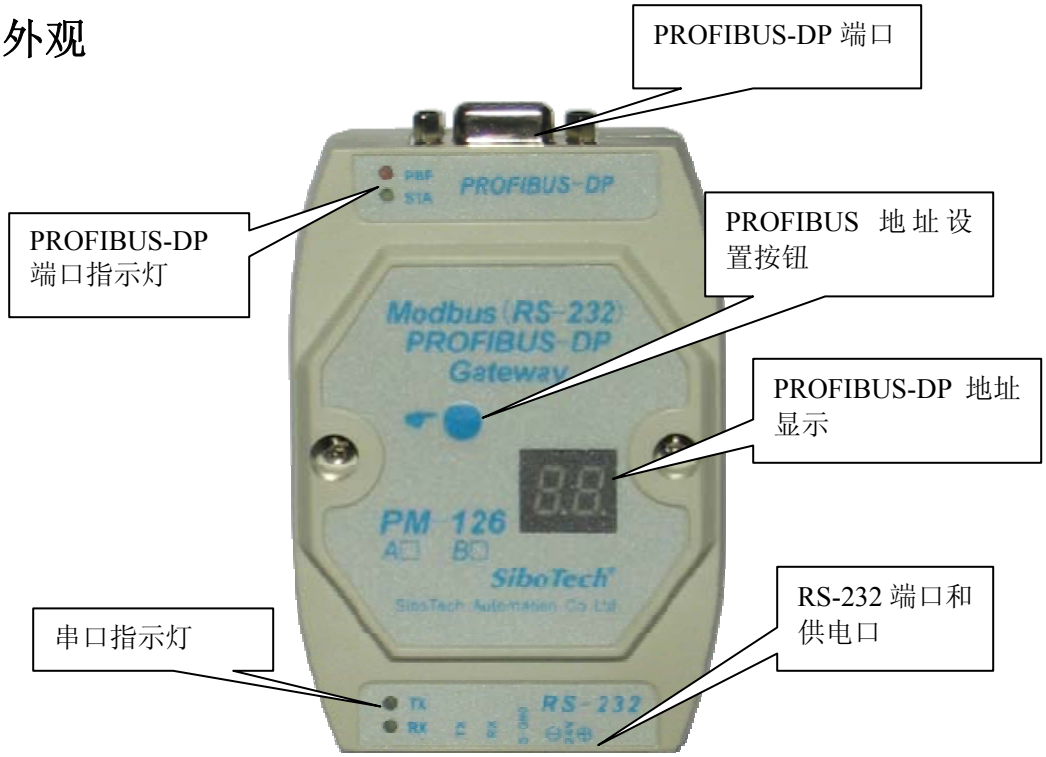
次数	每处 1 秒以上的间隔 10 回以上
极性	正极性

2.4.4 辐射电磁场(GB/T 17626.3 classⅢ)

电波频率	150MHz, 400MHz, 900MHz
试验场强	10 V/m
辐射方法	使得天线前端触碰装置,或接近端子,断续辐射电波

三、产品外观

3.1 产品外观



3.2 指示灯

指示灯	状态	含义
STA	绿灯闪烁	PROFIBUS-DP 总线上有数据通信
	绿灯灭	无数据通信
PBF	红灯常亮	PROFIBUS-DP 总线数据通信失败
	红灯灭	数据通信正常
RX	绿灯闪烁	串口接收有数据
	绿灯灭	串口无接收数据
TX	绿灯闪烁	串口发送有数据
	绿灯灭	串口无发送数据

3.3 按钮和数码管

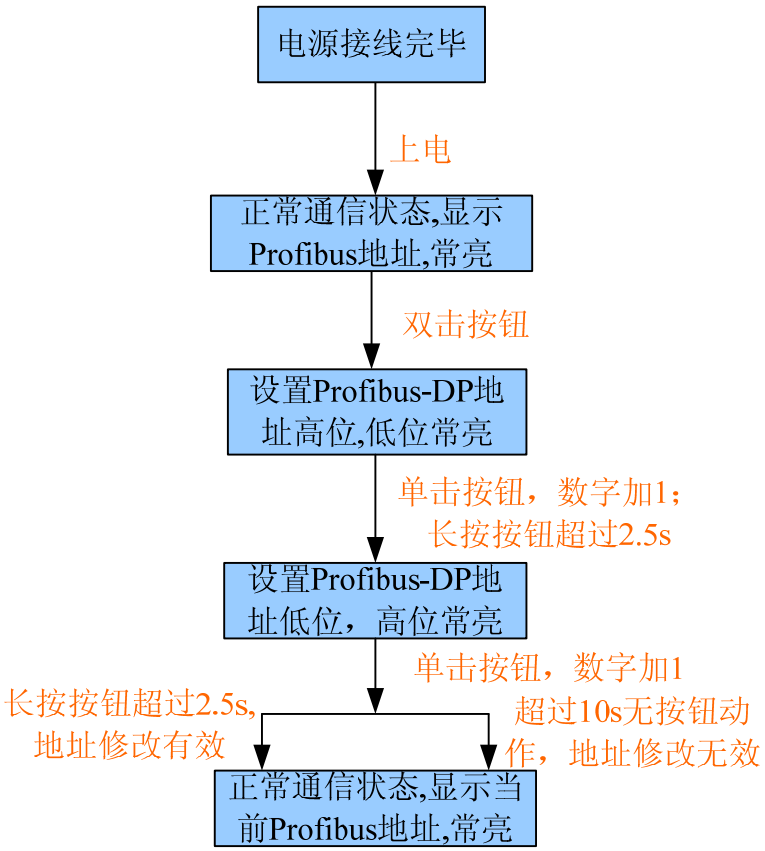
- 按钮功能：进入 Profibus-DP 地址修改模式并修改模块的 Profibus-DP 地址。
- 数码管功能：显示当前 Profibus-DP 地址。

PM-126B 上电后默认是正常通信模式，数码管显示 Profibus 地址，常亮。

双击按钮进入 Profibus 地址设置状态（数码管高位闪烁，低位常亮），单击按钮数字加一，长按按钮超过 2.5s 切换到设置低位地址（数码管高位常亮、低位闪烁），单击按钮数字加一，长按按钮超过 2.5s 保存新设置的地址使其生效，并进入正常状态常亮显示。

除正常状态外的其他状态，超过 10s 无按钮动作，自动不保存退出当前状态进入正常状态。

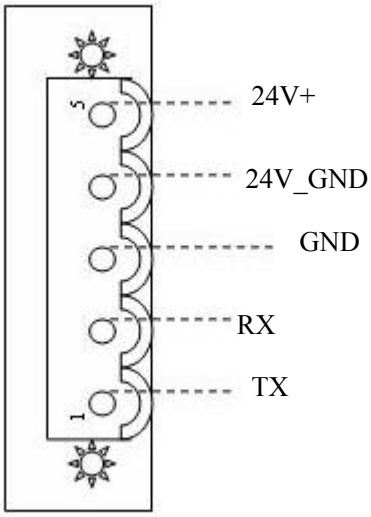
按钮、数码管设置方法如下：



3.4 通信端口

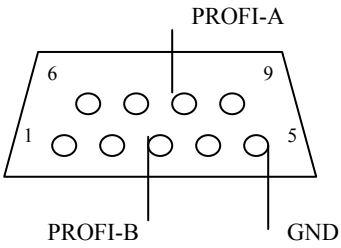
3.4.1 RS-232 端口

PM-126B产品的RS-232接口使用5针可插拔端子中的3针，其引脚描述如下：



引脚	功能
1	TX，接用户设备RS232的RX
2	RX，接用户设备RS232的TX
3	GND，接用户设备RS232的GND
4	24V_GND，电源地
5	24V+，电源正

3.4.2 PROFIBUS-DP 端口



DB9 引脚	功能
3	PROFI_B，数据正
5	GND （可选连接）
8	PROFI_A，数据负

四、快速应用指南

以下几个步骤可以快速应用您的 PM-126B：

1. 给 PM-126B 上电，双击按钮，进入 Profibus-DP 地址设置模式，按照本说明书 3.3 章节说明设置 PM-126B 的 Profibus-DP 地址。
2. 把 GSD 文件导入到您的 PROFIBUS 组态软件中，PM-126B 作为 Modbus 主站和从站时的 GSD 文件不同，请根据需要导入正确的 GSD 文件。
3. 在 PROFIBUS 组态软件中，设置 Profibus-DP 从站地址；根据您的需要配置 Modbus 通讯参数及读、写命令，即将 PM-126B 相应的输入输出映射到 PLC 或其它 Profibus 主站设备的内存中。
4. 按照第三章 RS-232 端口的说明，关闭电源，正确连接 5 针端子的每个引脚的相应接线。
5. 按照第三章 PROFIBUS-DP 端口的说明，正确连接至少 3 和 8 两个引脚。
6. 连接好 Modbus 设备和 Profibus-DP 通信线，给 PM-126B 上电，进入正常通信状态。

