



# G0306 Modbus 转 DP 网关 使用手册



沈阳中科博微科技股份有限公司

## 警告

1. 禁止用户自行拆装网关。
2. 请用户自行检查网关供电电压是否符合使用手册中的供电电压要求。

版本：V2.0

### 免责声明

已经检查过此手册的内容，确认所描述的硬件和软件的一致性。由于无法完全排除误差，不能保证绝对一致。然而我们将定期检查此手册中的数据，并在后续版本中予以必要的修正。欢迎任何关于改进的建议。

**Microcyber Corporation 2016**

技术数据随时有变。

## 公司简介

沈阳中科博微科技股份有限公司是由中国科学院沈阳自动化研究所发起创建的一家高新技术企业，主要从事网络化控制系统、工业通信及仪表、开发、生产和应用。中科博微承担了多个国家科技重大专项、国家高技术研究发展计划（863 计划）、智能制造装备发展专项等国家科技计划项目，是国家网络化控制系统工程研究中心建设依托单位。

中科博微成功地开发了国内第一个通过国际认证的现场总线协议主栈、第一个通过国家认证的现场总线仪表、国内第一个通过德国 TÜV 认证的安全仪表，与其它单位共同主持了制定国内第一个工业以太网协议标准 EPA、第一个工业无线通信协议标准 WIA-PA，并成为 IEC 国际标准。

中科博微的产品和技术曾荣获国家科技进步二等奖两项、国家科技发明奖一项、中国科学院科技进步一等奖一项、辽宁省科技进步一等奖一项，产品出口欧美等发达国家，美国 Emerson、英国 Rotork、英国 Bifold 等业内顶尖企业都在其产品中采用了博微的关键技术或关键部件，成功完成了 200 多项大型自动化工程项目。

中科博微是 FCG 组织成员；是 Profibus 用户组织（PNO）成员。

中科博微成功通过了 ISO9001:2008 质量管理体系认证和汽车行业的 ISO/TS16949 质量体系认证。优秀的研发团队，丰富的自动化工程设计与实施经验，业界领先的产品，庞大的市场网络，优秀的企业文化，都为公司的创业和持续发展奠定了坚实基础。承载员工理想，创造客户价值，促进企业发展。

承载员工理想，创造客户价值，促进企业发展。

## 目 录

第1章 概述 .....	1
1.1 设备分类 .....	1
1.2 外形结构 .....	2
1.2.1 网关外形尺寸图 .....	2
1.2.2 网关结构图 .....	2
第2章 安装 .....	3
2.1 DIN 导轨安装 .....	3
2.2 网关接口 .....	3
2.2.1 电源接口 .....	3
2.2.2 Modbus-RS485 接口（适用于 GW-MODB-DP-RS485） .....	3
2.2.3 Modbus-RS232 接口（适用于 GW-MODB-DP-RS232） .....	3
2.2.4 PROFIBUS DP 总线接口 .....	4
2.2.5 PROFIBUS 地址配置接口 .....	4
2.2.6 LED 指示灯 .....	4
2.2.7 特殊功能接口 .....	4
第3章 工作原理 .....	5
3.1 网关作为 Modbus 主站（G0306-MS） .....	5
3.2 网关作为 Modbus 从站（G0306-SS） .....	6
第4章 网关配置 .....	7
4.1 拓扑结构 .....	7
4.1.1 网络拓扑 .....	7
4.1.2 电缆和连接器 .....	7
4.2 设置网关地址 .....	7
4.3 网关循环组态 .....	8
4.3.1 GSD 文件说明 .....	8
(1) G0306-MS 的 GSD 文件说明 .....	8
● 模块描述 .....	8
● 设备用户参数 .....	12
● 模块用户参数 .....	14
(2) G0306-SS 的 GSD 文件说明 .....	15
● 模块描述 .....	15
● 设备用户参数 .....	16



- 模块用户参数 ..... 16
- Modbus 存储区与 Profibus 输入输出数据缓冲区的对应关系 ..... 17
- 4.3.2 安装 GSD 文件 ..... 17
- 4.3.3 使用 GSD 文件 ..... 17
  - (1) 如何使用 G0306-MS 的 GSD 文件..... 19
    - 配置设备用户参数..... 19
    - 配置网关模块简介..... 20
    - 总状态模块（模块 2） ..... 20
    - 控制模块（模块 3） ..... 21
    - 使用读 xxx 位模块举例（模块 4-67） ..... 21
    - 使用读 xxx 字模块举例（模块 68-143） ..... 23
    - 使用写 xxx 位模块举例（模块 144-175） ..... 24
    - 使用写 xxx 字模块举例（模块 176-199） ..... 26
    - 使用写单个线圈模块举例（模块 200） ..... 28
    - 使用写单个寄存器模块举例（模块 201） ..... 30
    - 使用 xxx 位 Modbus 从站监测模块举例（模块 202、204、206、208） ..... 32
    - 使用 xxx 字节 Modbus 从站监测模块举例（模块 203、205、207、209） ..... 34
  - (2) 如何使用 G0306-SS 的 GSD 文件..... 35
    - 配置设备用户参数..... 35
    - 配置网关模块简介..... 36
    - 总状态模块（模块 2） ..... 36
    - 控制模块（模块 3） ..... 37
    - 使用输入 xxx 位模块举例（模块 4-19） ..... 37
    - 使用输出 xxx 位模块举例（模块 36-51） ..... 38
    - 使用输入 xxx 字节模块举例（模块 20-35） ..... 40
    - 使用输出 xxx 字节模块举例（模块 52-67） ..... 41
- 4.3.4 使用注意事项 ..... 42
- 第 5 章 维护 ..... 43
- 第 6 章 技术规格 ..... 44
  - 6.1 基本参数 ..... 44
  - 6.2 性能指标 ..... 44
  - 6.3 物理特性 ..... 44
  - 6.4 默认通信参数 ..... 44
  - 6.5 支持 Modbus 功能码 ..... 44



附录 A	Modbus 通信协议	45
A. 1	Modbus 通信协议	45
A. 2	Modbus 协议要点	45
A. 3	Modbus 异常响应	46
A. 4	Modbus 存储区	47
A. 5	Modbus 功能码	47
A. 5. 1	01 (0x01) 读线圈举例	47
A. 5. 2	02 (0x02) 读离散量输入举例	48
A. 5. 3	03 (0x03) 读保持寄存器举例	48
A. 5. 4	04 (0x04) 读输入寄存器举例	48
A. 5. 5	05 (0x05) 写单个线圈举例	49
A. 5. 6	06 (0x06) 写单个寄存器举例	49
A. 5. 7	15 (0x0F) 写多个线圈举例	49
A. 5. 8	16 (0x10) 写多个寄存器	50
附录 B	G0306 Modbus 转 DP 网关选型代号表	51

## 第1章 概述

产品名称：Modbus 转 DP 网关

产品型号：G0306

此网关实现了 Modbus RTU 到 PROFIBUS DP 的转换功能。可以使多个符合 Modbus RTU 通信规则的从站设备接入到 PROFIBUS DP 网络中。Modbus 端既可做主站，也可做从站，此功能通过特殊功能按键切换。



图 1 G0306 Modbus 转 DP 网关

### 1.1 设备分类

此网关根据 Modbus 接口不同分为两种型号（与实际选型一致）：

产品选型	Modbus 接口
GW-MODB-DP-RS485	RS485
GW-MODB-DP-RS232	RS232

此网关根据通信方式区分（功能区分，用以下名称便于文档描述，不是实际选型，实际选型见附录）：

产品选型	Modbus 端	PROFIBUS 端
G0306-MS	主站	从站
G0306-SS	从站	从站

注意：

- 1) V1.0 版本仅实现了 GW-MODB-DP-RS485 版本，后续将增加 GW-MODB-DP-RS232 版本，敬请期待。
- 2) G0306 Modbus 转 DP 网关根据用户需求可通过特殊功能按键在 G0306-MS 和 G0306-SS 之间自由切换，切换方法见 2.2.7。

## 1.2 外形结构

### 1.2.1 网关外形尺寸图

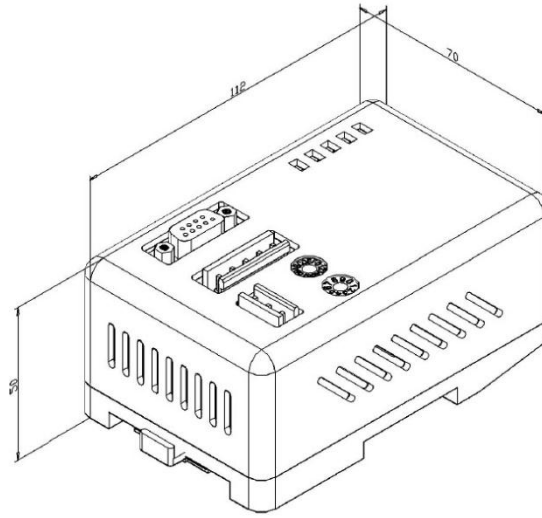


图2 网关外形尺寸图（112\*70\*50，单位 mm）

### 1.2.2 网关结构图

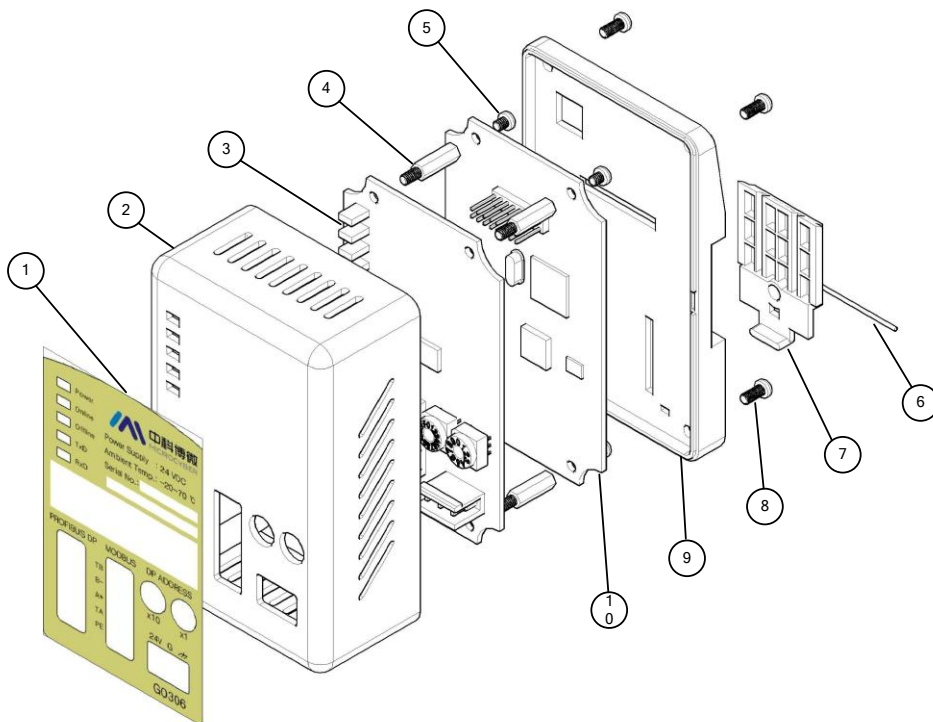


图3 网关结构图

1	贴膜	2	上盖	3	接口卡	4	六棱柱
5	宽沿螺钉	6	铁丝	7	卡子	8	宽沿螺钉
9	底座	10	通信卡				



## 第2章 安装

### 2.1 DIN 导轨安装

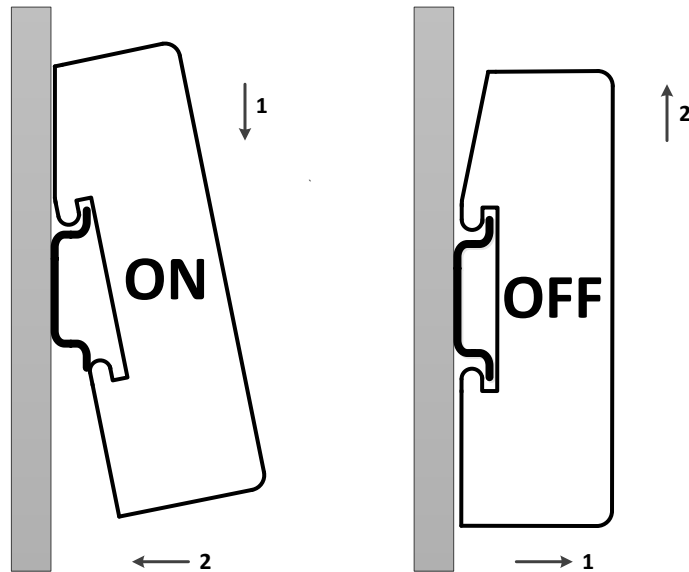
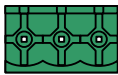


图 4 DIN 导轨安装图

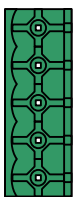
## 2.2 网关接口

### 2.2.1 电源接口



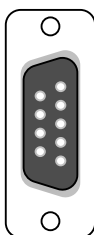
序号	端子名称	端子用途
1	24V	接 24V 直流电源正
2	G	接 24V 直流电源负
3	PE	接双绞线屏蔽

### 2.2.2 Modbus-RS485 接口（适用于 GW-MODB-DP-RS485）



序号	端子名称	端子用途
1	TB	与 B-短接使能终端
2	B-	接 Modbus 总线 B
3	A+	接 Modbus 总线 A
4	TA	与 A+短接使能终端
5	PE	接双绞线屏蔽

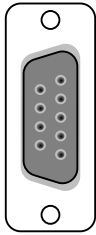
### 2.2.3 Modbus-RS232 接口（适用于 GW-MODB-DP-RS232）



序号	端子名称	端子用途
1	NC	悬空
2	TxD	接用户设备 RxD
3	RxD	接用户设备 TxD
4	NC	悬空
5	GND	接用户设备 GND
6-9	NC	悬空

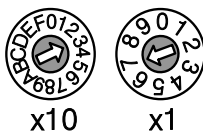
注意：用户请根据接口定义自制 RS232 电缆。

### 2.2.4 PROFIBUS DP 总线接口



序号	端子名称	端子用途
1-2	NC	悬空
3	RxD/TxD-P	接收/发送数据, 线 B (红色)
4	CNTR-P	中继器方向控制
5	DGND	数据地 (对 VP 的参考电压)
6	VPa	电源+5V (例如, 用于总线终端器)
7	NC	悬空
8	RxD/TxD-N	接收/发送数据, 线 A (绿色)
9	NC	悬空

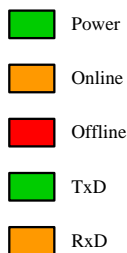
### 2.2.5 PROFIBUS 地址配置接口



地址拨码开关	描述
16 位旋钮拨码开关 x10	每个刻度代表 10, 范围 0-160;
10 位旋钮拨码开关 x1	每个刻度代表 1, 范围 0-9;

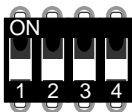
注意: 当地址大于 125 时, 固定地址为 125。  
 如图所示, 地址=3\*10+7\*1=37