五、Profibus-DP 主站组态界面参数设置

5.1 参数设置说明

在 Profibus-DP 主站组态界面中需要设置的参数包括：Profibus-DP 从站属性参数、Modbus 命令 Module 参数。

Profibus-DP 从站属性参数包括 Modbus 通讯波特率、串口参数、等待响应时间、轮询延时时间以及 Modbus 从站地址（从站时有效）。

Modbus 命令 Module 参数：当为 Modbus 主站时，Modbus 命令 Module 参数包括：从站地址、功能码、起始地址以及数据个数。

5.2 参数设置步骤

5.2.1 创建新工程

1. 打开 SIMATIC Manager ，如图 1：

图 1

2. 点击 File->New, 新建一个工程，如图 2：

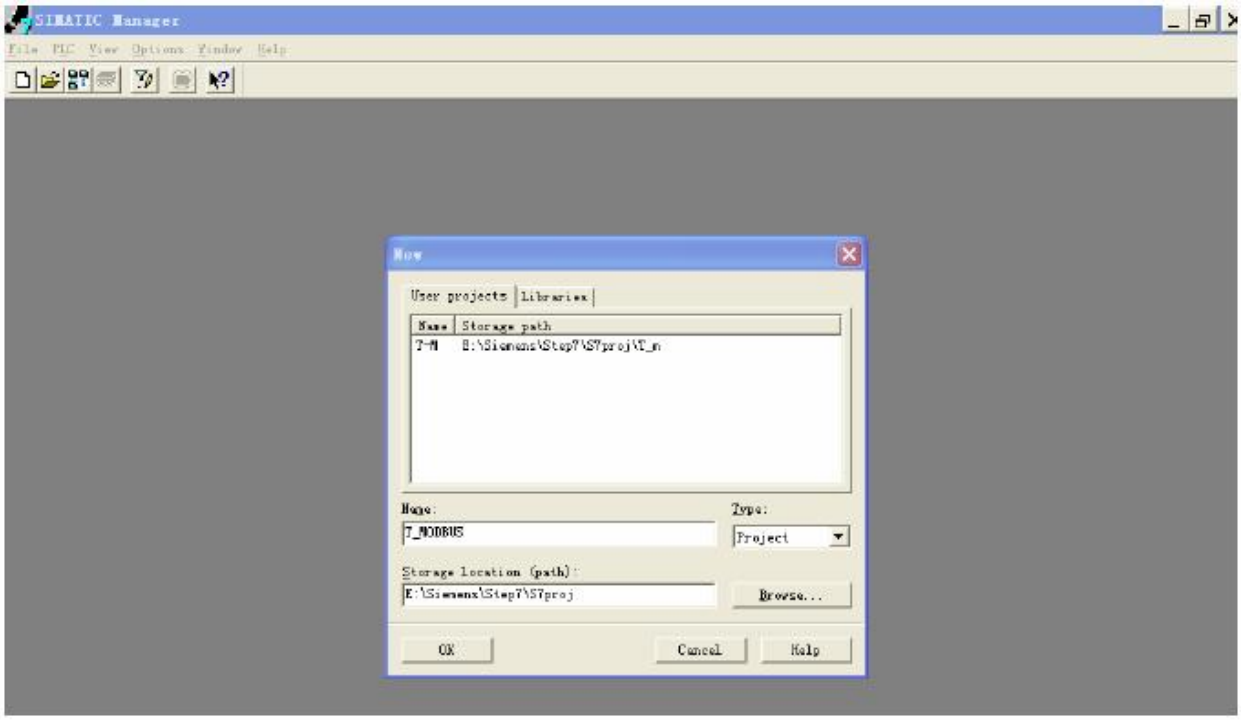


图 2

3. Insert->Station->SIMATIC 300 Station.，如图 3：

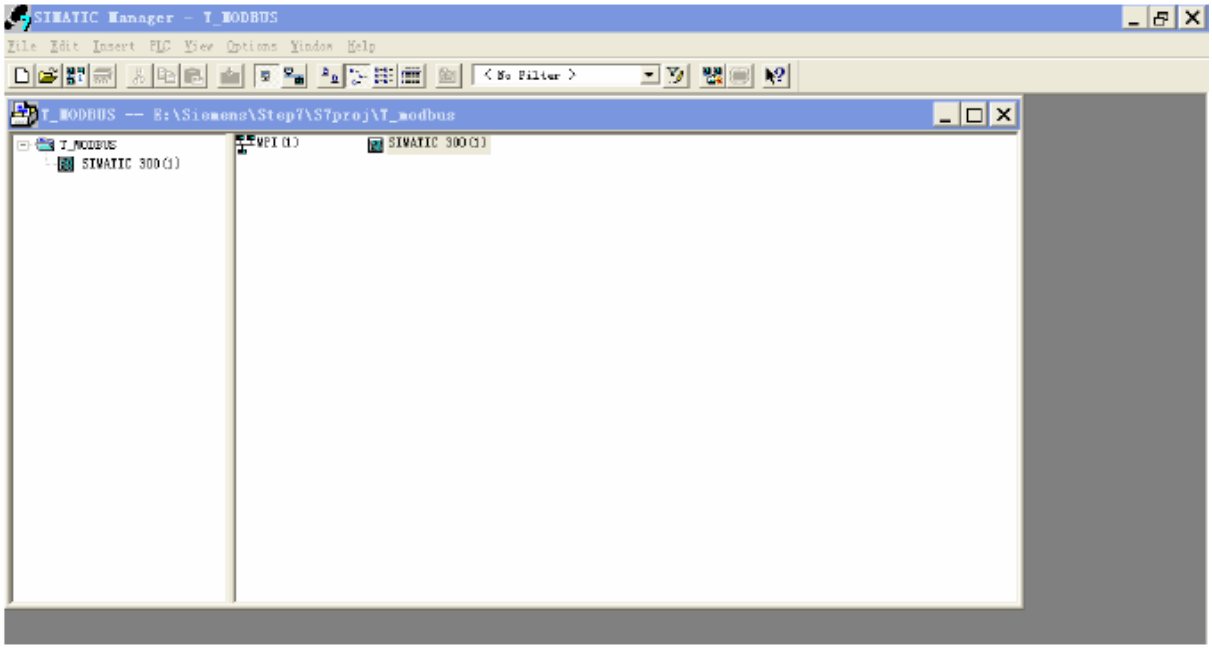


图 3

4. 双击 SIMATIC 300(1)->Hardware，打开 S7 PLC 硬件组态界面，如图 4：

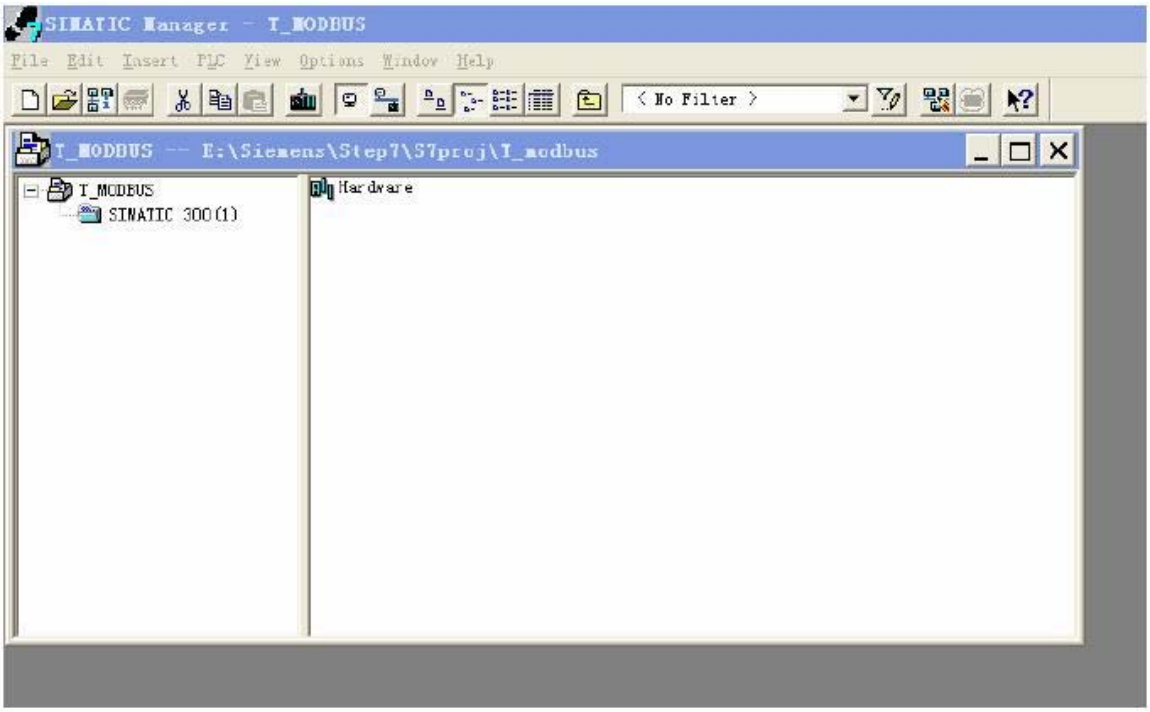


图 4

5. 弹出的组态界面如图 5 所示，注册 GSD 文件之前应该关闭当前工程的组态窗口。

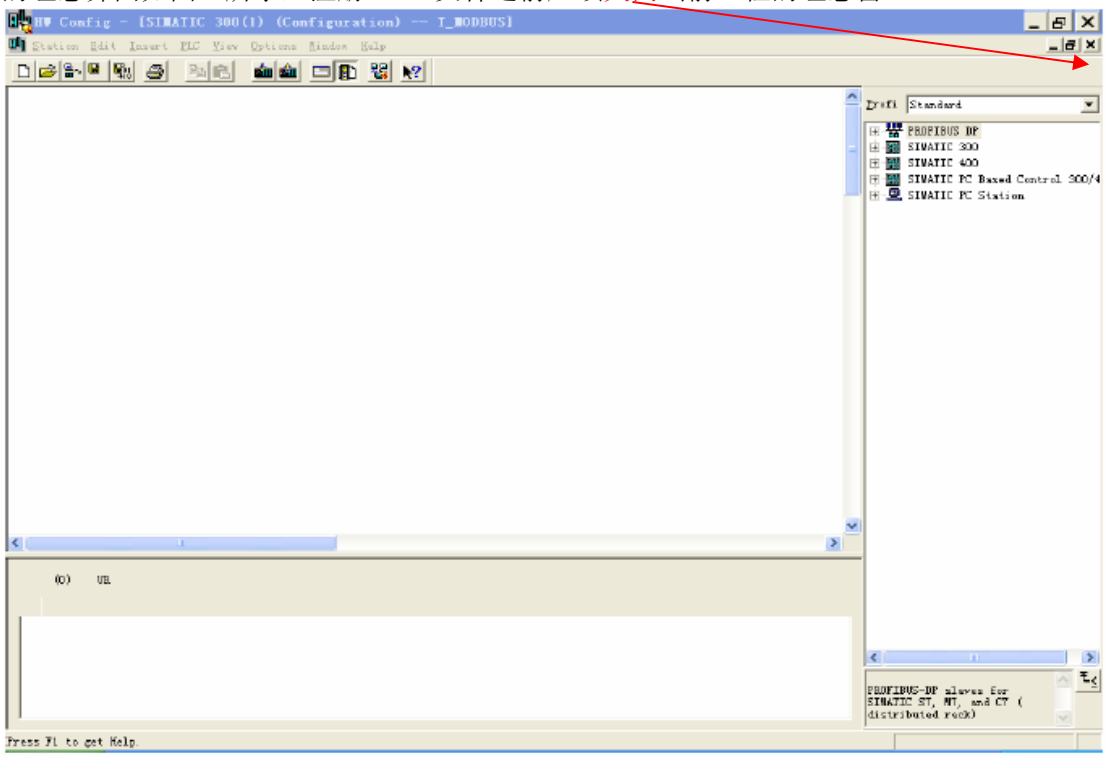


图 5

5.2.2 注册 GSD 文件

PM-126B 作为 Modbus 主站和从站时的 GSD 文件不同，请根据需要导入正确的 GSD 文件。把我们提供的产品相关 *.gsd 文件复制到以下路径：***Program files\Siemens\S7tmp***

1. 在图 5 中关闭当前工程组态窗口后，点击菜单栏 Options->Install GSD file，如图 6：

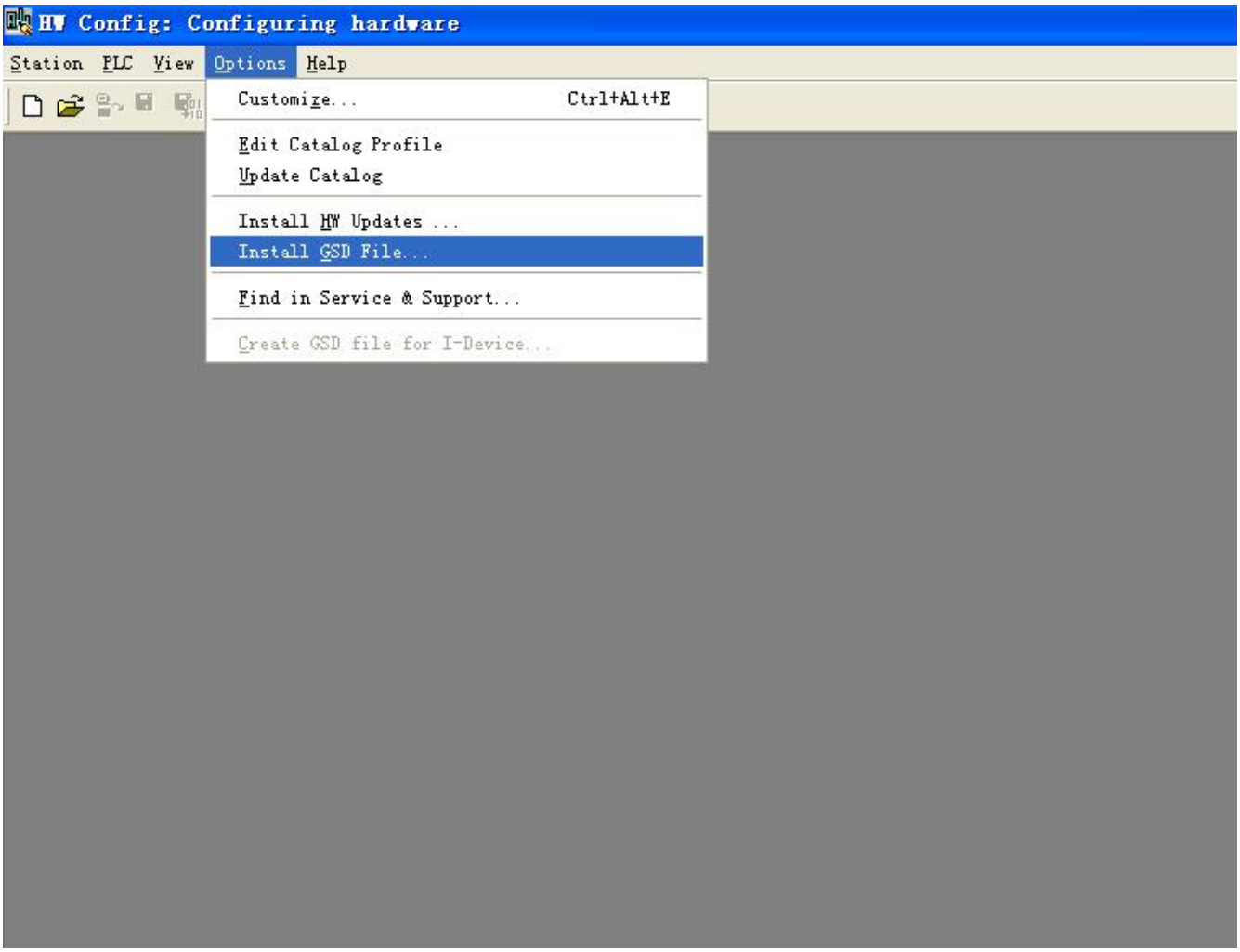


图 6

2. 弹出如图 7 所示窗口，选择 PM126M10.gsd 或者 PM-126S10.gsd，点击“Install”，注册完后，单击“Close”，关闭注册窗口。

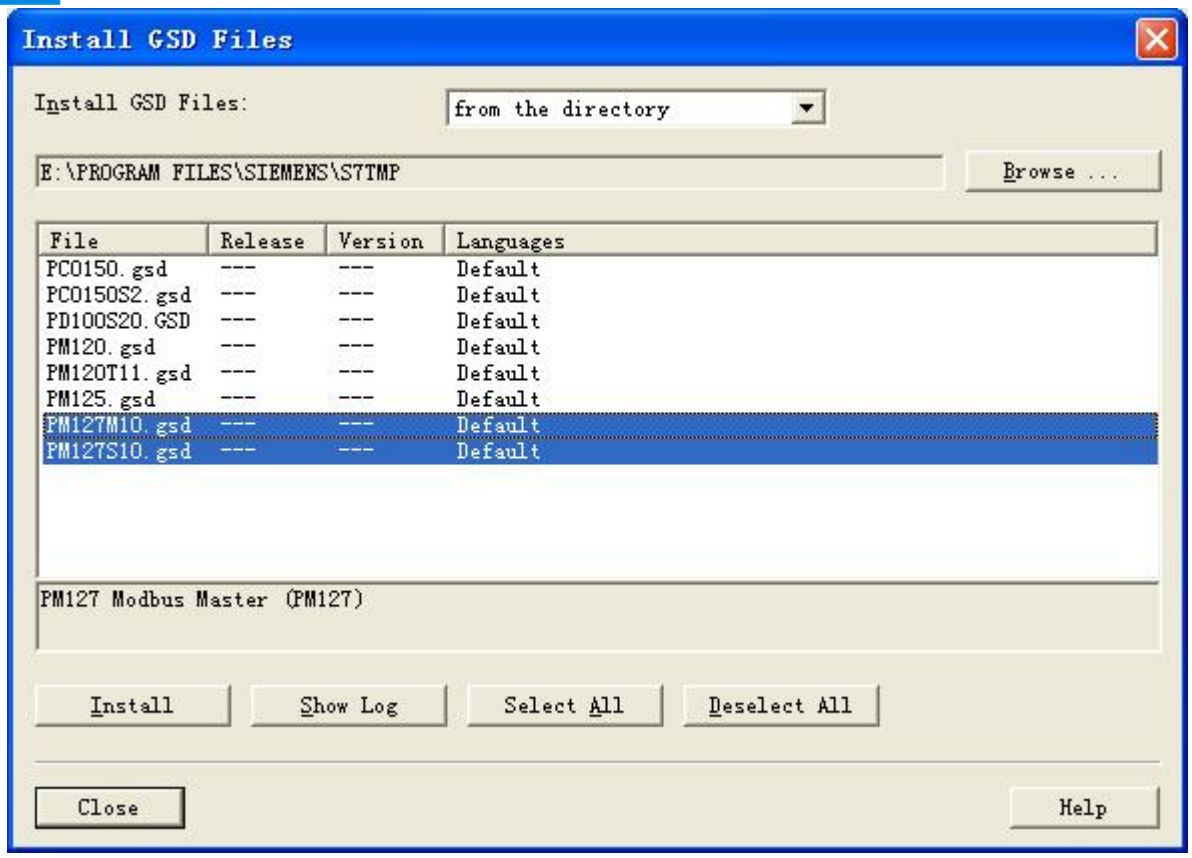


图 7

3. 在菜单栏中选择 Options->Update Catalog, 在 Device 目录中更新所注册的设备， 您可以在右侧窗口/Profibus DP/Additional Field Devices/Converter/找到您注册的设备，，如图 8 所示：

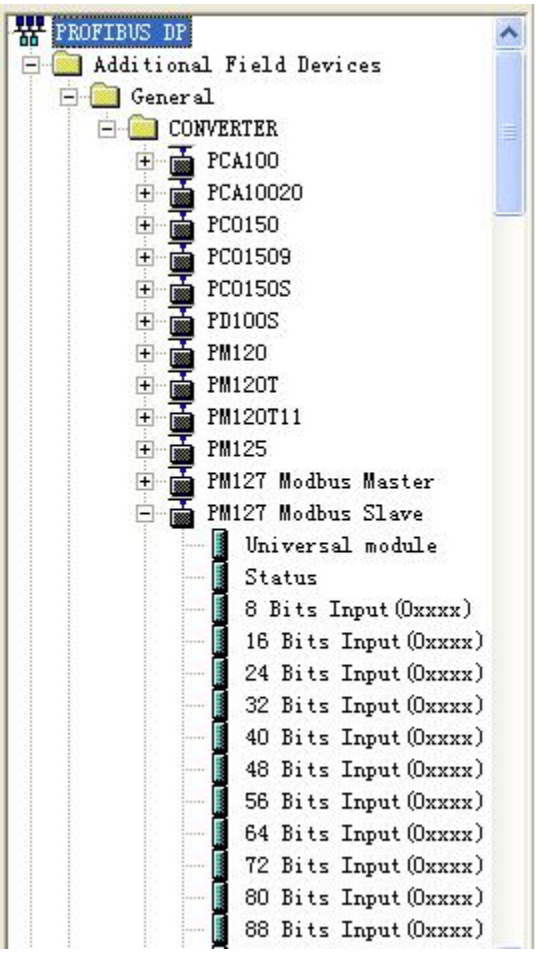


图 8

5.2.3 组态设置

1. 打开您创建工程的组态设置界面，设定 PLC rack，双击“Hardware Catalog\SIMATIC 300\RACK-300\Rail”，如图 9 所示：