### 2.2.6 LED 指示灯



指示灯名称	颜色	指示灯用途
<b>Power</b>	绿	设备电源指示灯
<b>Online</b>	黄	PROFIBUS 进入数据交换
<b>Offline</b>	红	PROFIBUS 未进入数据交换
<b>TxD</b>	绿	Modbus 发送指示灯
<b>RxD</b>	黄	Modbus 接收指示灯

### 2.2.7 特殊功能接口



序号	端子名称	端子用途
1	MS	Modbus 主从切换。 Off: G0306-MS On: G0306-SS
2	Not Used	暂未使用
3	Not Used	暂未使用
4	Not Used	暂未使用

### 第3章 工作原理

G0306 Modbus 转 DP 网关，是同时支持 Modbus RTU 协议与 PROFIBUS DP 协议的网关设备。它本身是 PROFIBUS DP 从站设备，作为 Modbus 主站（G0306-MS）时，理论上最多可以使 31 个 Modbus 从站设备接入到 PROFIBUS DP 网络中（这是限制于 485 总线环境，建议最多不要超过 10 个 Modbus 从站设备，以免影响通信质量），作为 Modbus 从站（G0306-SS）时，可通过 RS485/RS232 接口接到 Modbus 主站上。

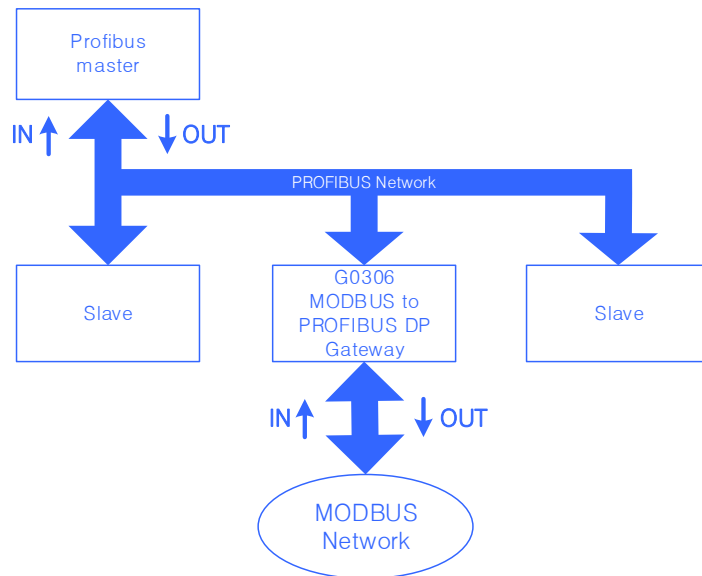


图 5 网关系统连接示意图

#### 3.1 网关作为 Modbus 主站（G0306-MS）

G0306-MS 的工作机制是通过配置模块来实现 Modbus 数据到 DP 数据的转换。每个模块可配置 1 条 Modbus 报文。G0306-MS 共有 39 个槽，209 个模块。其中，1、2 槽已经有固定作用，还有 37 个槽可用。每个槽可配置 1 个模块，相当于最多可以配置 37 条 Modbus 报文。

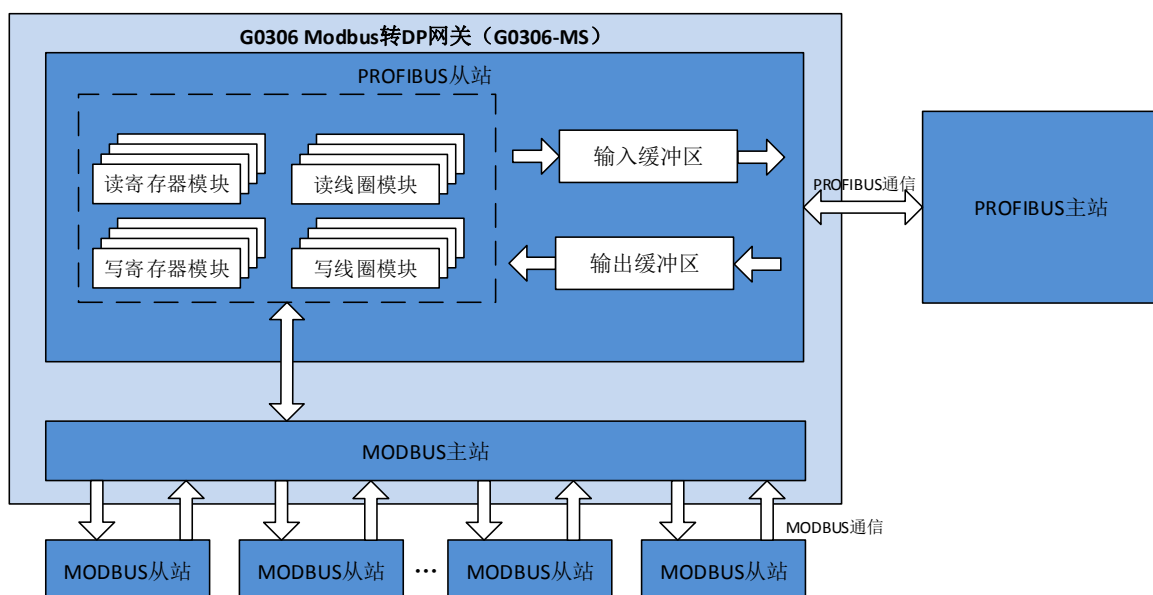


图 6 网关原理框图（G0306-MS）

### 3.2 网关作为 Modbus 从站 (G0306-SS)

G0306-SS 的工作机制是通过配置模块来实现 Profibus 的输入输出缓冲区分别到 Modbus 存储区的映射，从而便于 Modbus 主站在相应的 Modbus 存储区去读取想要的数

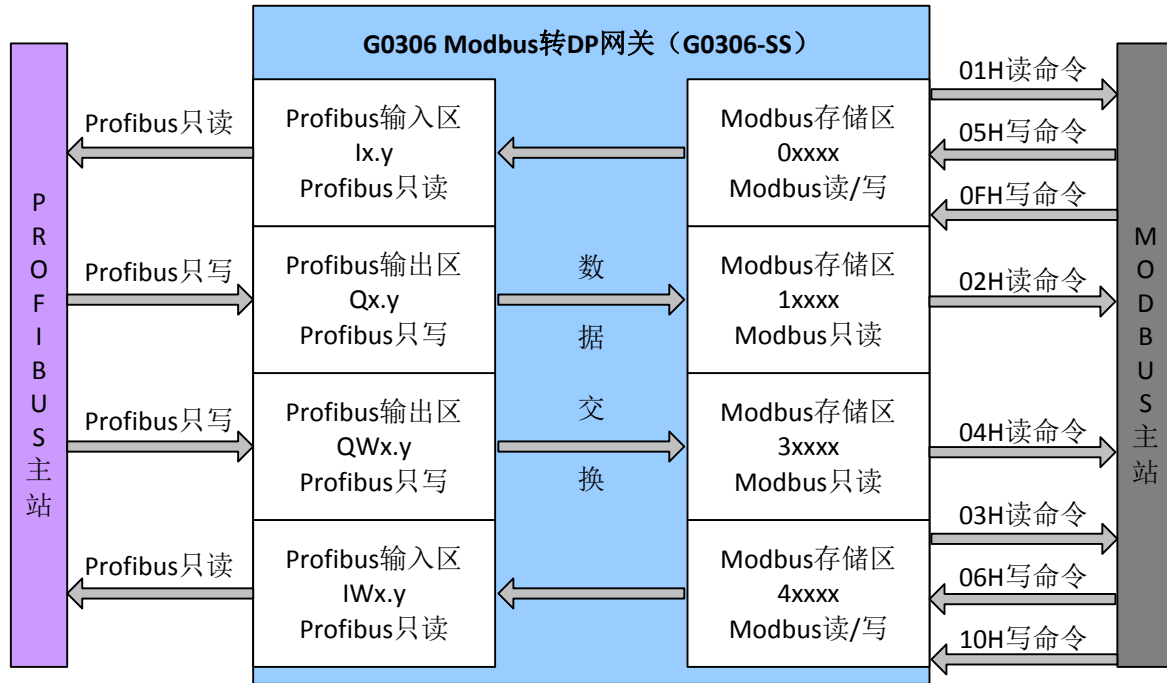


图 7 网关原理框图 (G0306-SS)

G0306-SS 共有 20 个槽，67 个模块。其中，1、2 槽已经有固定作用，还有 18 个槽可用。每个槽可配置 1 个模块，相当于最多可以建立 18 种 Profibus 的输入输出缓冲区到 Modbus 存储区的对应关系。

G0306-SS 跟其他 Modbus 从站设备一样，具有 4 个 Modbus 存储区：

表 1 Modbus 存储区

存储区标识	名称	类型	Modbus 主站读/写	存储单元地址范围
0xxxx	线圈	Bit	读/写	00001~01944, 共 1944bit=243byte
1xxxx	离散量输入	Bit	只读	10001~11944, 共 1944bit=243byte
4xxxx	保持寄存器	Word	读/写	40001~40121, 共 121word=242byte
3xxxx	输入寄存器	Word	只读	30001~30121, 共 121word =242byte

注意：0xxxx、1xxxx、4xxxx、3xxxx 为存储区标识。其中，0, 1, 4, 3 分别标识 4 个不同的存储区。xxxx 为 10 进制的存储单元地址，减 1 后为实际的起始地址。例如：离散量输入起始地址 0000 对应设备中 10001 地址。

## 第4章 网关配置

### 4.1 拓扑结构

#### 4.1.1 网络拓扑

G0306 Modbus 转 DP 网关采用 RS485 传输技术，可以在 9.6kbit/s 到 12Mbit/s 之间选择传输速率。所有设备都被连接到一个总线结构中，并且选择相同的传输速率。在一个总线分段中最多可连接 32 个站（主站或从站）。每个总线分段的开头和结尾均有一个有源的总线终端器。两个总线终端器都有永久不断的供电电源，以确保无差错地运行。总线终端器通常被接入在设备中或在连接器中（注：本网关 PROFIBUS 端无总线终端器，若作为末端，请使用带终端器的连接器）。如果在实现中大于 32 个站或需要扩大网络区域，则必须使用中继器来连接各个总线分段。

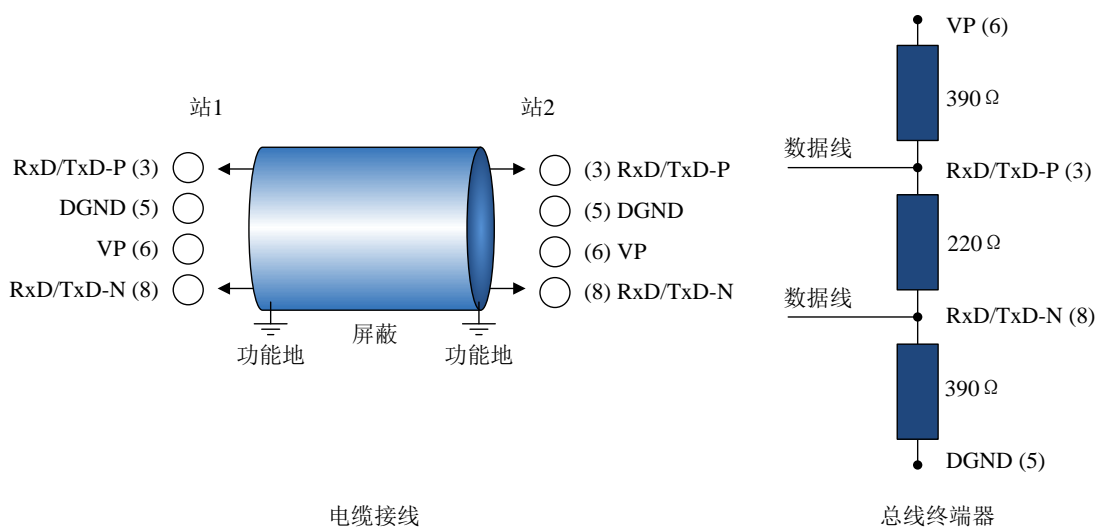


图 8 RS485 传输技术的布线和总线终端器

#### 4.1.2 电缆和连接器

对于不同的应用，在市场上有不同类型的电缆（类型 A-D）可供使用，即可用于设备与设备之间的连接，也可用于设备与网络元件（如，分段耦合器、链接器和中继器）之间的连接。当使用 RS485 传输技术时，PI 建议使用电缆 A。

表 2 电缆类型 A 的传输速率和范围

传输速率 (kbit/s)	每个总线分段的范围 (m)
9.6, 19.2, 45.45, 93.75	1200
187.5	1000
500	400
1500	200
3000, 6000, 12000	100

这些值适用于具有以下特性的 A 型电缆：  
 阻抗：135Ω~165Ω      电容：≤20pF/m  
 回路电阻：≤110Ω/km      线径：>0.64mm  
 导线截面积：>0.34mm<sup>2</sup>

## 4.2 设置网关地址

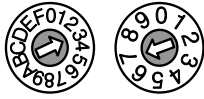
注：本网关不支持通过 Set\_Address 服务设置设备地址，仅支持硬件设地址。

首先，请在断电情况下设置地址。

PROFIBUS 地址配置接口包含两个旋钮拨码开关，PROFIBUS 地址是通过这两个旋钮拨码开关来设定的。

设定方法如下：

$$\text{PROFIBUS 总线地址} = (\text{x10 旋钮拨码开关的值}) * 10 + (\text{x1 旋钮拨码开关的值})$$



例如： x10 x1 PROFIBUS 地址=3\*10+7=37

### 4.3 网关循环组态

Profibus 设备的循环组态均是通过 GSD 文件实现的。Profibus 网络主站通过 GSD 文件执行设备初始化进程。主站将配置好的参数以及输入输出数据组态发送给从站。从站检测无误后，即可进入循环数据交换状态。

#### 4.3.1 GSD 文件说明

GSD 文件中包含了软硬件版本、总线波特率、循环数据交换相关信息等。由于网关有 MS 和 SS 的区别，所以本公司为该类产品申请了两个设备 ID，分别用于 G0306-MS、G0306-SS。用户需要根据实际的配置（详见 2.2.7）选择对应的 GSD 文件。

##### (1) G0306-MS 的 GSD 文件说明

用于 G0306-MS 的 GSD 文件名称为：MCYB0F1A.GSE。

此 GSD 文件包含 39 个槽，209 个模块，最多支持 237 个用户参数。

#### ● 模块描述

表 3 G0306-MS 的 GSD 模块描述

模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
1	empty	0	0	空模块
2	status	1	0	Modbus 通信状态模块
3	control	0	1	Modbus 通信控制模块
4	read 8 bits(0xxxx)	1	0	从某 Modbus 从站使用功能码 1 读取 8 个线圈数据
5	read 8 bits(1xxxx)	1	0	从某 Modbus 从站使用功能码 2 读取 8 个离散量输入
6	read 16 bits(0xxxx)	2	0	从某 Modbus 从站使用功能码 1 读取 16 个线圈数据
7	read 16 bits(1xxxx)	2	0	从某 Modbus 从站使用功能码 2 读取 16 个离散量输入
8	read 24 bits(0xxxx)	3	0	从某 Modbus 从站使用功能码 1 读取 24 个线圈数据
9	read 24 bits(1xxxx)	3	0	从某 Modbus 从站使用功能码 2 读取 24 个离散量输入
10	read 32 bits(0xxxx)	4	0	从某 Modbus 从站使用功能码 1 读取 32 个线圈数据
11	read 32 bits(1xxxx)	4	0	从某 Modbus 从站使用功能码 2 读取 32 个离散量输入
12	read 40 bits(0xxxx)	5	0	从某 Modbus 从站使用功能码 1 读取 40 个线圈数据
13	read 40 bits(1xxxx)	5	0	从某 Modbus 从站使用功能码 2 读取 40 个离散量输入
14	read 48 bits(0xxxx)	6	0	从某 Modbus 从站使用功能码 1 读取 48 个线圈数据
15	read 48 bits(1xxxx)	6	0	从某 Modbus 从站使用功能码 2 读取 48 个离散量输入
16	read 56 bits(0xxxx)	7	0	从某 Modbus 从站使用功能码 1 读取 56 个线圈数据
17	read 56 bits(1xxxx)	7	0	从某 Modbus 从站使用功能码 2 读取 56 个离散量输入
18	read 64 bits(0xxxx)	8	0	从某 Modbus 从站使用功能码 1 读取 64 个线圈数据
19	read 64 bits(1xxxx)	8	0	从某 Modbus 从站使用功能码 2 读取 64 个离散量输入
20	read 72 bits(0xxxx)	9	0	从某 Modbus 从站使用功能码 1 读取 72 个线圈数据
21	read 72 bits(1xxxx)	9	0	从某 Modbus 从站使用功能码 2 读取 72 个离散量输入



模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
22	read 80 bits(0xxxx)	10	0	从某 Modbus 从站使用功能码 1 读取 80 个线圈数据
23	read 80 bits(1xxxx)	10	0	从某 Modbus 从站使用功能码 2 读取 80 个离散量输入
24	read 88 bits(0xxxx)	11	0	从某 Modbus 从站使用功能码 1 读取 88 个线圈数据
25	read 88 bits(1xxxx)	11	0	从某 Modbus 从站使用功能码 2 读取 88 个离散量输入
26	read 96 bits(0xxxx)	12	0	从某 Modbus 从站使用功能码 1 读取 96 个线圈数据
27	read 96 bits(1xxxx)	12	0	从某 Modbus 从站使用功能码 2 读取 96 个离散量输入
28	read 104 bits(0xxxx)	13	0	从某 Modbus 从站使用功能码 1 读取 104 个线圈数据
29	read 104 bits(1xxxx)	13	0	从某 Modbus 从站使用功能码 2 读取 104 个离散量输入
30	read 112 bits(0xxxx)	14	0	从某 Modbus 从站使用功能码 1 读取 112 个线圈数据
31	read 112 bits(1xxxx)	14	0	从某 Modbus 从站使用功能码 2 读取 112 个离散量输入
32	read 120 bits(0xxxx)	15	0	从某 Modbus 从站使用功能码 1 读取 120 个线圈数据
33	read 120 bits(1xxxx)	15	0	从某 Modbus 从站使用功能码 2 读取 120 个离散量输入
34	read 128 bits(0xxxx)	16	0	从某 Modbus 从站使用功能码 1 读取 128 个线圈数据
35	read 128 bits(1xxxx)	16	0	从某 Modbus 从站使用功能码 2 读取 128 个离散量输入
36	read 136 bits(0xxxx)	17	0	从某 Modbus 从站使用功能码 1 读取 136 个线圈数据
37	read 136 bits(1xxxx)	17	0	从某 Modbus 从站使用功能码 2 读取 136 个离散量输入
38	read 144 bits(0xxxx)	18	0	从某 Modbus 从站使用功能码 1 读取 144 个线圈数据
39	read 144 bits(1xxxx)	18	0	从某 Modbus 从站使用功能码 2 读取 144 个离散量输入
40	read 152 bits(0xxxx)	19	0	从某 Modbus 从站使用功能码 1 读取 152 个线圈数据
41	read 152 bits(1xxxx)	19	0	从某 Modbus 从站使用功能码 2 读取 152 个离散量输入
42	read 160 bits(0xxxx)	20	0	从某 Modbus 从站使用功能码 1 读取 160 个线圈数据
43	read 160 bits(1xxxx)	20	0	从某 Modbus 从站使用功能码 2 读取 160 个离散量输入
44	read 168 bits(0xxxx)	21	0	从某 Modbus 从站使用功能码 1 读取 168 个线圈数据
45	read 168 bits(1xxxx)	21	0	从某 Modbus 从站使用功能码 2 读取 168 个离散量输入
46	read 176 bits(0xxxx)	22	0	从某 Modbus 从站使用功能码 1 读取 176 个线圈数据
47	read 176 bits(1xxxx)	22	0	从某 Modbus 从站使用功能码 2 读取 176 个离散量输入
48	read 184 bits(0xxxx)	23	0	从某 Modbus 从站使用功能码 1 读取 184 个线圈数据
49	read 184 bits(1xxxx)	23	0	从某 Modbus 从站使用功能码 2 读取 184 个离散量输入
50	read 192 bits(0xxxx)	24	0	从某 Modbus 从站使用功能码 1 读取 192 个线圈数据
51	read 192 bits(1xxxx)	24	0	从某 Modbus 从站使用功能码 2 读取 192 个离散量输入
52	read 200 bits(0xxxx)	25	0	从某 Modbus 从站使用功能码 1 读取 200 个线圈数据
53	read 200 bits(1xxxx)	25	0	从某 Modbus 从站使用功能码 2 读取 200 个离散量输入
54	read 208 bits(0xxxx)	26	0	从某 Modbus 从站使用功能码 1 读取 208 个线圈数据
55	read 208 bits(1xxxx)	26	0	从某 Modbus 从站使用功能码 2 读取 208 个离散量输入
56	read 216 bits(0xxxx)	27	0	从某 Modbus 从站使用功能码 1 读取 216 个线圈数据
57	read 216 bits(1xxxx)	27	0	从某 Modbus 从站使用功能码 2 读取 216 个离散量输入
58	read 224 bits(0xxxx)	28	0	从某 Modbus 从站使用功能码 1 读取 224 个线圈数据
59	read 224 bits(1xxxx)	28	0	从某 Modbus 从站使用功能码 2 读取 224 个离散量输入
60	read 232 bits(0xxxx)	29	0	从某 Modbus 从站使用功能码 1 读取 232 个线圈数据
61	read 232 bits(1xxxx)	29	0	从某 Modbus 从站使用功能码 2 读取 232 个离散量输入
62	read 240 bits(0xxxx)	30	0	从某 Modbus 从站使用功能码 1 读取 240 个线圈数据
63	read 240 bits(1xxxx)	30	0	从某 Modbus 从站使用功能码 2 读取 240 个离散量输入
64	read 248 bits(0xxxx)	31	0	从某 Modbus 从站使用功能码 1 读取 248 个线圈数据
65	read 248 bits(1xxxx)	31	0	从某 Modbus 从站使用功能码 2 读取 248 个离散量输入
66	read 256 bits(0xxxx)	32	0	从某 Modbus 从站使用功能码 1 读取 256 个线圈数据
67	read 256 bits(1xxxx)	32	0	从某 Modbus 从站使用功能码 2 读取 256 个离散量输入
68	read 1 Words(4xxxx)	2	0	从某 Modbus 从站使用功能码 3 读取 1 个寄存器数据
69	read 1 Words(3xxxx)	2	0	从某 Modbus 从站使用功能码 4 读取 1 个寄存器数据
70	read 2 Words(4xxxx)	4	0	从某 Modbus 从站使用功能码 3 读取 2 个寄存器数据
71	read 2 Words(3xxxx)	4	0	从某 Modbus 从站使用功能码 4 读取 2 个寄存器数据
72	read 3 Words(4xxxx)	6	0	从某 Modbus 从站使用功能码 3 读取 3 个寄存器数据
73	read 3 Words(3xxxx)	6	0	从某 Modbus 从站使用功能码 4 读取 3 个寄存器数据
74	read 4 Words(4xxxx)	8	0	从某 Modbus 从站使用功能码 3 读取 4 个寄存器数据
75	read 4 Words(3xxxx)	8	0	从某 Modbus 从站使用功能码 4 读取 4 个寄存器数据
76	read 5 Words(4xxxx)	10	0	从某 Modbus 从站使用功能码 3 读取 5 个寄存器数据



模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
77	read 5 Words (3xxxx)	10	0	从某 Modbus 从站使用功能码 4 读取 5 个寄存器数据
78	read 6 Words (4xxxx)	12	0	从某 Modbus 从站使用功能码 3 读取 6 个寄存器数据
79	read 6 Words (3xxxx)	12	0	从某 Modbus 从站使用功能码 4 读取 6 个寄存器数据
80	read 7 Words (4xxxx)	14	0	从某 Modbus 从站使用功能码 3 读取 7 个寄存器数据
81	read 7 Words (3xxxx)	14	0	从某 Modbus 从站使用功能码 4 读取 7 个寄存器数据
82	read 8 Words (4xxxx)	16	0	从某 Modbus 从站使用功能码 3 读取 8 个寄存器数据
83	read 8 Words (3xxxx)	16	0	从某 Modbus 从站使用功能码 4 读取 8 个寄存器数据
84	read 9 Words (4xxxx)	18	0	从某 Modbus 从站使用功能码 3 读取 9 个寄存器数据
85	read 9 Words (3xxxx)	18	0	从某 Modbus 从站使用功能码 4 读取 9 个寄存器数据
86	read 10 Words (4xxxx)	20	0	从某 Modbus 从站使用功能码 3 读取 10 个寄存器数据
87	read 10 Words (3xxxx)	20	0	从某 Modbus 从站使用功能码 4 读取 10 个寄存器数据
88	read 11 Words (4xxxx)	22	0	从某 Modbus 从站使用功能码 3 读取 11 个寄存器数据
89	read 11 Words (3xxxx)	22	0	从某 Modbus 从站使用功能码 4 读取 11 个寄存器数据
90	read 12 Words (4xxxx)	24	0	从某 Modbus 从站使用功能码 3 读取 12 个寄存器数据
91	read 12 Words (3xxxx)	24	0	从某 Modbus 从站使用功能码 4 读取 12 个寄存器数据
92	read 13 Words (4xxxx)	26	0	从某 Modbus 从站使用功能码 3 读取 13 个寄存器数据
93	read 13 Words (3xxxx)	26	0	从某 Modbus 从站使用功能码 4 读取 13 个寄存器数据
94	read 14 Words (4xxxx)	28	0	从某 Modbus 从站使用功能码 3 读取 14 个寄存器数据
95	read 14 Words (3xxxx)	28	0	从某 Modbus 从站使用功能码 4 读取 14 个寄存器数据
96	read 15 Words (4xxxx)	30	0	从某 Modbus 从站使用功能码 3 读取 15 个寄存器数据
97	read 15 Words (3xxxx)	30	0	从某 Modbus 从站使用功能码 4 读取 15 个寄存器数据
98	read 16 Words (4xxxx)	32	0	从某 Modbus 从站使用功能码 3 读取 16 个寄存器数据
99	read 16 Words (3xxxx)	32	0	从某 Modbus 从站使用功能码 4 读取 16 个寄存器数据
100	read 18 Words (4xxxx)	36	0	从某 Modbus 从站使用功能码 3 读取 18 个寄存器数据
101	read 18 Words (3xxxx)	36	0	从某 Modbus 从站使用功能码 4 读取 18 个寄存器数据
102	read 20 Words (4xxxx)	40	0	从某 Modbus 从站使用功能码 3 读取 20 个寄存器数据
103	read 20 Words (3xxxx)	40	0	从某 Modbus 从站使用功能码 4 读取 20 个寄存器数据
104	read 22 Words (4xxxx)	44	0	从某 Modbus 从站使用功能码 3 读取 22 个寄存器数据
105	read 22 Words (3xxxx)	44	0	从某 Modbus 从站使用功能码 4 读取 22 个寄存器数据
106	read 24 Words (4xxxx)	48	0	从某 Modbus 从站使用功能码 3 读取 24 个寄存器数据
107	read 24 Words (3xxxx)	48	0	从某 Modbus 从站使用功能码 4 读取 24 个寄存器数据
108	read 26 Words (4xxxx)	52	0	从某 Modbus 从站使用功能码 3 读取 26 个寄存器数据
109	read 26 Words (3xxxx)	52	0	从某 Modbus 从站使用功能码 4 读取 26 个寄存器数据
110	read 28 Words (4xxxx)	56	0	从某 Modbus 从站使用功能码 3 读取 28 个寄存器数据
111	read 28 Words (3xxxx)	56	0	从某 Modbus 从站使用功能码 4 读取 28 个寄存器数据
112	read 30 Words (4xxxx)	60	0	从某 Modbus 从站使用功能码 3 读取 30 个寄存器数据
113	read 30 Words (3xxxx)	60	0	从某 Modbus 从站使用功能码 4 读取 30 个寄存器数据
114	read 32 Words (4xxxx)	64	0	从某 Modbus 从站使用功能码 3 读取 32 个寄存器数据
115	read 32 Words (3xxxx)	64	0	从某 Modbus 从站使用功能码 4 读取 32 个寄存器数据
116	read 34 Words (4xxxx)	68	0	从某 Modbus 从站使用功能码 3 读取 34 个寄存器数据
117	read 34 Words (3xxxx)	68	0	从某 Modbus 从站使用功能码 4 读取 34 个寄存器数据
118	read 36 Words (4xxxx)	72	0	从某 Modbus 从站使用功能码 3 读取 36 个寄存器数据
119	read 36 Words (3xxxx)	72	0	从某 Modbus 从站使用功能码 4 读取 36 个寄存器数据
120	read 38 Words (4xxxx)	76	0	从某 Modbus 从站使用功能码 3 读取 38 个寄存器数据
121	read 38 Words (3xxxx)	76	0	从某 Modbus 从站使用功能码 4 读取 38 个寄存器数据
122	read 40 Words (4xxxx)	80	0	从某 Modbus 从站使用功能码 3 读取 40 个寄存器数据
123	read 40 Words (3xxxx)	80	0	从某 Modbus 从站使用功能码 4 读取 40 个寄存器数据
124	read 42 Words (4xxxx)	84	0	从某 Modbus 从站使用功能码 3 读取 42 个寄存器数据
125	read 42 Words (3xxxx)	84	0	从某 Modbus 从站使用功能码 4 读取 42 个寄存器数据
126	read 44 Words (4xxxx)	88	0	从某 Modbus 从站使用功能码 3 读取 44 个寄存器数据
127	read 44 Words (3xxxx)	88	0	从某 Modbus 从站使用功能码 4 读取 44 个寄存器数据
128	read 46 Words (4xxxx)	92	0	从某 Modbus 从站使用功能码 3 读取 46 个寄存器数据
129	read 46 Words (3xxxx)	92	0	从某 Modbus 从站使用功能码 4 读取 46 个寄存器数据
130	read 48 Words (4xxxx)	96	0	从某 Modbus 从站使用功能码 3 读取 48 个寄存器数据
131	read 48 Words (3xxxx)	96	0	从某 Modbus 从站使用功能码 4 读取 48 个寄存器数据