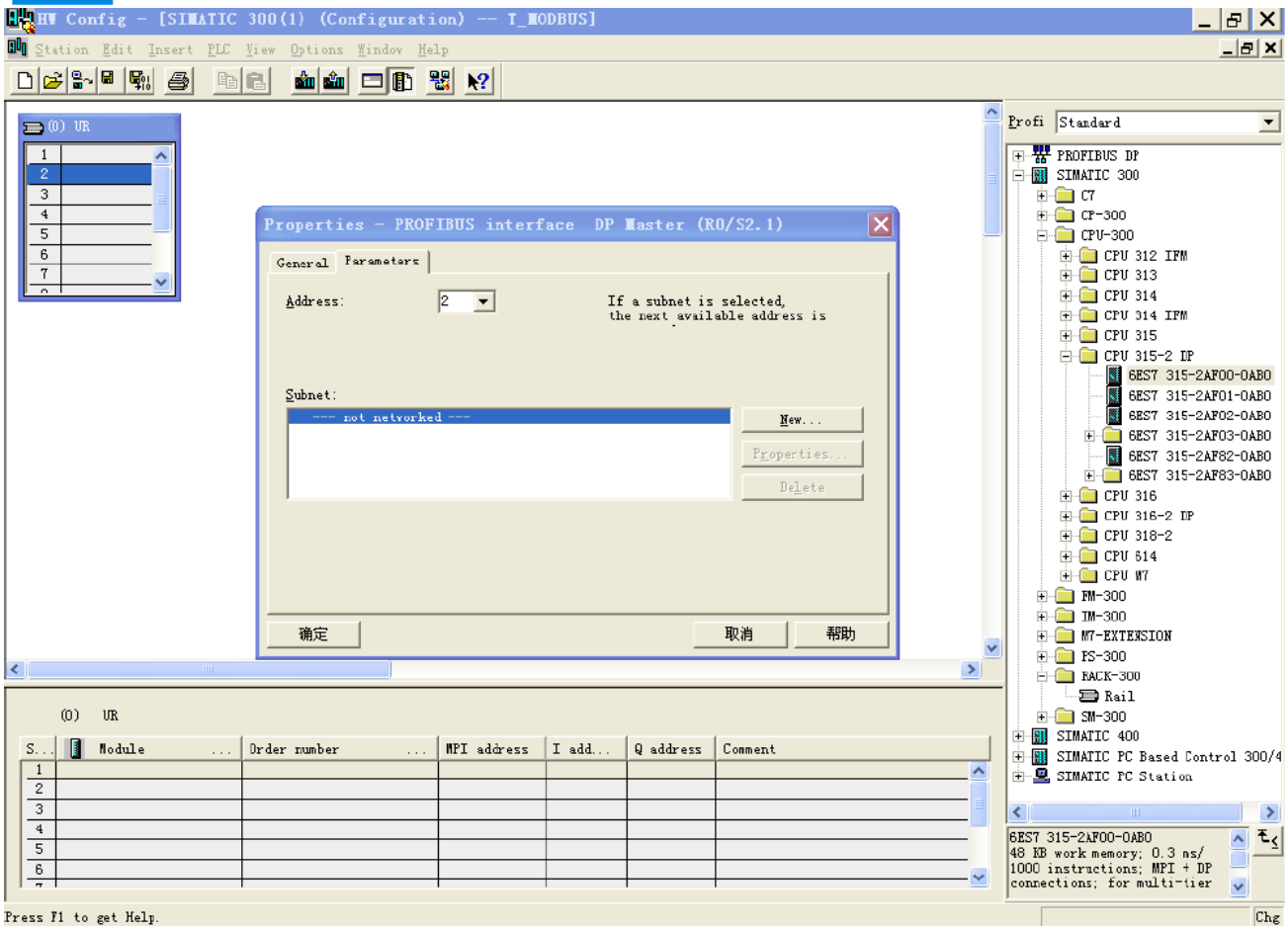


图 9

2. 设定 CPU 模块，选择对应的设备类型和所占用的槽位；

3. 创建 Profibus-DP 网络，设置 Profibus-DP：New->Network settings，选择 DP，选择一个波特率如 187.5Kbps，然后“OK”，双击它；如图 10：