模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
132	read 50 Words(4xxxx)	100	0	从某 Modbus 从站使用功能码 3 读取 50 个寄存器数据
133	read 50 Words(3xxxx)	100	0	从某 Modbus 从站使用功能码 4 读取 50 个寄存器数据
134	read 52 Words(4xxxx)	104	0	从某 Modbus 从站使用功能码 3 读取 52 个寄存器数据
135	read 52 Words(3xxxx)	104	0	从某 Modbus 从站使用功能码 4 读取 52 个寄存器数据
136	read 54 Words(4xxxx)	108	0	从某 Modbus 从站使用功能码 3 读取 54 个寄存器数据
137	read 54 Words(3xxxx)	108	0	从某 Modbus 从站使用功能码 4 读取 54 个寄存器数据
138	read 56 Words(4xxxx)	112	0	从某 Modbus 从站使用功能码 3 读取 56 个寄存器数据
139	read 56 Words(3xxxx)	112	0	从某 Modbus 从站使用功能码 4 读取 56 个寄存器数据
140	read 58 Words(4xxxx)	116	0	从某 Modbus 从站使用功能码 3 读取 58 个寄存器数据
141	read 58 Words(3xxxx)	116	0	从某 Modbus 从站使用功能码 4 读取 58 个寄存器数据
142	read 60 Words(4xxxx)	120	0	从某 Modbus 从站使用功能码 3 读取 60 个寄存器数据
143	read 60 Words(3xxxx)	120	0	从某 Modbus 从站使用功能码 4 读取 60 个寄存器数据
144	write 8 bits(0xxxx)	0	1	使用功能码 15 往某 Modbus 从站写入 1~8 个线圈数据
145	write 16 bits(0xxxx)	0	2	使用功能码 15 往某 Modbus 从站写入 1~16 个线圈数据
146	write 24 bits(0xxxx)	0	3	使用功能码 15 往某 Modbus 从站写入 1~24 个线圈数据
147	write 32 bits(0xxxx)	0	4	使用功能码 15 往某 Modbus 从站写入 1~32 个线圈数据
148	write 40 bits(0xxxx)	0	5	使用功能码 15 往某 Modbus 从站写入 1~40 个线圈数据
149	write 48 bits(0xxxx)	0	6	使用功能码 15 往某 Modbus 从站写入 1~48 个线圈数据
150	write 56 bits(0xxxx)	0	7	使用功能码 15 往某 Modbus 从站写入 1~56 个线圈数据
151	write 64 bits(0xxxx)	0	8	使用功能码 15 往某 Modbus 从站写入 1~64 个线圈数据
152	write 72 bits(0xxxx)	0	9	使用功能码 15 往某 Modbus 从站写入 1~72 个线圈数据
153	write 80 bits(0xxxx)	0	10	使用功能码 15 往某 Modbus 从站写入 1~80 个线圈数据
154	write 88 bits(0xxxx)	0	11	使用功能码 15 往某 Modbus 从站写入 1~88 个线圈数据
155	write 96 bits(0xxxx)	0	12	使用功能码 15 往某 Modbus 从站写入 1~96 个线圈数据
156	write 104 bits(0xxxx)	0	13	使用功能码 15 往某 Modbus 从站写入 1~104 个线圈数据
157	write 112 bits(0xxxx)	0	14	使用功能码 15 往某 Modbus 从站写入 1~112 个线圈数据
158	write 120 bits(0xxxx)	0	15	使用功能码 15 往某 Modbus 从站写入 1~120 个线圈数据
159	write 128 bits(0xxxx)	0	16	使用功能码 15 往某 Modbus 从站写入 1~128 个线圈数据
160	write 136 bits(0xxxx)	0	17	使用功能码 15 往某 Modbus 从站写入 1~136 个线圈数据
161	write 144 bits(0xxxx)	0	18	使用功能码 15 往某 Modbus 从站写入 1~144 个线圈数据
162	write 152 bits(0xxxx)	0	19	使用功能码 15 往某 Modbus 从站写入 1~152 个线圈数据
163	write 160 bits(0xxxx)	0	20	使用功能码 15 往某 Modbus 从站写入 1~160 个线圈数据
164	write 168 bits(0xxxx)	0	21	使用功能码 15 往某 Modbus 从站写入 1~168 个线圈数据
165	write 176 bits(0xxxx)	0	22	使用功能码 15 往某 Modbus 从站写入 1~176 个线圈数据
166	write 184 bits(0xxxx)	0	23	使用功能码 15 往某 Modbus 从站写入 1~184 个线圈数据
167	write 192 bits(0xxxx)	0	24	使用功能码 15 往某 Modbus 从站写入 1~192 个线圈数据
168	write 200 bits(0xxxx)	0	25	使用功能码 15 往某 Modbus 从站写入 1~200 个线圈数据
169	write 208 bits(0xxxx)	0	26	使用功能码 15 往某 Modbus 从站写入 1~208 个线圈数据
170	write 216 bits(0xxxx)	0	27	使用功能码 15 往某 Modbus 从站写入 1~216 个线圈数据
171	write 224 bits(0xxxx)	0	28	使用功能码 15 往某 Modbus 从站写入 1~224 个线圈数据
172	write 232 bits(0xxxx)	0	29	使用功能码 15 往某 Modbus 从站写入 1~232 个线圈数据
173	write 240 bits(0xxxx)	0	30	使用功能码 15 往某 Modbus 从站写入 1~240 个线圈数据
174	write 248 bits(0xxxx)	0	31	使用功能码 15 往某 Modbus 从站写入 1~248 个线圈数据
175	write 256 bits(0xxxx)	0	32	使用功能码 15 往某 Modbus 从站写入 1~256 个线圈数据
176	write 1 Words(4xxxx)	0	2	使用功能码 16 往某 Modbus 从站写入 1 个寄存器数据
177	write 2 Words(4xxxx)	0	4	使用功能码 16 往某 Modbus 从站写入 2 个寄存器数据
178	write 3 Words(4xxxx)	0	6	使用功能码 16 往某 Modbus 从站写入 3 个寄存器数据
179	write 4 Words(4xxxx)	0	8	使用功能码 16 往某 Modbus 从站写入 4 个寄存器数据
180	write 5 Words(4xxxx)	0	10	使用功能码 16 往某 Modbus 从站写入 5 个寄存器数据
181	write 6 Words(4xxxx)	0	12	使用功能码 16 往某 Modbus 从站写入 6 个寄存器数据
182	write 7 Words(4xxxx)	0	14	使用功能码 16 往某 Modbus 从站写入 7 个寄存器数据
183	write 8 Words(4xxxx)	0	16	使用功能码 16 往某 Modbus 从站写入 8 个寄存器数据
184	write 9 Words(4xxxx)	0	18	使用功能码 16 往某 Modbus 从站写入 9 个寄存器数据
185	write 10 Words(4xxxx)	0	20	使用功能码 16 往某 Modbus 从站写入 10 个寄存器数据
186	write 11 Words(4xxxx)	0	22	使用功能码 16 往某 Modbus 从站写入 11 个寄存器数据



模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
187	write 12 Words(4xxxx)	0	24	使用功能码 16 往某 Modbus 从站写入 12 个寄存器数据
188	write 13 Words(4xxxx)	0	26	使用功能码 16 往某 Modbus 从站写入 13 个寄存器数据
189	write 14 Words(4xxxx)	0	28	使用功能码 16 往某 Modbus 从站写入 14 个寄存器数据
190	write 15 Words(4xxxx)	0	30	使用功能码 16 往某 Modbus 从站写入 15 个寄存器数据
191	write 16 Words(4xxxx)	0	32	使用功能码 16 往某 Modbus 从站写入 16 个寄存器数据
192	write 18 Words(4xxxx)	0	36	使用功能码 16 往某 Modbus 从站写入 18 个寄存器数据
193	write 20 Words(4xxxx)	0	40	使用功能码 16 往某 Modbus 从站写入 20 个寄存器数据
194	write 22 Words(4xxxx)	0	44	使用功能码 16 往某 Modbus 从站写入 22 个寄存器数据
195	write 24 Words(4xxxx)	0	48	使用功能码 16 往某 Modbus 从站写入 24 个寄存器数据
196	write 26 Words(4xxxx)	0	52	使用功能码 16 往某 Modbus 从站写入 26 个寄存器数据
197	write 28 Words(4xxxx)	0	56	使用功能码 16 往某 Modbus 从站写入 28 个寄存器数据
198	write 30 Words(4xxxx)	0	60	使用功能码 16 往某 Modbus 从站写入 30 个寄存器数据
199	write 32 Words(4xxxx)	0	64	使用功能码 16 往某 Modbus 从站写入 32 个寄存器数据
200	force single bit (05H Command)	0	1	使用功能码 5 往某 Modbus 从站写入 1 个线圈数据
201	set single word (06H Command)	0	2	使用功能码 6 往某 Modbus 从站写入 1 个寄存器数据
202	8Bits MODBUS Slaves Status	1	0	读取 8 位 Modbus 从站状态
203	8Bytes MODBUS Slaves Status	8	0	读取 8 字节 Modbus 从站状态
204	16Bits MODBUS Slaves Status	2	0	读取 16 位 Modbus 从站状态
205	16Bytes MODBUS Slaves Status	16	0	读取 16 字节 Modbus 从站状态
206	24Bits MODBUS Slaves Status	3	0	读取 24 位 Modbus 从站状态
207	24Bytes MODBUS Slaves Status	24	0	读取 24 字节 Modbus 从站状态
208	32Bits MODBUS Slaves Status	4	0	读取 32 位 Modbus 从站状态
209	32Bytes MODBUS Slaves Status	32	0	读取 32 字节 Modbus 从站状态

如上表所示，上述 209 个模块大致可以分为 4 类：

- a) 空模块（模块 1）
- b) Modbus 通信模块（模块 4-201）
- c) 控制模块（模块 3）
- d) 总状态模块（模块 2）以及详细状态模块（202-209）

其中，槽 1 固定为总状态模块（模块 2），槽 2 固定为控制模块（模块 3），其余 37 个槽可根据需求任意配置。

注意：如有详细状态模块需求（模块 202-209），详细状态模块仅能放在最后一个有效槽（例如：Modbus 通信模块使用了 5 个槽，那么槽 1 为总状态模块，槽 2 为控制模块，槽 3-7 为 Modbus 通信模块，槽 8 在此例子中为最后一个有效槽，如需要详细状态模块，则放入槽 8 中）。

Modbus 通信相关配置是通过用户参数来实现的，这部分用户参数将其命名为**设备用户参数**。除了前三个模块外，其余所有模块均有用户参数可以配置，这部分参数将其命名为**模块用户参数**。

### ● 设备用户参数

此部分参数包含了 Modbus 通信波特率、校验信息、数据更新模式、写入模式、主站发送间隔、间隔时

间、以及是否有 Modbus 从站状态检测等信息。

表 4 G0306-MS 设备用户参数表

序号	参数名称	描述
1	波特率 (Baudrate)	0:300 bps 1:600 bps 2:1200 bps 3:2400 bps 4:4800 bps 5:9600 bps 6:19200 bps 7:38400 bps 8:57600 bps
2	校验 (Parity)	0:8 位, 无校验, 1 停止位(8Bits, No Parity, 1stop bit) 1:8 位, 偶校验, 1 停止位(8Bits, Even Parity, 1stop bit) 2:8 位, 奇校验, 1 停止位(8Bits, Odd Parity, 1stop bit) 3:8 位, 无校验, 2 停止位(8Bits, No Parity, 2stop bits)
3	MODBUS 从站状态监测 (MODBUS Slave Monitoring)	此参数非 0 时, 必须使用相对应的详细状态模块(202-209) 0:无状态监测(NoMonitoring) 1:8 位状态监测(8BitsMonitoring) 2:8 字节状态监测(8BytesMonitoring) 3:16 位状态监测(16BitsMonitoring) 4:16 字节状态监测(16BytesMonitoring) 5:24 位状态监测(24BitsMonitoring) 6:24 字节状态监测(24BytesMonitoring) 7:32 位状态监测(32BitsMonitoring) 8:32 字节状态监测(32BytesMonitoring)
4	数据更新模式 (Data Update Mode)	1:在全部 MD 响应后(All Items End) 2:在每条 MD 响应后(Each Item End)
5	写入模式 (Writing Mode)	0:一直写(Write always) 1:数据变化时写(Write on change)
6	主站发送间隔 (Master Send Interval)	0:从站应答发送(Slave Response) 此种方式如果从站没有响应, 那么响应超时时间固定为 1 秒。 1:相同时间间隔发送(Same Interval) 此种方式发送间隔与响应超时时间均为间隔时间值参数所设定的时间。
7	间隔时间值 (Interval Timer Value)	1:10ms 2:20ms 3:30ms 4:40ms 5:50ms 6:60ms 8:80ms 10:100ms 12:120ms 15:150ms 20:200ms 25:250ms 30:300ms 35:350ms 40:400ms 45:450ms 50:500ms 55:550ms 60:600ms 65:650ms 70:700ms 75:750ms 80:800ms 85:850ms 90:900ms

	95:950ms 100:1000ms 255:无限期待响应 (Waiting...)
--	---

### ● 模块用户参数

此部分参数，与实际的 Modbus 从设备相关，包含 Modbus 从设备地址、要读写的 Modbus 寄存器起始地址、要写入的输出数据数量等。

表 5 G0306-MS 模块（4-143、176-199）用户参数表

序号	参数名称	描述
1	Modbus 从站地址 (MODBUS Slave Address)	Modbus 从站地址，地址范围 0-255。
2	起始地址 (Starting Address)	所要读写数据的寄存器起始地址。

表 6 G0306-MS 模块（144-175）用户参数表

序号	参数名称	描述
1	Modbus 从站地址 (MODBUS Slave Address)	Modbus 从站地址，地址范围 0-255。
2	起始地址 (Starting Address)	所要读写数据的寄存器起始地址。
3	输出线圈数量 (Quantity of Outputs)	输出线圈数量。

表 7 G0306-MS 模块 200 用户参数表

序号	参数名称	描述
1	Modbus 从站地址 (MODBUS Slave Address)	Modbus 从站地址，地址范围 0-255。
2	输出地址 (Output Address)	被写数据的线圈输出地址。

表 8 G0306-MS 模块 201 用户参数表

序号	参数名称	描述
1	Modbus 从站地址 (MODBUS Slave Address)	Modbus 从站地址，地址范围 0-255。
2	寄存器地址 (Register Address)	被写数据的寄存器地址。

注意：表 4-7 仅列出了这些模块可修改的用户参数，并不是这些模块所有参数。例如：某一模块对应的 Modbus 功能码、读写数据的寄存器数量、字节数等这些与模块相关且不可修改的参数未列在上表中。

表 9 G0306-MS 详细状态模块（202-203）用户参数表

参数长度	参数默认值	描述
8 字节	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08	每个字节代表一个待测 Modbus 从设备地址。

表 10 G0306-MS 详细状态模块（204-205）用户参数表

参数长度	参数默认值	描述
16 字节	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f, 0x10	每个字节代表一个待测 Modbus 从设备地址。

表 11 G0306-MS 详细状态模块（206-207）用户参数表

参数长度	参数默认值	描述
24 字节	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f, 0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18	每个字节代表一个待测 Modbus 从设备地址。

表 12 G0306-MS 详细状态模块（208-209）用户参数表

参数长度	参数默认值	描述
32 字节	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f, 0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19, 0x1a, 0x1b, 0x1c, 0x1d, 0x1e, 0x1f, 0x20	每个字节代表一个待测 Modbus 从设备地址。

## (2) G0306-SS 的 GSD 文件说明

用于 G0306-SS 的 GSD 文件名称为：MCYB0F19.GSE。

此 GSD 文件包含 20 个槽，67 个模块，最多支持 237 个用户参数。

### ● 模块描述

表 13 G0306-SS 的 GSD 模块描述

模块序号	模块名称	输入数据长度 (字节)	输出数据长度 (字节)	描述
1	empty	0	0	空模块
2	status	1	0	Modbus 通信状态模块
3	control	0	1	Modbus 通信控制模块
4	Input:8 bits(0xxxx)	1	0	将 1 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
5	Input:16 bits(0xxxx)	2	0	将 2 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
6	Input:24 bits(0xxxx)	3	0	将 3 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
7	Input:32 bits(0xxxx)	4	0	将 4 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
8	Input:40 bits(0xxxx)	5	0	将 5 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
9	Input:48 bits(0xxxx)	6	0	将 6 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
10	Input:56 bits(0xxxx)	7	0	将 7 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
11	Input:64 bits(0xxxx)	8	0	将 8 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
12	Input:72 bits(0xxxx)	9	0	将 9 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
13	Input:80 bits(0xxxx)	10	0	将 10 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
14	Input:88 bits(0xxxx)	11	0	将 11 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
15	Input:96 bits(0xxxx)	12	0	将 12 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
16	Input:104 bits(0xxxx)	13	0	将 13 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
17	Input:112 bits(0xxxx)	14	0	将 14 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
18	Input:120 bits(0xxxx)	15	0	将 15 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
19	Input:128 bits(0xxxx)	16	0	将 16 个字节输入数据按顺序映射到 Modbus 的 0xxxx 存储区
20	Input:1 Word(4xxxx)	2	0	将 2 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
21	Input:2 Words(4xxxx)	4	0	将 4 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
22	Input:3 Words(4xxxx)	6	0	将 6 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
23	Input:4 Words(4xxxx)	8	0	将 8 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
24	Input:5 Words(4xxxx)	10	0	将 10 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
25	Input:6 Words(4xxxx)	12	0	将 12 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
26	Input:7 Words(4xxxx)	14	0	将 14 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
27	Input:8 Words(4xxxx)	16	0	将 16 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
28	Input:9 Words(4xxxx)	18	0	将 18 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
29	Input:10 Words(4xxxx)	20	0	将 20 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
30	Input:11 Words(4xxxx)	22	0	将 22 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
31	Input:12 Words(4xxxx)	24	0	将 24 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
32	Input:13 Words(4xxxx)	26	0	将 26 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
33	Input:14 Words(4xxxx)	28	0	将 28 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
34	Input:15 Words(4xxxx)	30	0	将 30 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
35	Input:16 Words(4xxxx)	32	0	将 32 个字节输入数据按顺序映射到 Modbus 的 4xxxx 存储区
36	Output:8 bits(1xxxx)	0	1	将 1 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
37	Output:16 bits(1xxxx)	0	2	将 2 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
38	Output:24 bits(1xxxx)	0	3	将 3 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
39	Output:32 bits(1xxxx)	0	4	将 4 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
40	Output:40 bits(1xxxx)	0	5	将 5 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
41	Output:48 bits(1xxxx)	0	6	将 6 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
42	Output:56 bits(1xxxx)	0	7	将 7 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
43	Output:64 bits(1xxxx)	0	8	将 8 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
44	Output:72 bits(1xxxx)	0	9	将 9 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
45	Output:80 bits(1xxxx)	0	10	将 10 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
46	Output:88 bits(1xxxx)	0	11	将 11 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
47	Output:96 bits(1xxxx)	0	12	将 12 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
48	Output:104 bits(1xxxx)	0	13	将 13 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区



模块序号	模块名称	输入数据长度(字节)	输出数据长度(字节)	描述
49	Output:112 bits(1xxxx)	0	14	将 14 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
50	Output:120 bits(1xxxx)	0	15	将 15 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
51	Output:128 bits(1xxxx)	0	16	将 16 个字节输出数据按顺序映射到 Modbus 的 1xxxx 存储区
52	Output:1 Word(3xxxx)	0	2	将 2 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
53	Output:2 Words(3xxxx)	0	4	将 4 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
54	Output:3 Words(3xxxx)	0	6	将 6 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
55	Output:4 Words(3xxxx)	0	8	将 8 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
56	Output:5 Words(3xxxx)	0	10	将 10 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
57	Output:6 Words(3xxxx)	0	12	将 12 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
58	Output:7 Words(3xxxx)	0	14	将 14 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
59	Output:8 Words(3xxxx)	0	16	将 16 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
60	Output:9 Words(3xxxx)	0	18	将 18 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
61	Output:10 Words(3xxxx)	0	20	将 20 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
62	Output:11 Words(3xxxx)	0	22	将 22 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
63	Output:12 Words(3xxxx)	0	24	将 24 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
64	Output:13 Words(3xxxx)	0	26	将 26 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
65	Output:14 Words(3xxxx)	0	28	将 28 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
66	Output:15 Words(3xxxx)	0	30	将 30 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区
67	Output:16 Words(3xxxx)	0	32	将 32 个字节输出数据按顺序映射到 Modbus 的 3xxxx 存储区

如上表所示，上述 67 个模块大致可以分为 4 类：

- a) 空模块（模块 1）
- b) 总状态模块（模块 2）
- c) 控制模块（模块 3）
- d) Modbus 映射模块（模块 4-67）其中，槽 1 固定为总状态模块（模块 2），槽 2 固定为控制模块（模块 3），其余 18 个槽可根据需求任意配置。

Modbus 通信相关配置是通过用户参数来实现的，这部分用户参数将其命名为**设备用户参数**。除了前三个模块外，其余所有模块均有用户参数可以配置，这部分参数将其命名为**模块用户参数**。

### ● 设备用户参数

此部分参数包含了 Modbus 通信波特率、校验信息以及是否有 Modbus 从站状态检测等信息。

表 14 G0306-SS 设备用户参数表

序号	参数名称	描述
1	波特率 (Baudrate)	3:2400 bps 4:4800 bps 5:9600 bps 6:19200 bps 7:38400 bps 8:57600 bps
2	校验 (Parity)	0:8 位, 无校验, 1 停止位(8Bits, No Parity, 1stop bit) 1:8 位, 偶校验, 1 停止位(8Bits, Even Parity, 1stop bit) 2:8 位, 奇校验, 1 停止位(8Bits, Odd Parity, 1stop bit) 3:8 位, 无校验, 2 停止位(8Bits, No Parity, 2stop bits)
3	MODBUS 从站设备地址 (MODBUS Slave Device Address)	此参数用来设定当前网关作为 MODBUS 从设备的地址。范围：1-247。

### ● 模块用户参数

此部分参数，与 Modbus 存储区以及数据长度相关。参数值与模块相关联，不可修改。例如：“Input:24 bits(0xxxx)” 模块的用户参数为 0x00, 0x03。表明此模块与 Modbus 的 0xxxx 存储区相关联，数据长度为

3 个字节。

### ● Modbus 存储区与 Profibus 输入输出数据缓冲区的对应关系

表 15 Modbus 存储区与 Profibus 输入输出数据缓冲区的对应关系表

模块	对应的 Modbus 存储区	输入输出数据最大长度	存储单元地址范围
Input:8 bits(0xxxx) ~ Input:128 bits(0xxxx)	线圈 0xxxx	243 字节=1944bit	0~1943
Output:8 bits(1xxxx) ~ Output:128 bits(1xxxx)	离散量输入 1xxxx	243 字节=1944bit	0~1943
Input:1 Word(4xxxx) ~ Input:16 Words(4xxxx)	保持寄存器 4xxxx	242 字节=121word	0~120
Output:1 Word(3xxxx) ~ Output:16 Words(3xxxx)	输入寄存器 3xxxx	242 字节=121word	0~120

#### 4.3.2 安装 GSD 文件

以西门子 STEP 7 软件、G0306-MS 为例，选择任意工程，打开硬件组态界面，选择“Options Install GSD File…”选项，将打开导入 GSD 文件窗口。

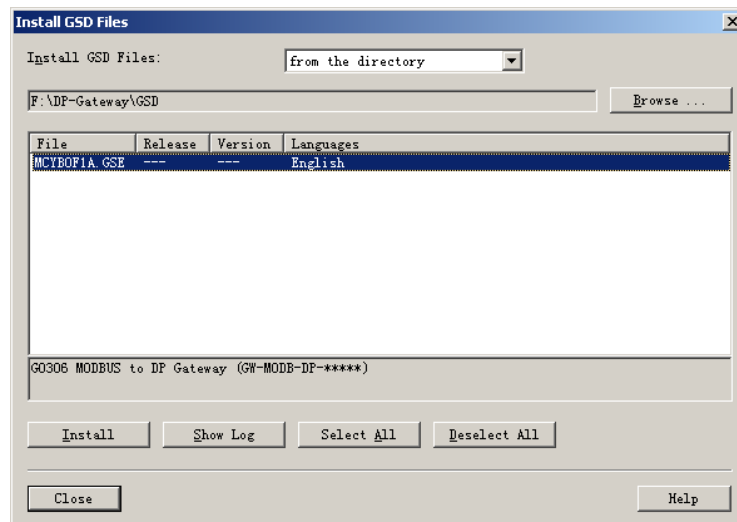


图 9 导入 GSD 文件窗口

点击“Browse…”，选择 GSD 文件所在路径，将会罗列出当前路径下的所有 GSD 文件。选择需要导入的 GSD 文件，然后点击“Install”。一直点击“Yes”，直到出现图 10 为止。