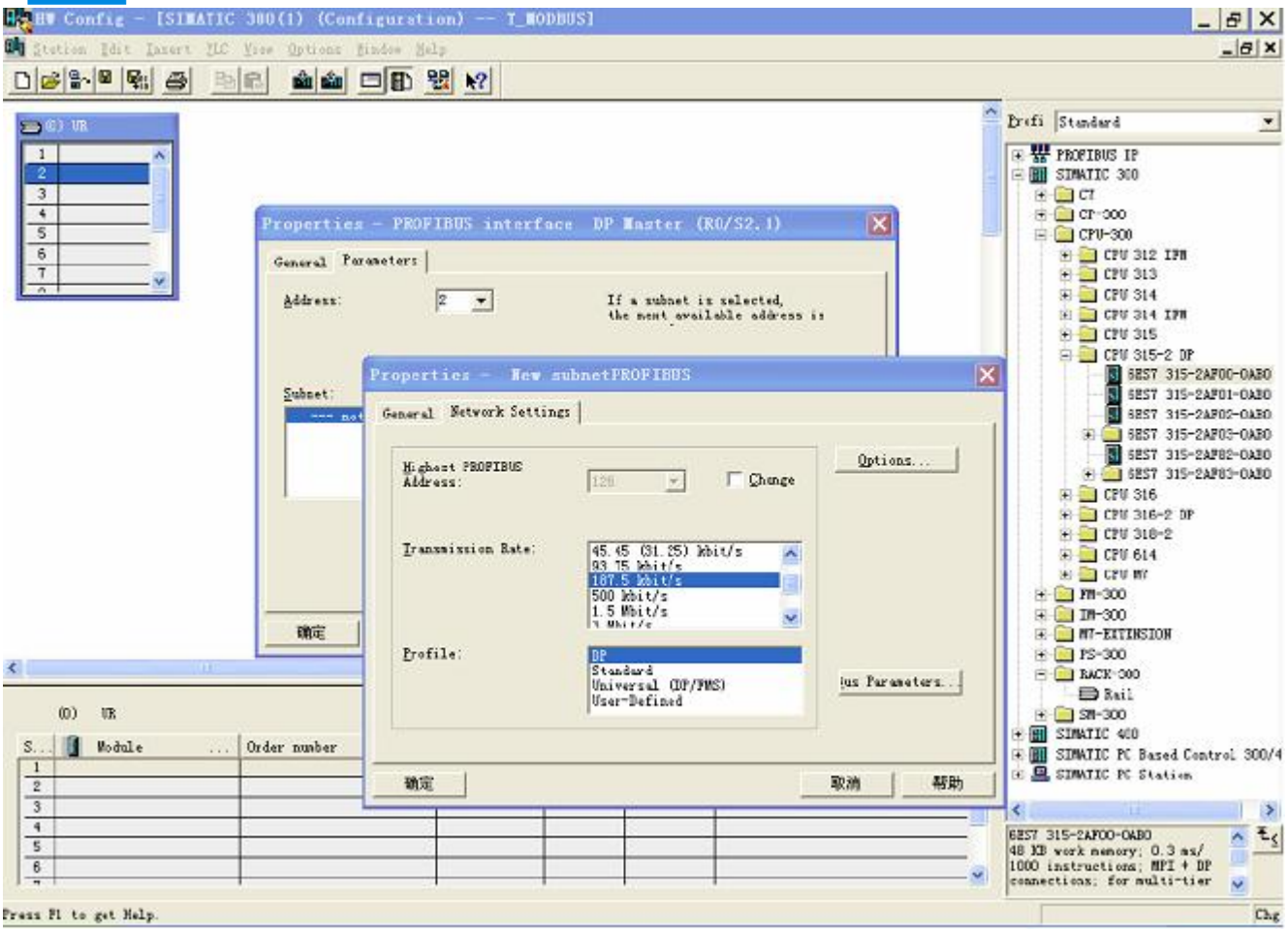


图 10

4. 选择 Profibus Master station 地址，如图 11：

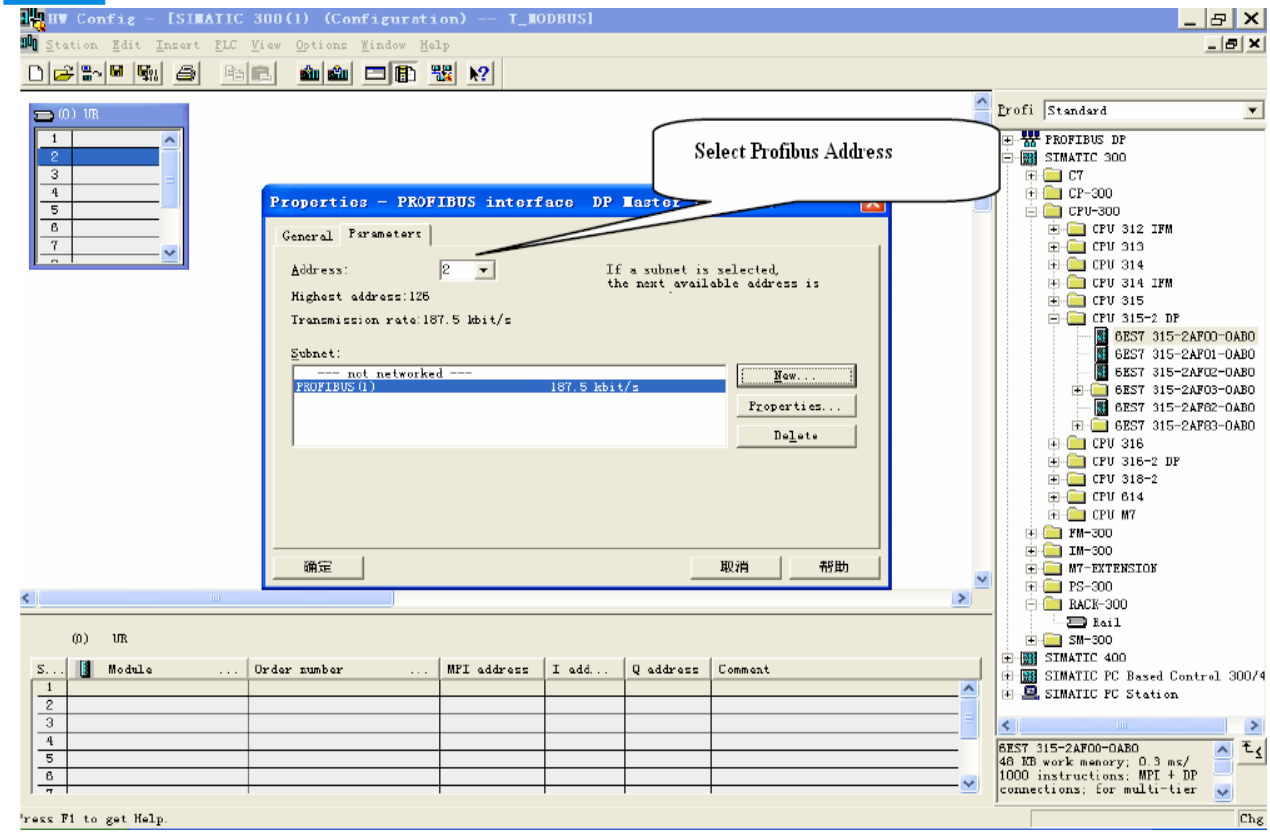


图 11

5. 将从站 PM-126B 配入到 PROFIBUS 网络配置当中，并将输入输出数据块映射到 S7-300 或者其它控制器的内存当中，如图 12：

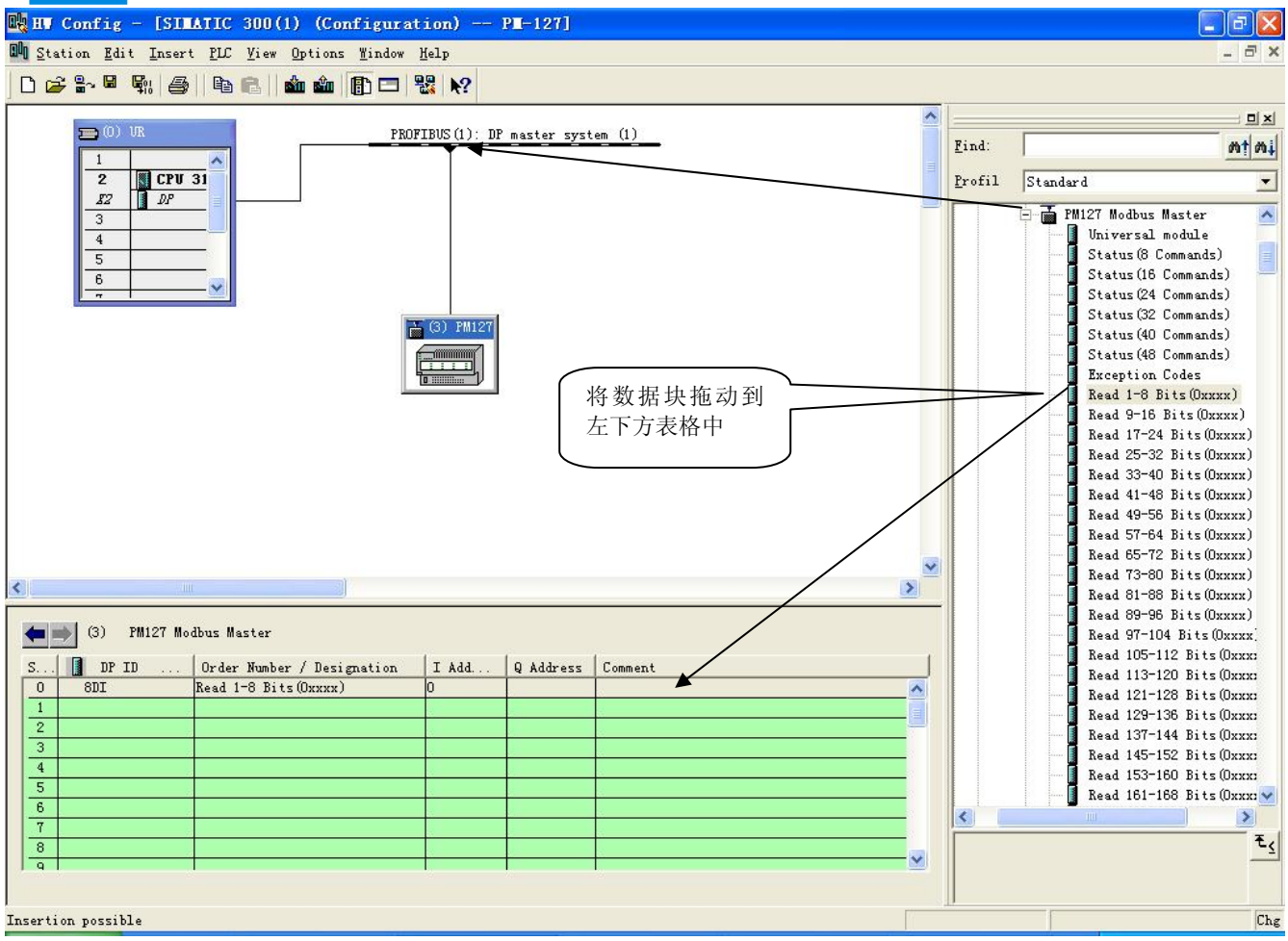


图 12

操作中分为两步，第一步将 PM-126B 图标（PM-126 Modbus Master 或者 PM-126 Modbus Slave）拖到左上方网络配置中，拖到 Profibus-DP 总线之上，鼠标会变化形状，表示可以放入了。第二步是将数据块拖动到左下方数据映射表格中，表格会变成绿色，说明可以放入，使相应字节映射到 PLC 内存。

注意：PROFIBUS-DP 从站的地址要与按扭的设置一致！

6. 设置 Profibus-DP 从站属性参数及相关 Modbus 命令 Module 参数，请参考 5.2.4 章节，保存并下载到 PLC。

5.2.4 参数设置

在参数设置之前，我们需要了解 PM-126 Modbus Master、PM-126 Modbus Slave 各自作为 Profibus-DP 从站的属性参数以及各自所支持的不同 Module 的参数。

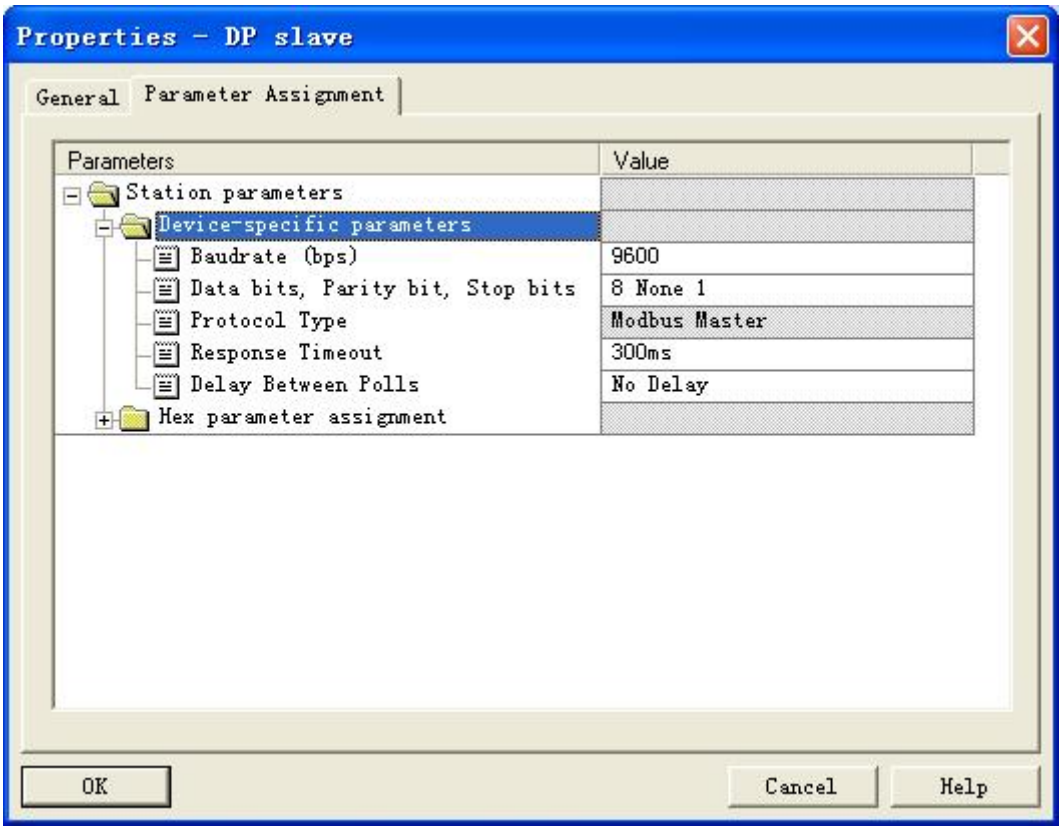
■ PM-126 Modbus Master

注册完 PM-126M10.gsd 文件后，在目录中可找到该名称的设备，也就是说 PM-126B 在 Modbus 端作为

Modbus 主站。

✧ **Profibus-DP 从站属性参数：**

在组态界面，双击已拖动到 Profibus-DP 网络上的 PM-126 Modbus Master，弹出的属性界面如下图所示：



可配置的参数包括：

Baudrate（bps）：配置串口波特率，300、600、1200、2400、9600、19200、38400、57600、115200bps 可选；

Data bits，Parity bit，Stop bits：配置数据位、检验方式以及停止位，8 None 1、8 Odd 1、8 Even 1、8 Mark 1、8 Space 1、8 None 2 可选；

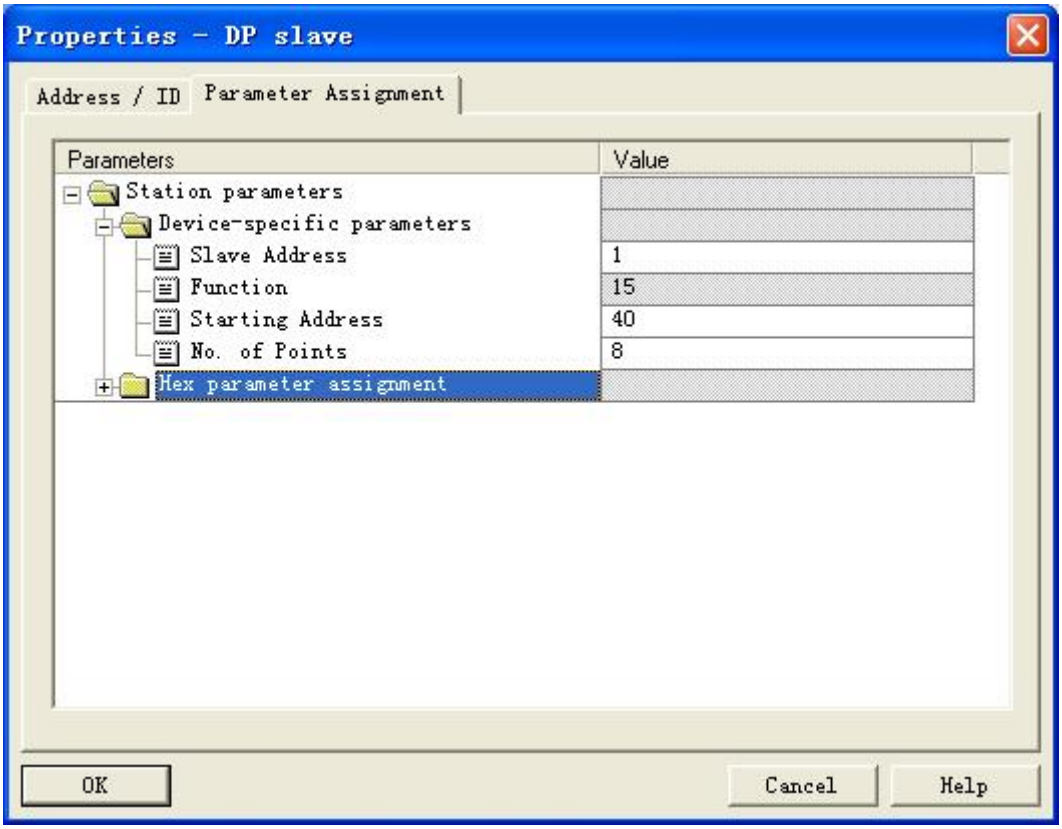
Protocol Type：当拖动到 Profibus-DP 总线上的是 PM-126 Modbus Master，则该项为“Modbus Master”；当拖动到 Profibus-DP 总线上的是 PM-126 Modbus Slave，则该项为“Modbus Slave”；

Response Timeout：当 Protocol Type 为 Modbus Master 时有效，100、200、300、400、500、600、700、800、900、1000、1500、2000、3000、4000、5000ms 可选；

Delay Between Polls：当 Protocol Type 为 Modbus Master 时有效，No Delay、50、100、150、200、300、400、500、600、700、800、900、1000、1500、2000ms 可选；