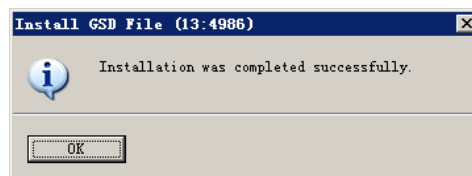


图 10 导入成功

G0306-SS 的 GSD 文件导入方法相同。

#### 4.3.3 使用 GSD 文件

安装好 GSD 文件后，网关将会出现在硬件组态界面的右侧树形列表中。

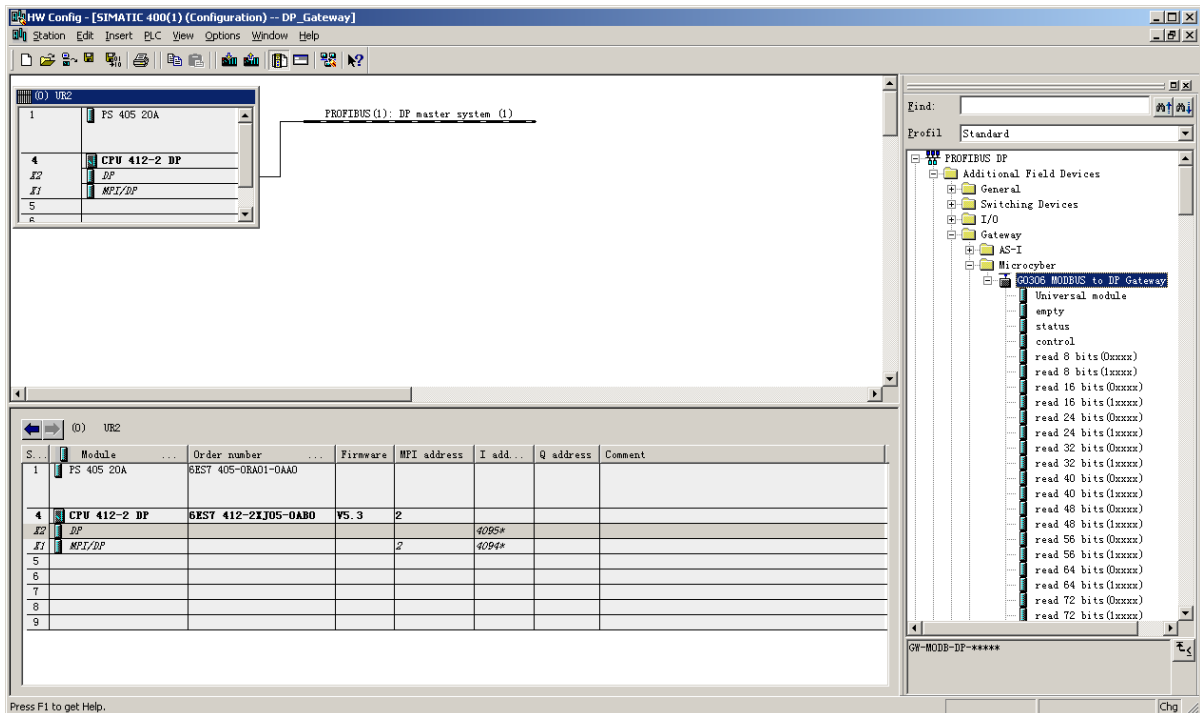


图 11 正确安装的设备

拖拽网关到 DP 总线上。将会自动弹出属性窗口。配置网关地址为您所需的地址。在这里我使用地址 10。

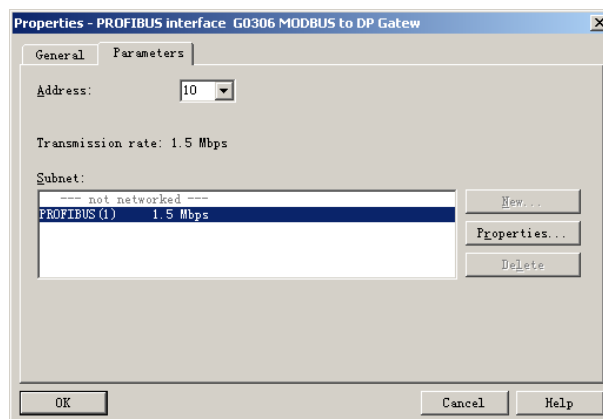


图 12 配置设备属性

点击“OK”，完成网关的添加。

选中组态图中的网关，在视图左下方将会出现该设备的组态配置，如下图所示：



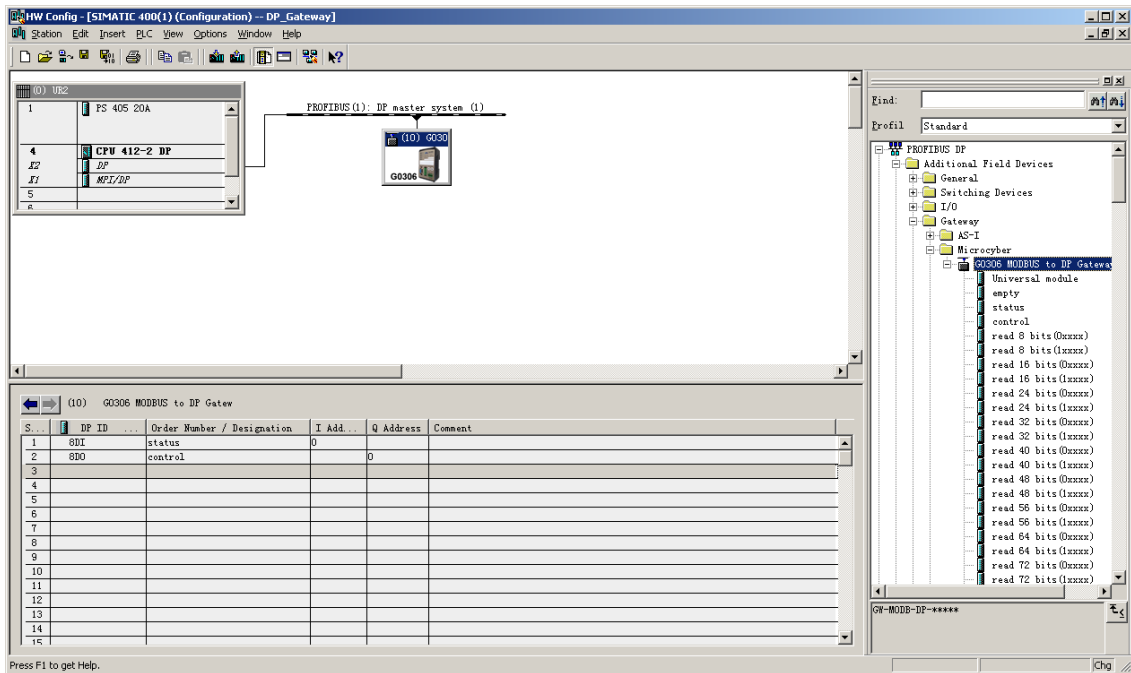


图 13 设备组态配置

在进行硬件组态时，用户根据实际需求，做相应的组态调整，从而使网关的输入输出数据与 Modbus 数据形成有效的组态信息。

G0306-SS 的 GSD 文件导入方法与此相同。

下面将举例说明网关如何使用。

### (1) 如何使用 G0306-MS 的 GSD 文件

#### ● 配置设备用户参数

在如图 13 界面，在网关设备上点右键，选择对象属性 参数分配。

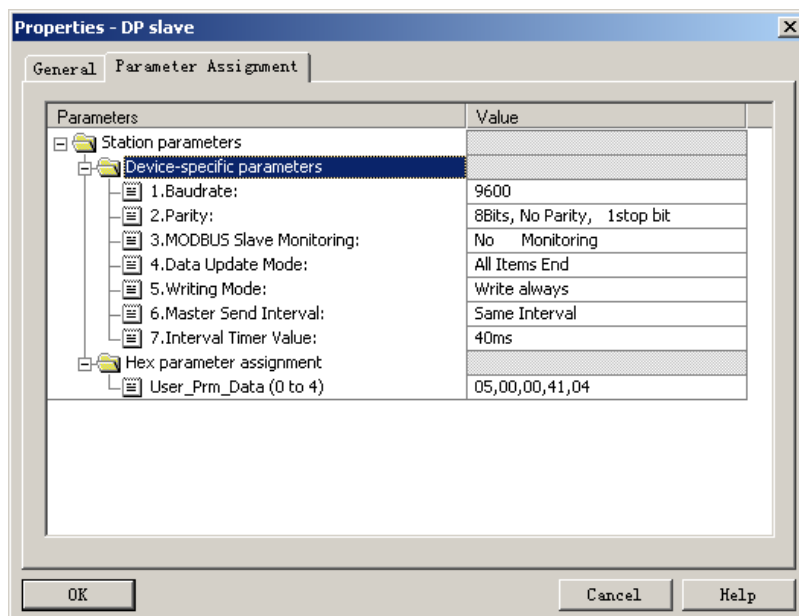


图 14 G0306-MS 设备用户参数配置界面

在这里可以修改表 4 中提到的所有参数。用户要根据实际情况进行修改。例如：间隔时间值就跟选择的波特率、实际连接的从站设备响应时间、连接设备的多少，都有关系，如果配置不当，可能产生连包，导致

从站没有响应，或响应错误。

### ● 配置网关模块简介

在 4.3.1 章 (1) 中已经介绍过，本网关 GSD 中包含 39 个槽，209 个模块，最多支持 237 个用户参数，每个模块选项的具体含义见表 3。

其中，槽 1 固定为总状态模块（模块 2），槽 2 固定为控制模块（模块 3），其余 37 个槽可根据需求任意配置。

以配置“read 24 bits(0xxxx)”模块（模块 8）放入槽 3 举例，选中槽 3，在右侧设备列表中，双击“read 24 bits(0xxxx)”模块即可将该模块添加到槽 3 中。该模块还有模块用户参数可配置，详细配置方法见下文。

本网关根据用户实际配置的模块顺序，形成 Modbus 报文队列。往下将详细介绍各个模块如何使用。

### ● 总状态模块（模块 2）

此模块按照 Modbus 报文队列循环显示每一条 Modbus 报文的实时状态。

表 16 总状态模块格式

B7:奇偶校验	B6:CRC 校验	B5:响应超时	B4-B1:异常响应码	B0:发送/接收
0:当前从站奇偶校验正确	0:当前从站 CRC 正确	0:当前从站响应未超时	详细见附录 A.3	0:发送
1:当前从站奇偶校验错误	1:当前从站 CRC 错误	1:当前从站响应超时		1:接收

#### a) B0:发送/接收

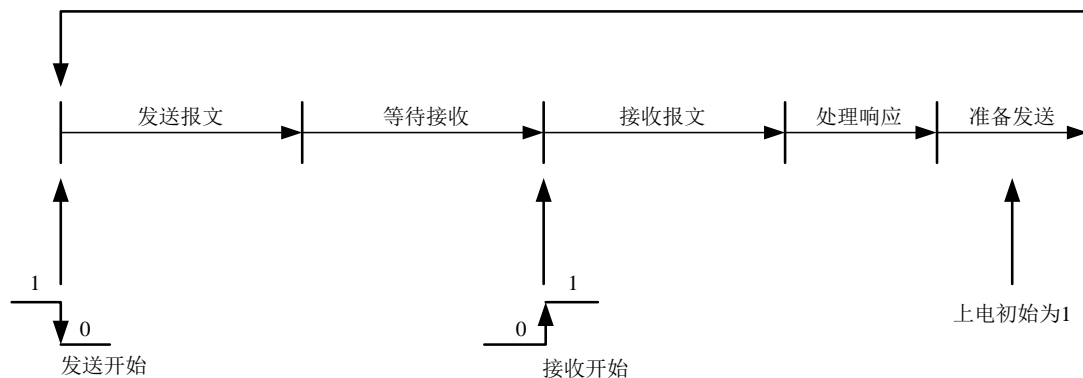


图 15 发送接收状态转换图

如上图所示，设备上电后，此位处于 1 状态。随着 Modbus 报文队列正常运行，此位将如上图所示实时变化。发送时置为 0，接收时置为 1。

#### b) B4-B1:异常响应码

此 4 位用来显示当前 Modbus 报文的异常响应码，异常响应码的具体含义详细见附录 A.3。

注意：此 4 位还有一个特殊用法，即如果某个槽所配置的从站命令，在详细状态模块（202-209）中没有配置检测此从站，则在总状态模块中将异常响应码置为 F。

#### c) B5:响应超时

此位表示按照设备用户参数中主站发送间隔参数、间隔时间值参数的设置，如果用户设备超时没有响应，则此位置 1。Modbus 报文队列指针指向下一条 Modbus 报文。

**d) B6: CRC 校验**

当网关接收到一条 MODBUS 响应报文，CRC 校验出现错误时，此位置 1。此时，网关认为 MODBUS 响应数据不可靠，废弃不用，不与 PROFIBUS 对应数据区交换。

**e) B7: 奇偶校验**

当网关接收数据发现奇偶校验错误时，此位置 1。此时，网关认为 MODBUS 响应数据不可靠，废弃不用，不与 PROFIBUS 对应数据区交换。

**● 控制模块（模块 3）**

此模块用作调度 Modbus 报文。用户可通过此模块启动或停止 Modbus 扫描，调节只读或只写，跳过当前 Modbus 报文等操作。

表 17 控制模块格式

B7: 强制复位	B6: 停止等待	B5: 错误检测	B4-B3: 保留	B2: 写命令	B1: 读命令	B0: 停止/启动
0: 正常执行	0: 正常执行	0: 使能错误检测	——	0: 允许写	0: 允许读	0: 启动 Modbus 扫描
1: 复位	1: 跳过等待	1: 禁止错误检测	——	1: 禁止写	1: 禁止读	1: 停止 Modbus 扫描

**a) B0: 停止/启动**

默认为启动扫描 Modbus 报文队列。用户可将此位置为 1，即停止 Modbus 报文扫描。

**b) B1: 读命令**

默认为允许网关发送 Modbus 读命令。用户可将此位置为 1，即禁止发送 Modbus 读命令（01H、02H、03H、04H 命令）。

**c) B2: 写命令**

默认为允许网关发送 Modbus 写命令。用户可将此位置为 1，即禁止发送 Modbus 写命令（05H、06H、0FH、10H 命令）。

**d) B5: 错误检测**

默认为使能错误检测。用户可将此位置为 1，即禁止错误检测，可用作清除之前的错误信息。

**e) B6: 停止等待**

当设备用户参数中主站发送间隔参数设为相同时间间隔发送且间隔时间值设为无限期等待响应时，此位配置有效。用户可将此位置为 1，可跳过当前等待，Modbus 报文队列扫描下一条 Modbus 报文。

**f) B7: 强制复位**

设置该位，可将 Modbus 报文队列强制复位到扫描第一条 Modbus 报文。

**● 使用读 xxx 位模块举例（模块 4-67）**

这些模块可以使用功能码 1（或 2）来读取任意位数的线圈数据。

以“read 24 bits(0xxxx)”模块为例，此模块使用功能码 1 来读取 24 位线圈数据。



a) 添加“read 24 bits(0xxxx)”模块，如图 16 所示：

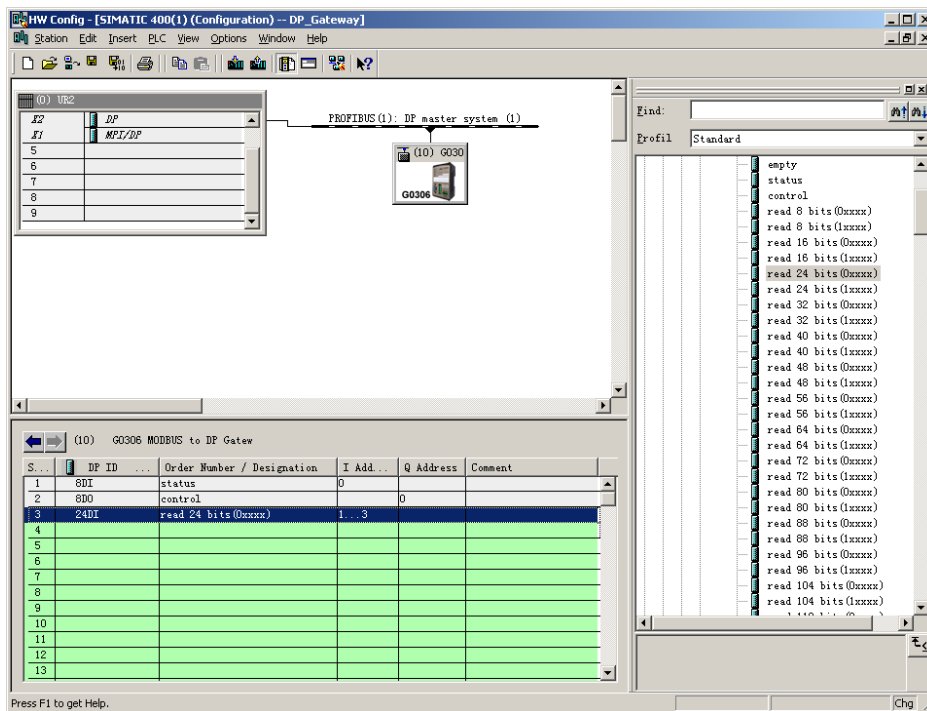


图 16 添加“read 24 bits(0xxxx)”模块

以将此模块放入槽 3 为例，选中槽 3，双击“read 24 bits(0xxxx)”模块。IB1...3 为 Profibus 主站为网关分配的输入数据地址，对应于 Modbus 读取的 24 位线圈(0xxxx)数据。

b) 配置“read 24 bits(0xxxx)”模块用户参数，如图 17 所示：

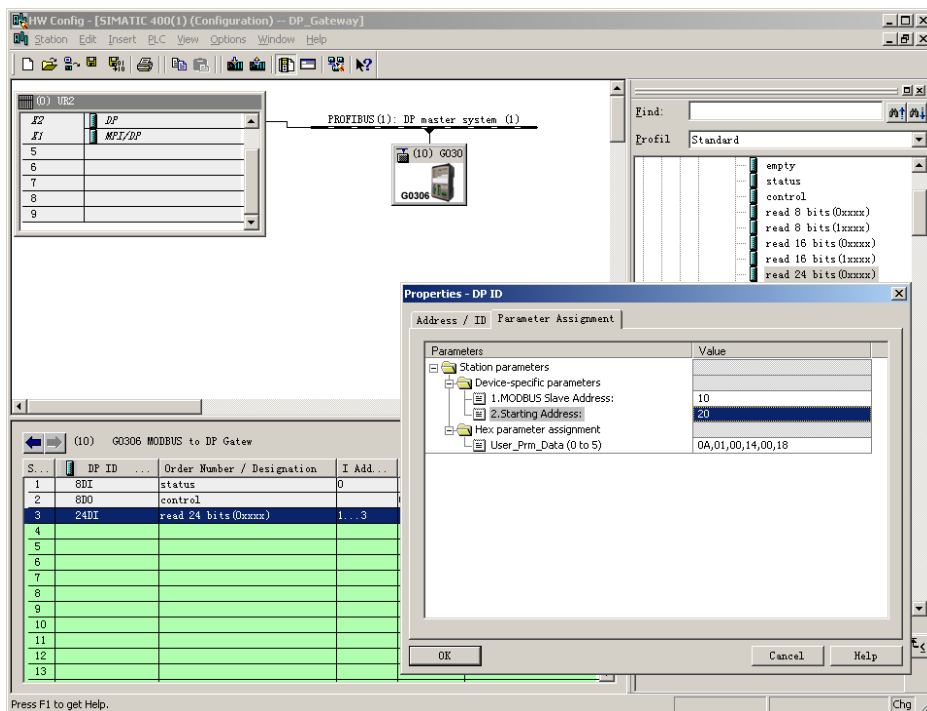


图 17 配置“read 24 bits(0xxxx)”模块用户参数

双击槽 3 中的“24 DI”或“read 24 bits(0xxxx)”或“1...3”；选择“Parameter Assigment”，完成从站地址 (MODBUS Slave Address) 和起始地址 (Starting Address) 的参数设定。

**从站地址:** 指该 Modbus 通信模块发送到 Modbus 从站的地址, 对应该 MODBUS 报文的第一个字节。

**起始地址:** 指要读取的 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。

“1. MODBUS Slave Address:” ⇒ 键入 MODBUS 从站地址 10, 如图 17。

“2. Starting Address:” ⇒ 键入欲读取的线圈 0xxxx 的起始地址 00021, 设置地址为 20 ⇒ “OK”, 如图 17。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 18 所示, 其中 IB1..IB3 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输入数据地址, 对应本 MODBUS 报文读到的 24 bits (0xxxx)。