✧ **Module 参数**

在组态界面，双击已拖动到 PM-126B 对应的左下方表格中的 Module，弹出的属性界面如下图所示：



可配置的参数包括：

Slave Address：设置 PM-126B 所要连接的 Modbus 从站的地址，1～247 可选；

Function：无需设置，功能码有各自对应的 Module；

Starting Address：设置寄存器起始地址，0～65535 可选；

No. of Points：数据个数，只有 01H、02H、0FH 功能码对应的 Module 需要设置数据个数。

✧ **支持的 Modbus 命令 Module**

PM-126B 作为 Modbus Master 时支持的 Module 包括：Status Module、Read Module、Write Module

Status Module：Status(8 Commands)～Status(48 Commands)、Exception Codes

作为 Modbus 主站，Profibus 端可以监视 Modbus 命令的状态，提供两种 Modbus 命令状态监视功能：

Status(8 Commands)～Status(48 Commands)：6 选 1，每个位分别表示每条 Modbus 命令的状态，响应正确时置位，响应异常、超时或错误计数达到 3 次时清零，计数在响应正确时清零。

a) Status(8 Commands)：监视 8 条命令；

b) Status(16 Commands)：监视 16 条命令；

c) Status(24 Commands)：监视 24 条命令；

d) Status(32 Commands)：监视 32 条命令；

e) Status(40 Commands)：监视 40 条命令；

f) Status(48 Commands)：监视 48 条命令；

Exception Codes：为 1word Module，高字节表示 Modbus 命令索引 0～47；低字节表示异常代码或错误码。当响应正确时错误码为 0；当响应异常、超时或错误时高字节最高位置位，异常代码来自从设备，响应超时或错误时错误码为 0xFF。

Read Module：Read 1-8 Bits（0xxxx）～Read 249-256 Bits（0xxxx）、Read 1-8 Bits（1xxxx）～Read 249-256 Bits（1xxxx）、Read 1 Words（4xxxx）～Read 64 Words（4xxxx）、Read 2 Words（4xxxx）Consistent～Read 16 Words（4xxxx）Consistent、Read 1 Words（3xxxx）～Read 64 Words（3xxxx）、Read 2 Words（3xxxx）Consistent～Read 16 Words（3xxxx）Consistent

作为 Modbus 主站，支持的 Modbus 读命令 Module 如上所述，用户可根据需要拖动不同的 Module 并进行简单相关设置即可。

Write Module：Write Single Bits（0xxxx）～Write 249-256 Bits（0xxxx）、Write Single Words（4xxxx）～Write 64 Words（4xxxx）、Write 2 Words（4xxxx）Consistent～Write 16 Words（4xxxx）Consistent

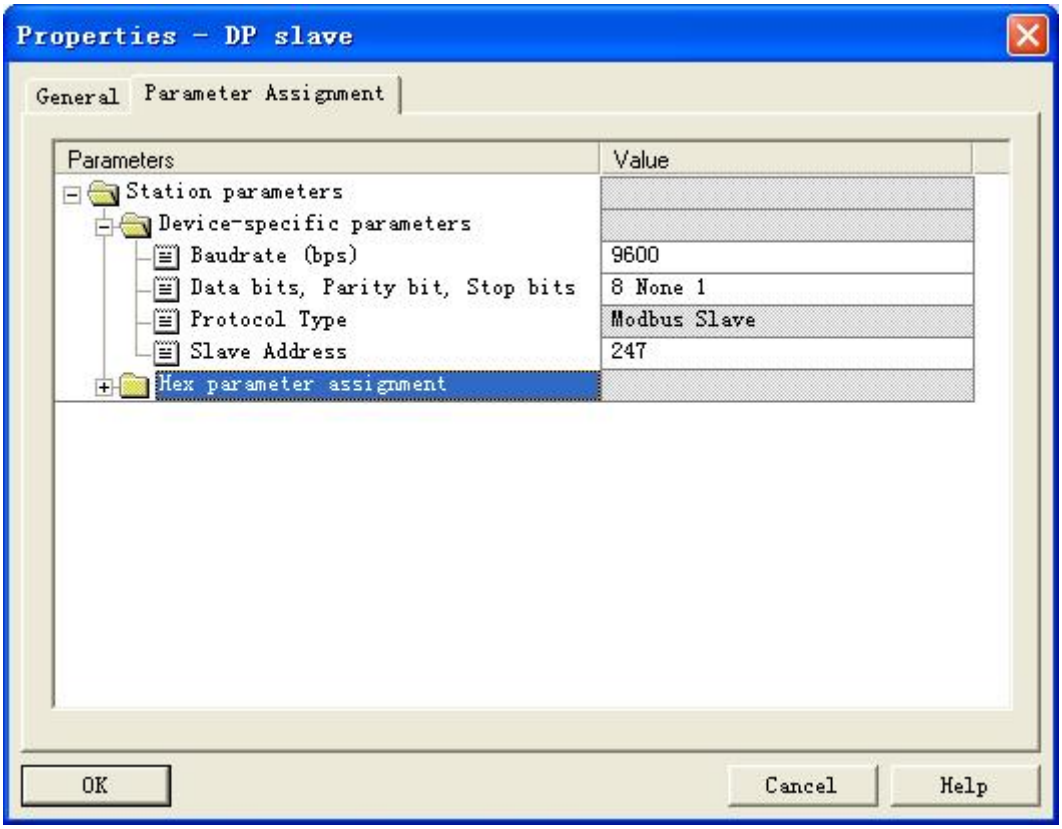
作为 Modbus 主站，支持的 Modbus 写命令 Module 如上所述，用户可根据需要拖动不同的 Module 并进行简单相关设置即可。

■ PM-126 Modbus Slave

注册完 PM-126S10.gsd 文件后，在目录中可找到该名称的设备，也就是说 PM-126B 在 Modbus 端作为 Modbus 从站。

✧ **Profibus-DP 从站属性参数：**

在组态界面，双击已拖动到 Profibus-DP 网络上的 PM-126 Modbus Slave，弹出的属性界面如下图所示：



可配置的参数包括：

Baudrate（bps）：配置串口波特率，300、600、1200、2400、9600、19200、38400、57600、115200bps 可选；

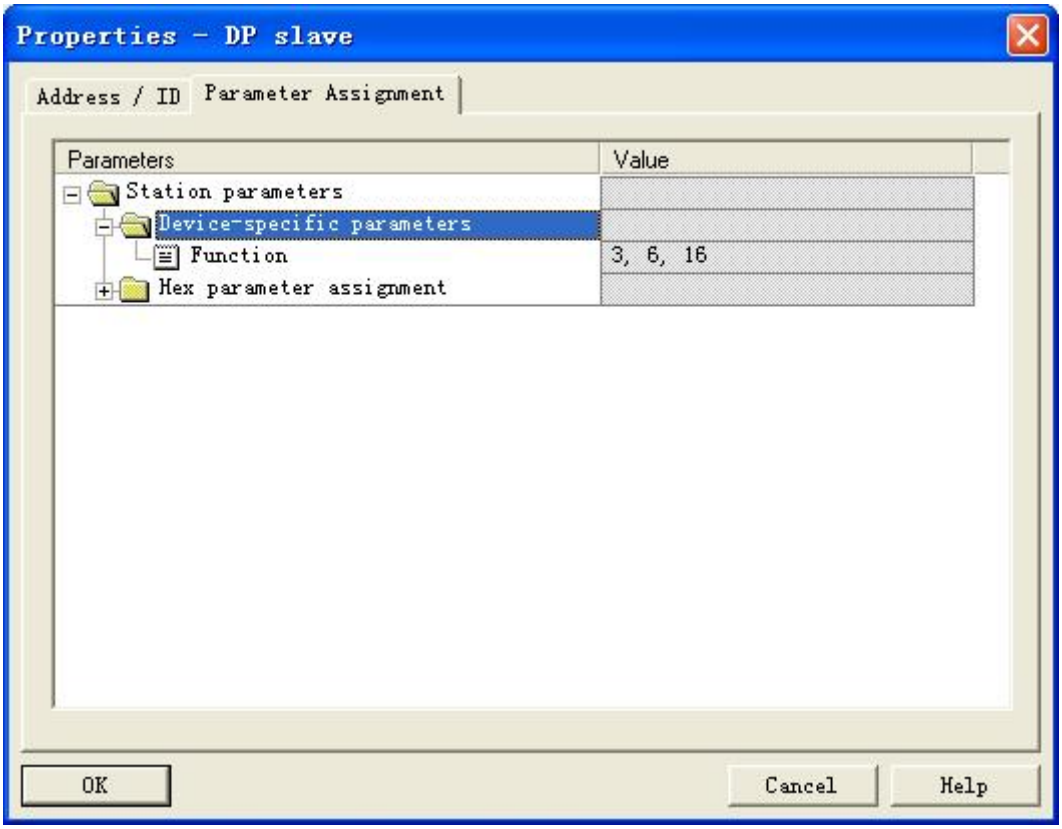
Data bits，Parity bit，Stop bits：配置数据位、检验方式以及停止位，8 None 1、8 Odd 1、8 Even 1、8 Mark 1、8 Space 1、8 None 2 可选；

Protocol Type：当拖动到 Profibus-DP 总线上的是 PM-126 Modbus Master，则该项为“Modbus Master”；当拖动到 Profibus-DP 总线上的是 PM-126 Modbus Slave，则该项为“Modbus Slave”；

Slave Address：当 Protocol Type 为 Modbus Slave 时有效，设置 PM-126B 作为 Modbus 从站的地址，1～247 可选。

✧ **Module 参数**

在组态界面，双击已拖动到 PM-126B 对应的左下方表格中的 Module，弹出的属性界面如下图所示：



其中：

Function：当拖动某一 Module 时，Function 已经确定，表示该 Module 支持的 Function 包括 03H（3）、06H（6）、10H（16）。

✧ **支持的 Modbus 命令 Module**

PM-126B 作为 Modbus Slave 时支持的 Module 包括：Status Module、Input Module、Output Module

Status Module：Status

作为 Modbus 从站，Profibus 端可以监视 Modbus 网络状态，Profibus 端提供 Modbus 网络状态 Module，占一个字节，当从站收到一条正确请求时，状态字节加一。

Input Module：8 Bits Input（0xxxx）～128 Bits Input（0xxxx）、1 Word Input（4xxxx）～64 Words Input（4xxxx）、2 Words Input（4xxxx）Consistent～16 Words Input（4xxxx）Consistent