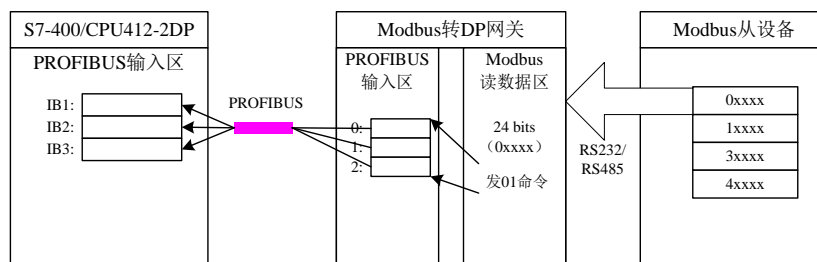


图 18 PROFIBUS 地址与 Modbus 地址对应关系

### ● 使用读 xxx 字模块举例 (模块 68-143)

这些模块可以使用功能码 3 (或 4) 来读取任意个字的寄存器数据。

以 “read 4 Words (3xxxx)” 模块为例, 此模块使用功能码 3 来读取 4 个字的寄存器数据。

#### a) 添加 “read 4 Words (3xxxx)” 模块, 如图 19 所示:

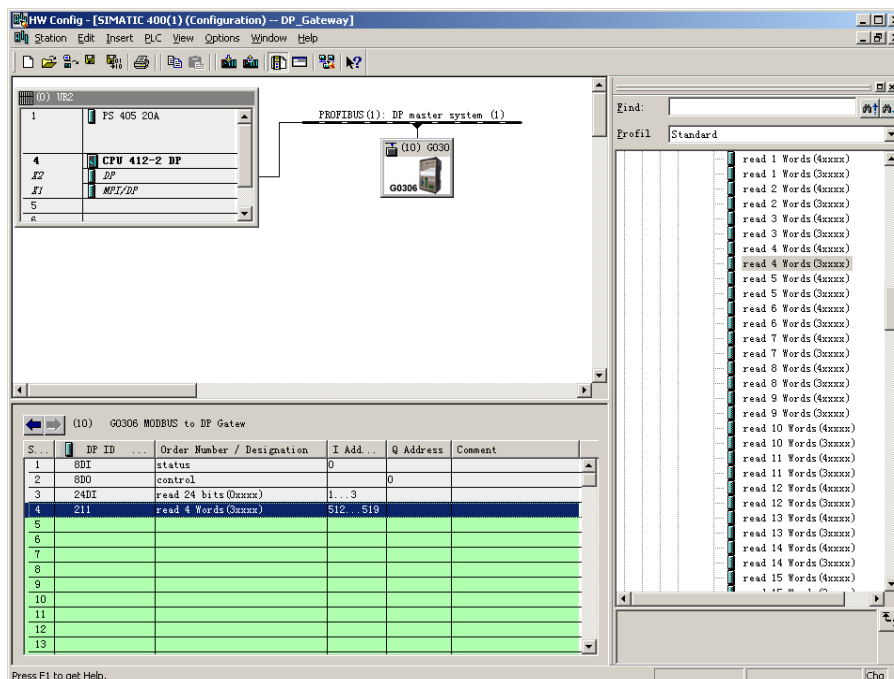


图 19 添加 “read 4 Words (3xxxx)” 模块

以将此模块放入槽 4 为例, 选中槽 4, 双击 “read 4 Words (3xxxx)” 模块。IB512...519 为 Profibus 主站为网关分配的输入数据地址, 对应于 Modbus 读取的 4 个字的寄存器 (3xxxx) 数据。

b) 配置“read 4 Words(3xxxx)”模块用户参数，如图 20 所示：

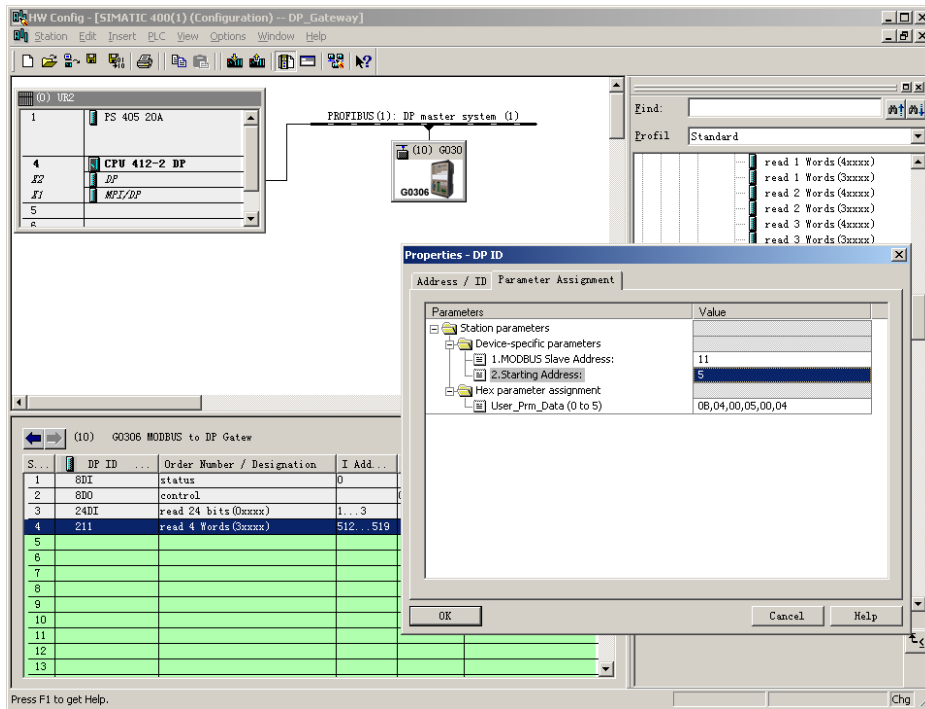


图 20 配置“read 4 Words(3xxxx)”模块用户参数

双击槽 4 中的“211”或“read 4 Words(3xxxx)”或“512...519”；选择“Parameter Assigement”，完成从站地址（MODBUS Slave Address）和起始地址（Starting Address）的参数设定。

**从站地址：**指该 Modbus 通信模块发送到 Modbus 从站的地址，对应该 MODBUS 报文的第一个字节。

**起始地址：**指要读取的 3xxxx 起始地址。注意：报文中寄存器起始地址 30000 对应设备中 30001 地址，其他顺延。

“1. MODBUS Slave Address:” ⇒ 键入 MODBUS 从站地址 11，如图 20。

“2. Starting Address:” ⇒ 键入欲读取寄存器 3xxxx 的起始地址 30006，设置地址为 5 ⇒ “OK”，如图 20。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 21 所示，其中 IB512... IB519 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输入数据地址，对应本 MODBUS 报文读到的 4 Words（3xxxx）。

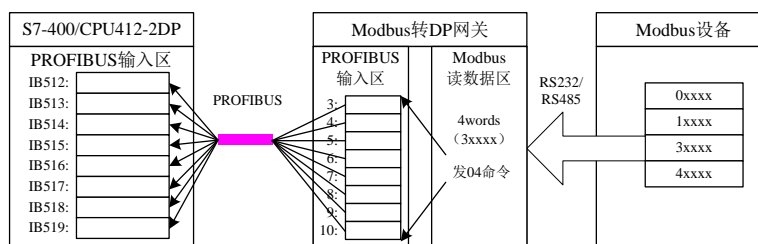


图 21 PROFIBUS 地址与 Modbus 地址对应关系

### ● 使用写 xxx 位模块举例（模块 144-175）

这些模块可以使用功能码 15 来往任意位数的线圈写入数据。

以“write 16 bits(0xxxx)”模块为例，此模块使用功能码 15 来往 16 位线圈写入数据。



a) 添加“write 16 bits(0xxxx)”模块，如图 22 所示：

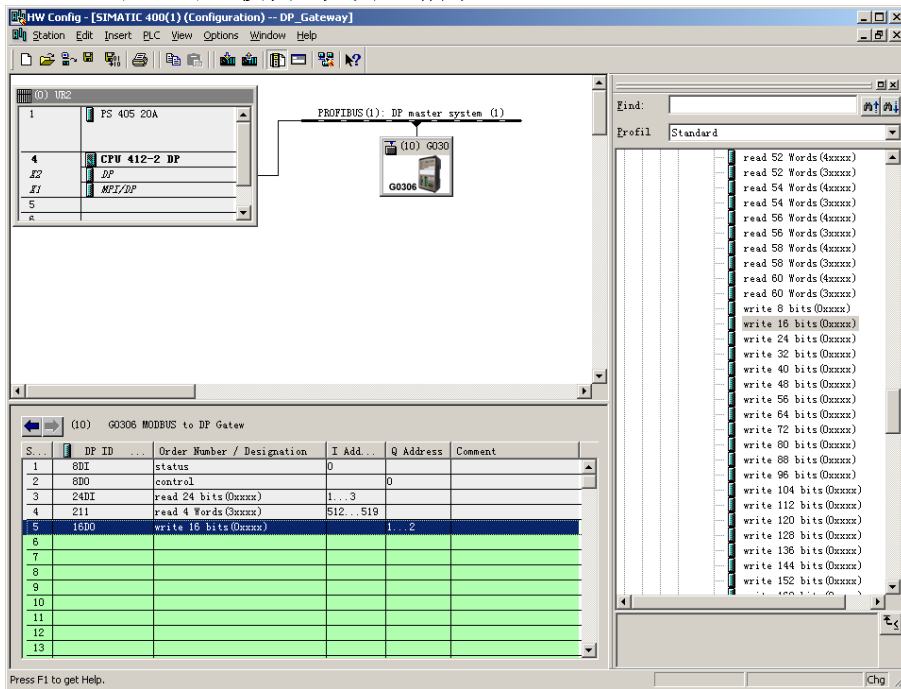


图 22 添加“write 16 bits(0xxxx)”模块

以将此模块放入槽 5 为例，选中槽 5，双击“write 16 bits(0xxxx)”模块。QB1...2 为 Profibus 主站为网关分配的输出数据地址，对应于 Modbus 写的 16 位(0xxxx)数据。

b) 配置“write 16 bits(0xxxx)”模块用户参数，如图 23 所示：

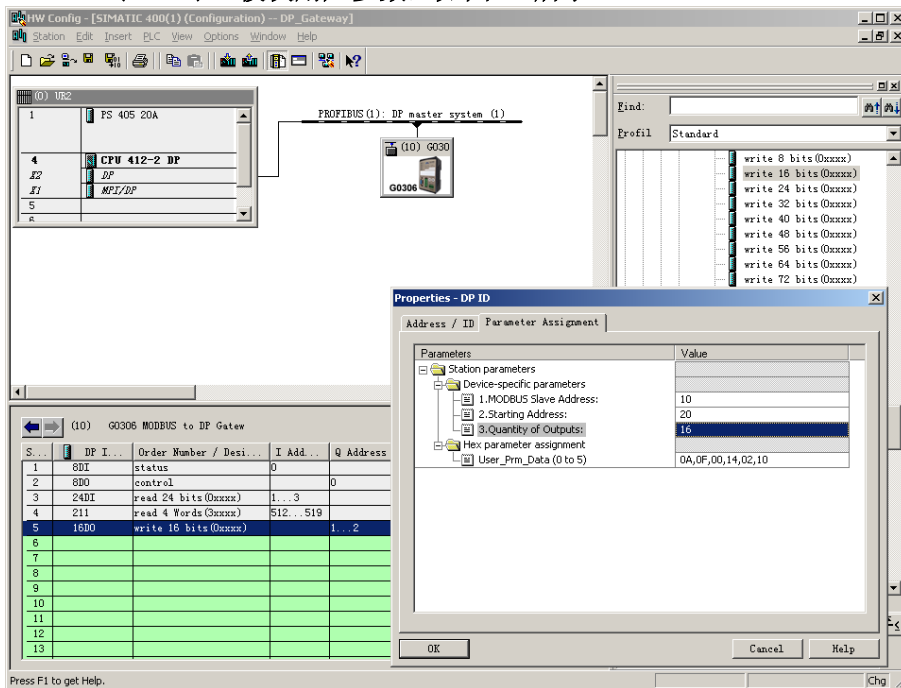


图 23 配置“write 16 bits(0xxxx)”模块用户参数

双击槽 5 中的“16DO”或“write 16 bits(0xxxx)”或“1...2”；选择“Parameter Assigement”，完成从站地址 (MODBUS Slave Address)、起始地址 (Starting Address) 及线圈数量 (Quantity of Outputs) 的参数设定。

**从站地址：**指该 Modbus 通信模块发送到 Modbus 从站的地址，对应该 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。

**线圈数量:** 指本 Modbus 报文要写入 0xxxx 中位的个数

“1. MODBUS Slave Address:” ⇒ 键入 Modbus 从站地址 10, 如图 23。

“2. Starting Address:” ⇒ 键入欲写入的线圈 0xxxx 的起始地址 00021, 设置地址为 20, 如图 23。

“3. Quantity of Outputs:” ⇒ 键入欲写入的线圈个数 16 ⇒ “OK”, 如图 23。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 24 所示, 其中 QB1、QB2 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输出地址, 共 2 字节, 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 QB1、QB2 中 2 字节 (16 位) 值写入 Modbus 设备的 0xxxx 数据区, 起始地址本例为 00020; 即将 PROFIBUS 的 QB1、QB2 写入 Modbus 设备的 00021~00036。