作为 Modbus 从站，支持的 Modbus 读命令 Module 如上所述，用户可根据需要拖动不同的 Module 并进行简单相关设置即可。

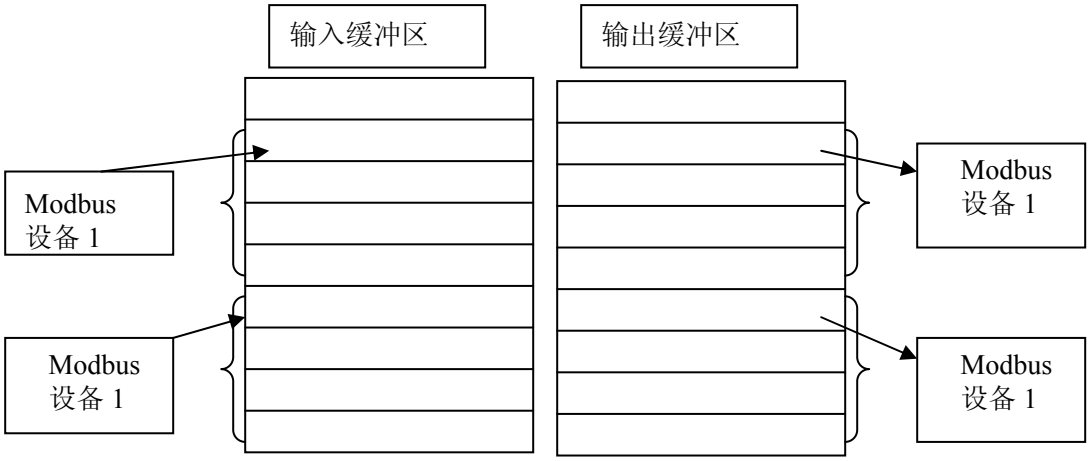
Output Module：8 Bits Input（1xxxx）～128 Bits Input（1xxxx）、1 Word Input（3xxxx）～64 Words Input（3xxxx）、2 Words Input（3xxxx）Consistent～16 Words Input（3xxxx）Consistent

作为 Modbus 从站，支持的 Modbus 写命令 Module 如上所述，用户可根据需要拖动不同的 Module 并进行简单相关设置即可。

六、Modbus 主、从站工作原理

6.1 Modbus 主站工作原理

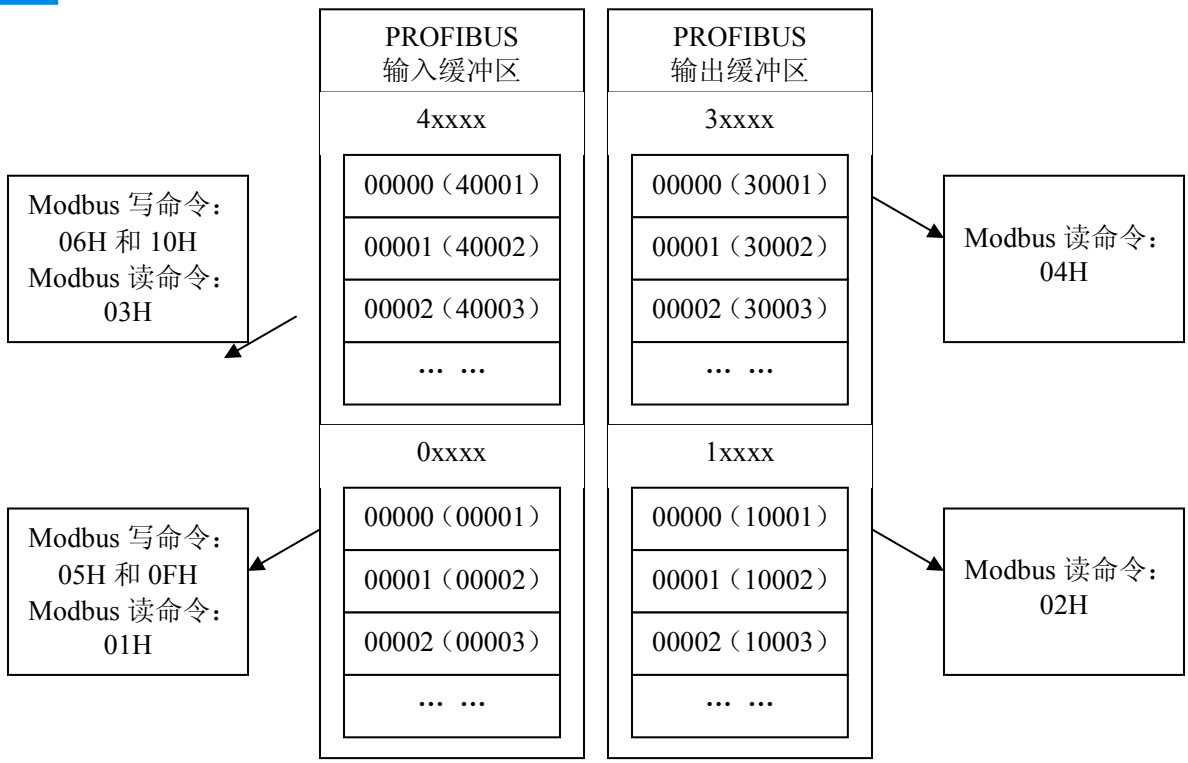
PM-126 Modbus Master 的 Modbus 和 PROFIBUS 之间的数据转换通过“映射”关系来建立。在 PM-126B 中有两块数据缓冲区，一块是 PROFIBUS 网络输入缓冲区，另一块是 PROFIBUS 网络输出缓冲区。Modbus 读取命令将读取的数据写入到网络输入缓冲区，供 PROFIBUS 网络读取。Modbus 写寄存器类的命令从网络输出缓冲区取数据，通过写命令输出到相应的 Modbus 设备。



支持 01H、02H、03H、04H、05H、06H、0FH、10H 号功能码，用户可以配置 **48** 条 Modbus 命令 Module。

6.2 Modbus 从站工作原理

PM-126 Modbus Slave 的 Modbus 和 PROFIBUS 之间的数据转换通过“映射”关系来建立。在 PM-126B 中有两块数据缓冲区，一块是 **PROFIBUS 网络输入** 缓冲区，另一块是 **PROFIBUS 网络输出** 缓冲区。网络输入和输出缓冲区都是相对于 PROFIBUS 而言的。Modbus 写寄存器类命令将数据写入到网络输入缓冲区，供 PROFIBUS 网络读取。Modbus 读取命令从网络输出缓冲区取数据，通过响应报文传输给 Modbus 主站设备。



支持 Modbus 寄存器地址 3 区（3xxxx）、4 区（4xxxx）、0 区（0xxxx）和 1 区（1xxxx）；其中，3 区支持功能码 04H；4 区支持功能码 03H、06H、10H；0 区支持功能码 01H、05H、0FH；1 区支持功能码 02H；

PROFIBUS-DP 输入缓冲区对于 Modbus 一侧，是 Modbus 主站输出，映射到 Modbus 保持寄存器 4xxxx（使用 10H 和 06H 命令写入数据，使用 03H 命令回读数据）和线圈 0xxxx（使用 0FH 和 05H 命令写入数据，使用 01H 命令回读数据）。

PROFIBUS-DP 输出缓冲区对于 Modbus 一侧，是 Modbus 主站输入，映射到 Modbus 输入寄存器 3xxxx（使用 04H 命令读取数据）和输入位 1xxxx（使用 02H 命令读取数据）。

七、Step7 如何读写网关数据

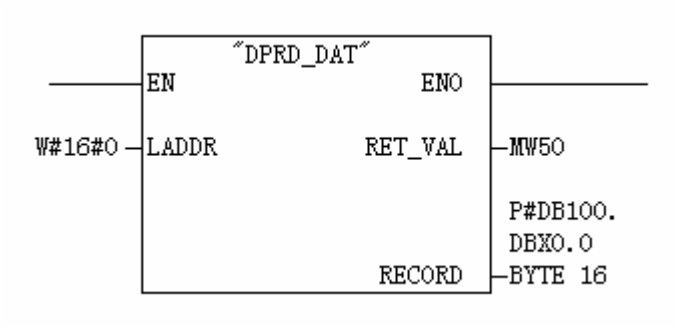
PM-126B 作为 Modbus Master 支持长度完整的 Modbus 命令 Module 如下所示：

Read 2 Words（4xxxx）Consistent～Read 16 Words（4xxxx）Consistent、Read 2 Words（3xxxx）Consistent～Read 16 Words（3xxxx）Consistent、Write 2 Words（4xxxx）Consistent～Write16 Words（4xxxx）Consistent

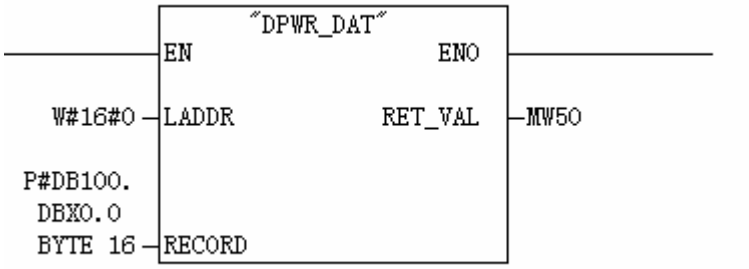
PM-126B 作为 Modbus Slave 支持长度完整的 Modbus 命令 Module 如下所示：

2 Words Input（4xxxx）Consistent～16 Words Input（4xxxx）Consistent、2 Words Output（3xxxx）Consistent～16 Words Output（3xxxx）Consistent

对于长度完整的 Modbus 命令 Module，在 Step7 编程时须采用打包式发送与接收。打包式发送与接收主要用到 SFC15（打包发送）和 SFC14（打包接收）。



SFC14



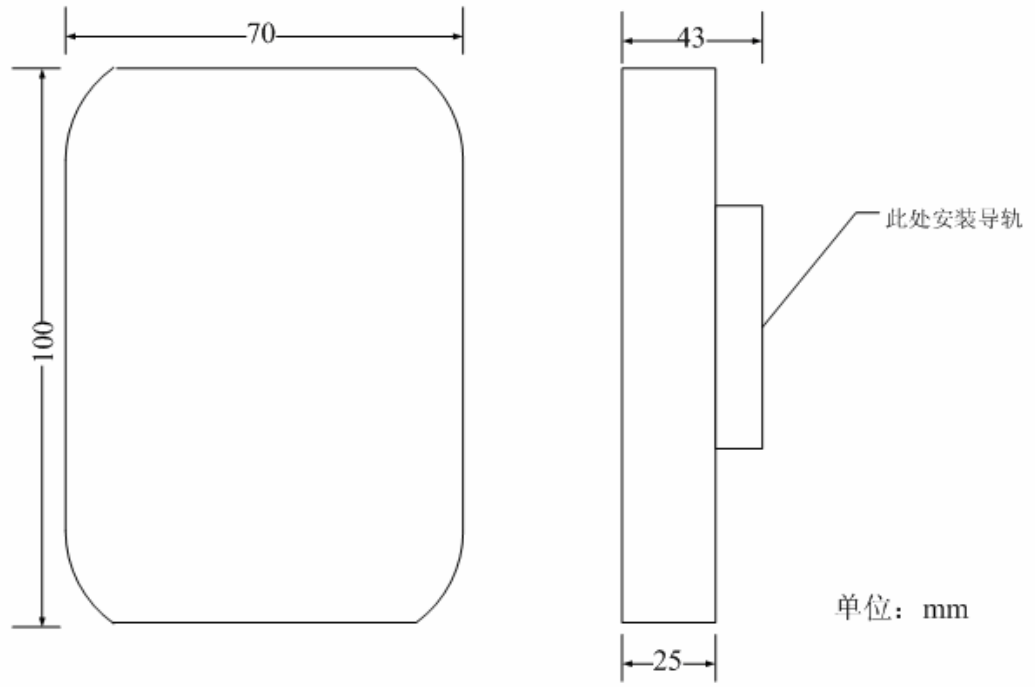
SFC15

对于长度完整之外的其它 Modbus 命令 Module，在 Step7 编程时可以直接使用 MOVE 指令对数据进行读写。

八、安装

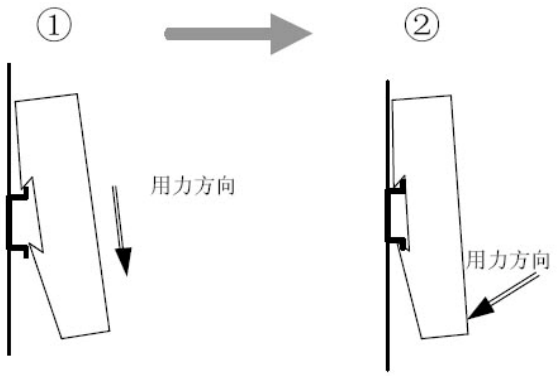
8.1 机械尺寸

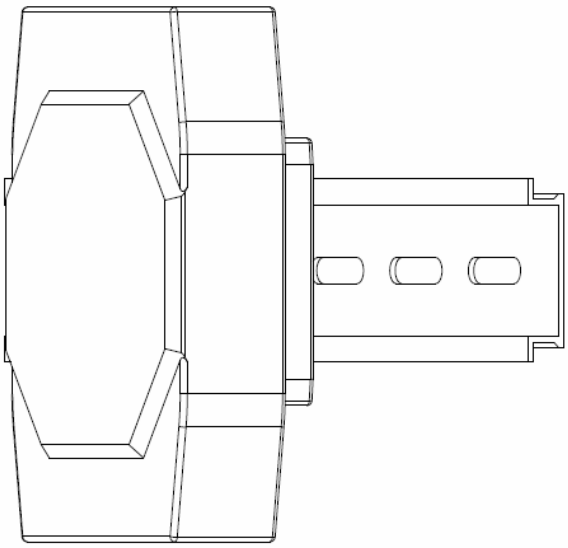
尺寸： 100mm（长）×70mm（宽）×25mm（深）



8.2 安装方法

35mm DIN 导轨安装





九、运行维护及注意事项

- ✧ 模块需防止重压，以防面板损坏。
- ✧ 模块需防止撞击，有可能会损坏内部器件。
- ✧ 供电电压控制在说明书的要求范围内，以防模块烧坏。
- ✧ 模块需防止进水，进水后将影响正常工作。
- ✧ 上电前请请检查接线，有无错接或者短路。

附录：Modbus 协议

Modbus-RTU 协议:
说明：与本产品通讯的设备必须带有 Modbus 接口，同时设备 Modbus 协议必须符合下面的规定，本公司提供用户定制服务。

1.协议概述
物理层：传输方式：RS485
通讯地址：0-247
通讯波特率：可设定
通讯介质：屏蔽双绞线
传输方式：主从半双工方式
协议在一根通讯线上使用应答式连接（半双工），这意味着在一根单独的通讯线上信号沿着相反的两个方向传输。首先，主计算机的信号寻址到一台唯一的终端设备（从机），然后，在相反的方向上终端设备发出的应答信号传输给主机。
协议只允许在主计算机和终端设备之间，而不允许独立的设备之间的数据交换，这就不会在使它们初始化时占据通讯线路，而仅限于响应到达本机的查询信号。

一个数据帧格式：
1 位起始位，8 位数据，1 位停止位。
一个数据包格式

地址	功能码	数据	校验码
8-Bits	8-Bits	N x 8-Bits	16-Bits

协议详细定义了校验码、数据序列等，这些都是特定数据交换的必要内容。
当数据帧到达终端设备时，它通过一个简单的“口”进入寻址到的设备，该设备去掉数据帧的“信封”（数据头），读取数据，如果没有错误，就执行数据所请求的任务，然后，它将自己生成的数据加入到取得的“信封”中，把数据帧返回给发送者。返回的响应数据中包含了以下内容：终端从机地址(Address)、被执行了的命令(Function)、执行命令生成的被请求数据(Data)和一个校验码(Check)。发生任何错误都不会有成功的响应。

地址（Address）域
地址域在帧的开始部分，由 8 位（0～255）组成，这些位标明了用户指定的终端设备的地址，该设备将接收来自与之相连的主机数据。每个终端设备的地址必须是唯一的，仅仅被寻址到的终端会响应包含了该地址的查询。当终端发送回一个响应，响应中的从机地址数据便告诉了主机哪台终端正与之进行通信。

功能（Function）域
功能域代码告诉了被寻址到的终端执行何种功能。表 1－1 列出了所有的功能码、它们的意义及它们的初始功能。

表 1－1 功能码

代码	意义	行为
03	读数据	获得一个或多个寄存器的当前二进制值
06	预置单寄存器	放置一个特定的二进制值到一个单寄存器中
16	预置多寄存器	放置特定的二进制值到一系列多寄存器中

数据域

数据域包含了终端执行特定功能所需要的数据或者终端响应查询时采集到的数据。这些数据的内容可能是数值、参考地址或者极限值。例如：功能域码告诉终端读取一个寄存器，数据域则需要指明从哪个寄存器开始及读取多少个数据，内嵌的地址和数据依照类型和从机之间的不同能力而有所不同。

错误校验域

该域允许主机和终端检查传输过程中的错误。有时，由于电噪声和其它干扰，一组数据在从一个设备传输到另一个设备时在线路上可能会发生一些改变，出错校验能够保证主机或者终端不去响应那些传输过程中发生了改变的数据，这就提高了系统的安全性和效率，出错校验使用了 16 位循环冗余的方法。

[注] 发送序列总是相同的 – 地址、功能码、数据和与方向相关的出错校验。

错误检测

循环冗余校验（CRC）域占用两个字节，包含了一个 16 位的二进制值。CRC 值由传送设备计算出来，然后附加到数据帧上，接收设备在接收数据时重新计算 CRC 值，然后与接收到的 CRC 域中的值进行比较，如果这两个值不相等，就发生了错误。

CRC 运算时，首先将一个 16 位的寄存器预置为全 1，然后连续把数据帧中的 8 位字节与该寄存器的当前值进行运算，仅仅每个字节的 8 个数据位参与生成 CRC，起始位和终止位以及可能使用的奇偶位都不影响 CRC。

在生成 CRC 时，每个 8 位字节与寄存器中的内容进行异或，然后将结果向低位移位，高位则用“0”补充，最低位（LSB）移出并检测，如果是 1，该寄存器就与一个预设的固定值进行一次异或运算，如果最低位为 0，不作任何处理。

上述处理重复进行，知道执行完了 8 次移位操作，当最后一位（第 8 位）移完以后，下一个 8 位字节与寄存器材的当前值进行异或运算，同样进行上述的另一个 8 次移位异或操作，当数据帧中的所有字节都作了处理，生成的最终值就是 CRC 值。

生成一个 CRC 的流程为：

预置一个 16 位寄存器为 0FFFFH（全 1），称之为 CRC 寄存器。

把数据帧中的第一个 8 位字节与 CRC 寄存器中的低字节进行异或运算，结果存回 CRC 寄存器。将 CRC 寄存器向右移一位，最高位填以 0，最低位移出并检测。

如果最低位为 0：重复第三步（下一次移位）。

如果最低位为 1：将 CRC 寄存器与一个预设的固定值（0A001H）进行异或运算。

重复第三步和第四步直到 8 次移位。这样处理完了一个完整的八位。

重复第 2 步到第 5 步来处理下一个八位，直到所有的字节处理结束。

最终 CRC 寄存器得值就是 CRC 的值。

2．应用层功能详解

第一章已经简述了协议和数据帧，使用此软件的程序员可以使用下述的方法以便通过协议正确的建立他们的特定应用程序。

本章所述协议将尽可能的使用如图 2－1 所示的格式，（数字为 16 进制）。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

图 2－1 协议例述

读数据（功能码 03）
查询
图 2－2 的例子是从 03 号从机读 3 个采集到的基本数据 U1,U2,U3, U1 的地址为 0001H, U2 的地址为 0002H, U3 的地址为 0003H,

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

图 2－2 读 Uca 和 Ia 的查询数据帧

响应
响应包含从机地址、功能码、数据的数量和 CRC 错误校验。
图 2－3 的例子是读取 U1,U2,U3 的响应。

地址	功能码	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	03H	06H	01H	7CH	01H	7DH	01H	7CH	F9H	9BH

图 2－3 读 U1,U2,U3 的响应数据帧

2．2 预置多寄存器（功能码 10）
查询
功能码 10H 允许用户改变多个寄存器的内容，设备可从任何地址开始设置最多 16 个变量的值。控制器是以动态扫描方式工作的，任何时刻都可以改变寄存器内容。
图 2-4 是修改 3 号从站设备的负载监控 1 和负载监控 2 的动作及延时时间的设定值，其中负载监控 1 的动作设定值地址为 2AH，延时时间的设定值为 2BH，负载监控 2 的动作设定值地址为 2CH，延时时间的设定值为 2DH。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	10H	00H	2AH	00H	04H	08H	07H	D0H	00H	0AH	07H	0D0H	00H	0AH	25H	7CH

图示 2-4 修改负载监控 1 和负载监控 2 的动作值及延时时间的设定值

响应

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校对验码低字节	校对验码高字节
03	10H	00H	2AH	00H	04H	EBH	8DH

图示 2-5 修改负载监控 1 和负载监控 2 的动作值及延时时间的设定值的响应

2．3 预置单寄存器（功能码 06）

查询

功能码06允许用户改变单个寄存器的内容，DAE系统内部的任何单寄存器都可以使用此命令来改变其值。既然仪器是以动态扫描方式工作的，任何时刻都可以改变单寄存器内容。

下面的例子是请求 03 号从机修改过载动作设定值 Ir1，Ir1 地址是 002EH.

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

图示 2-6 修改过载动作设定值 Ir1

响应

对于预置单寄存器请求的正常响应是在寄存器值改变以后将接收到的数据传送回去。

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量值高字节	变量值低字节	校对验码低字节	校对验码高字节
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

图示 2-7 修改过载动作设定值 Ir1