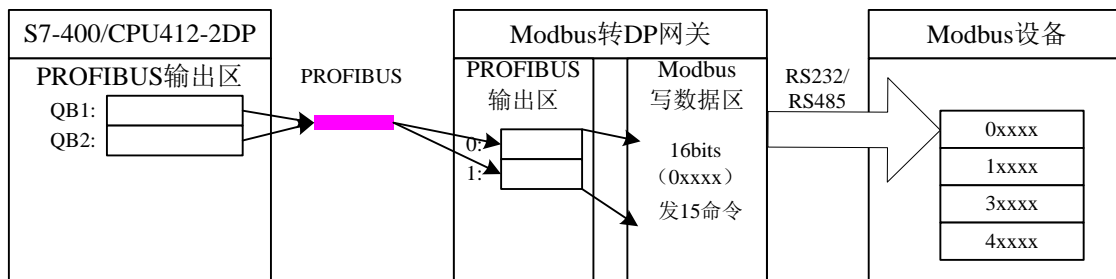


图 24 PROFIBUS 地址与 Modbus 地址对应关系

### ● 使用写 xxx 字模块举例 (模块 176-199)

这些模块可以使用功能码 16 来往任意寄存器写入数据。

以 “write 4 Words(4xxxx)” 模块为例, 此模块使用功能码 16 来往 4 个寄存器里写入数据。



a) 添加“write 4 Words(4xxxx)”模块，如图 25 所示：

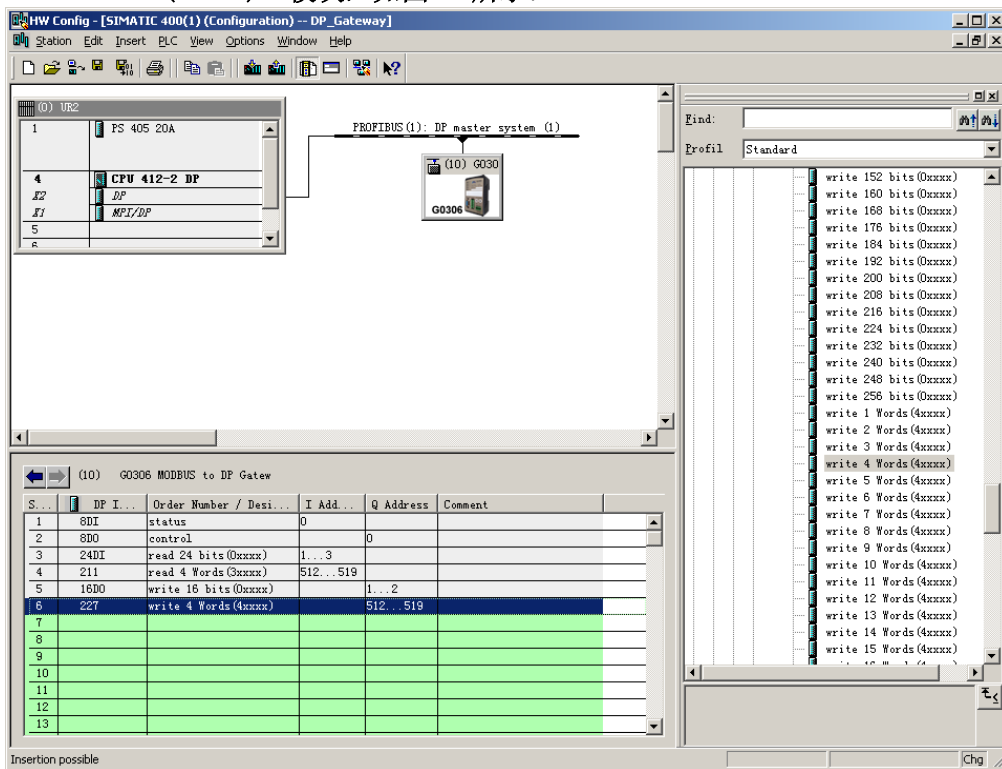


图 25 添加“write 16 bits(0xxxx)”模块

以将此模块放入槽 6 为例，选中槽 6，双击“write 4 Words(4xxxx)”模块。QB512...519 为 Profibus 主站为网关分配的输出数据地址，对应于 Modbus 写的 4 个字的寄存器(4xxxx)数据。

b) 配置“write 4 Words(4xxxx)”模块用户参数，如图 26 所示：

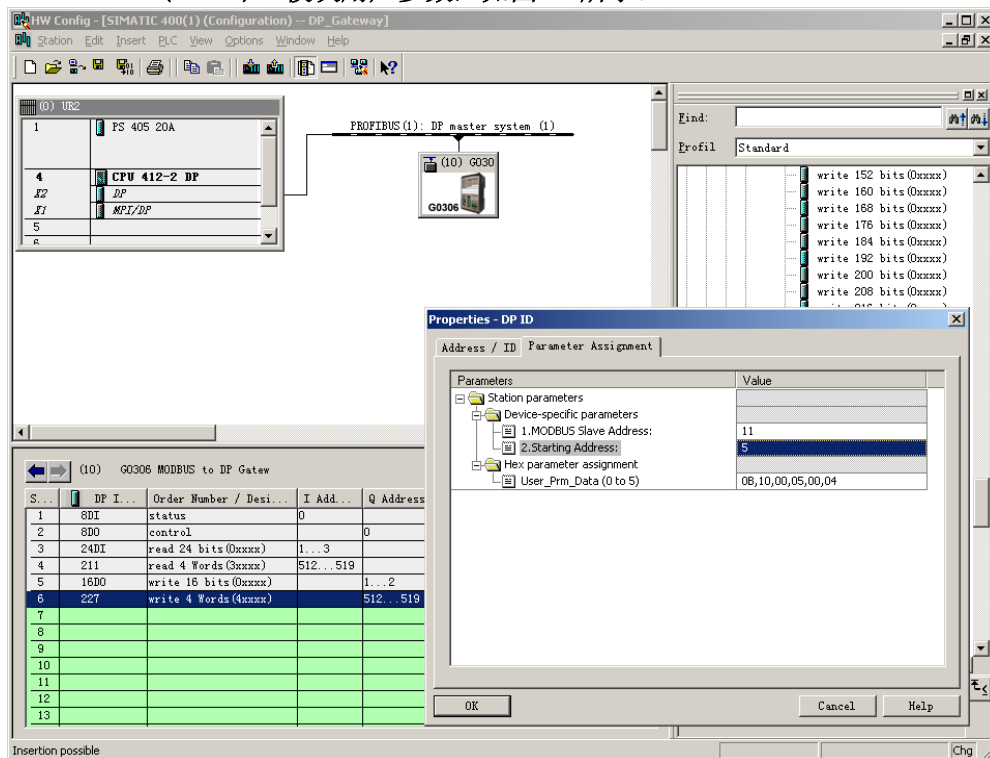


图 26 配置“write 4 Words(4xxxx)”模块用户参数

双击槽 6 中的“227”或“write 4 Words(4xxxx)”或“512...519”；选择“Parameter Assigment”，

完成从站地址 (MODBUS Slave Address) 和起始地址 (Starting Address) 的参数设定。

**从站地址:** 指该 Modbus 通信模块发送到 Modbus 从站的地址, 对应该 Modbus 报文的第一个字节。

**起始地址:** 指要写入的 4xxxx 起始地址。注意: 报文中寄存器起始地址 40000 对应设备中 40001 地址, 其他顺延。

“1. MODBUS Slave Address:” ⇒ 键入 Modbus 从站地址 11, 如图 26。

“2. Starting Address:” ⇒ 键入欲写入寄存器 0xxxx 的起始地址 00006, 设置地址为 5 ⇒ “OK”, 如图 26。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 27 所示, 其中 QB512..QB519 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输出数据地址共 8 字节, 对应本 Modbus 报文写到 Modbus 设备中的 4 Words (4xxxx)。

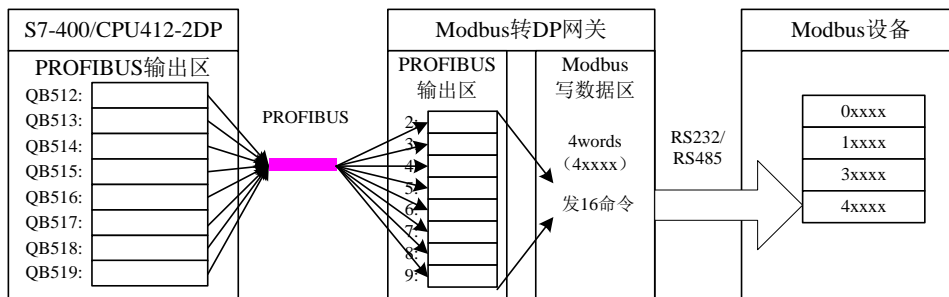


图 27 PROFIBUS 地址与 Modbus 地址对应关系

### ● 使用写单个线圈模块举例 (模块 200)

“force single bit (05H Command)” 模块使用功能码 5 来往某一线圈写入数据。

a) 添加 “force single bit (05H Command)” 模块, 如图 28 所示:

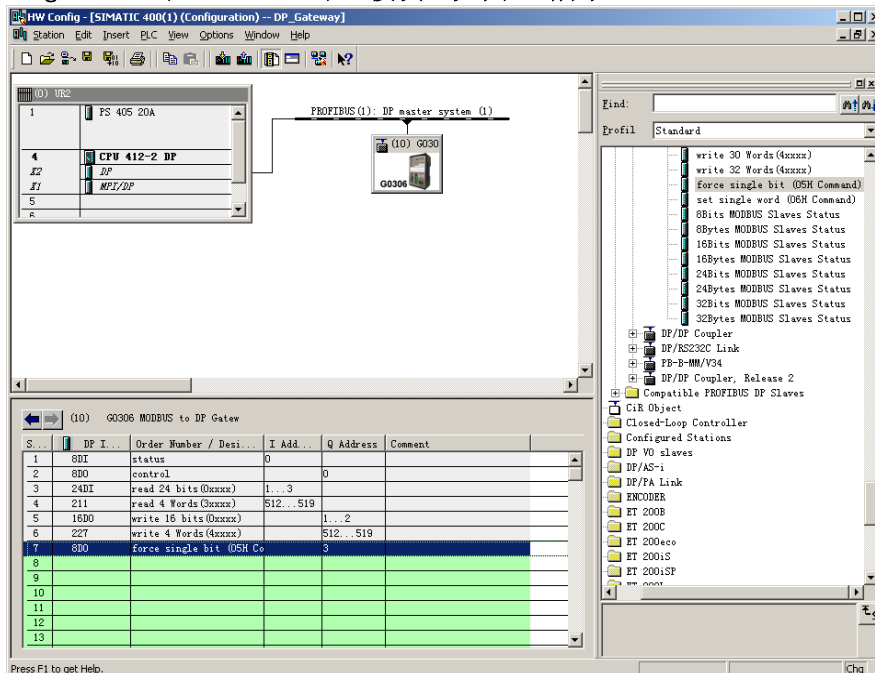


图 28 添加 “force single bit (05H Command)” 模块

以将此模块放入槽 7 为例, 选中槽 7, 双击 “force single bit (05H Command)” 模块。QB3 为 Profibus 主站为网关分配的输出数据地址, 对应于 Modbus 写的 1 位 (0xxxx) 数据。

b) 配置“force single bit (05H Command)”模块用户参数，如图 29 所示：

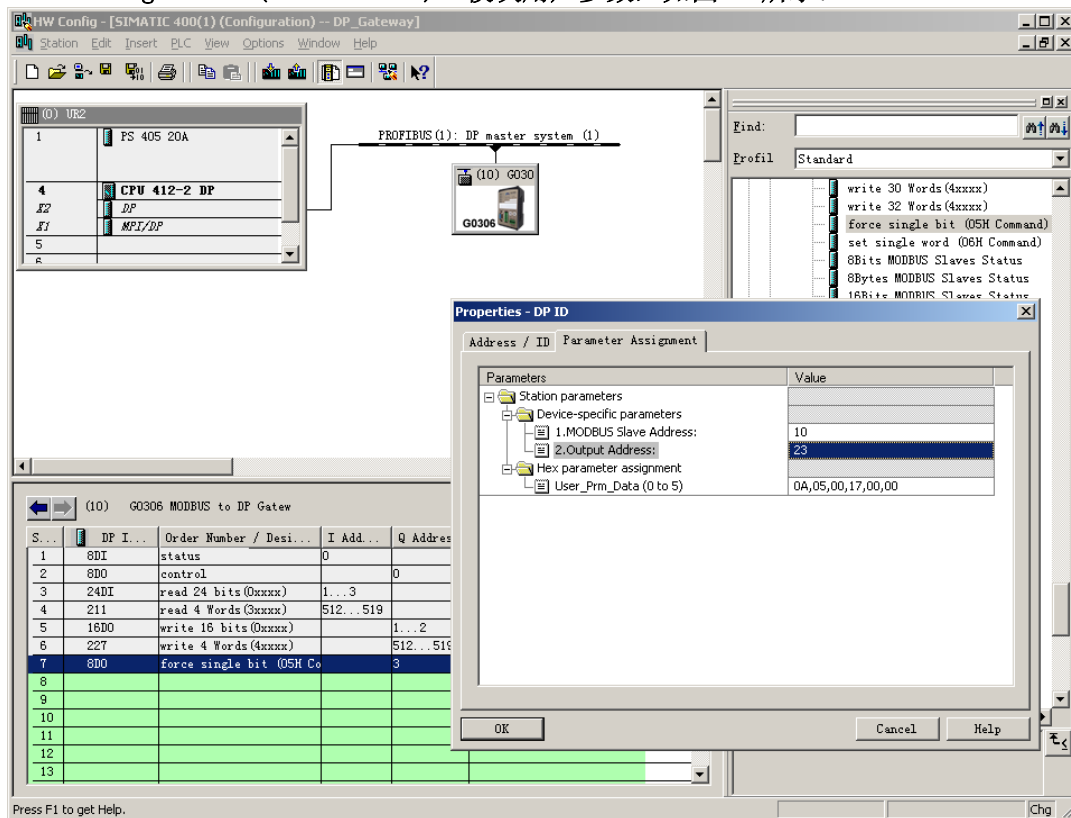


图 29 配置“force single bit (05H Command)”模块用户参数

双击槽 7 中的“8DO”或“force single bit (05H Command)”或“3”；选择“Parameter Assigement”，完成从站地址（MODBUS Slave Address）和输出地址（Output Address）的参数设定。

**从站地址：**指该 Modbus 通信模块发送到 Modbus 从站的地址，对应该 Modbus 报文的第一个字节。

**输出地址：**指要写入的 0xxxx 输出地址。注意：报文中线圈输出地址 00000 对应设备中 00001 地址，其他顺延。

“1. MODBUS Slave Address:” ⇒ 键入 Modbus 从站地址 10，如图 29。

“2. Output Address:” ⇒ 键入欲写入线圈 0xxxx 的输出地址 00024，设置地址为 23 ⇒ “OK”，如图 29。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 30 所示，其中 QB3 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输出数据地址共 1 字节，对应本 Modbus 报文写到 Modbus 设备中的单线圈 (0xxxx)。该 Modbus 模块根据 QB3 的值，发送 05 号 Modbus 命令，将 Modbus 设备的单线圈 0xxxx 置 1 或置 0。本例单线圈输出地址为 00023，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。

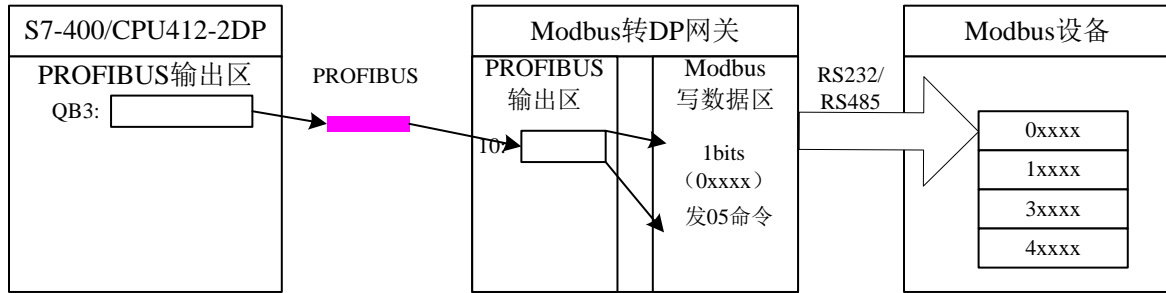


图 30 PROFIBUS 地址与 Modbus 地址对应关系

### ● 使用写单个寄存器模块举例（模块 201）

“set single word (06H Command)” 模块使用功能码 6 来往某一寄存器写入数据。

#### a) 添加“set single word (06H Command)” 模块，如图 31 所示：

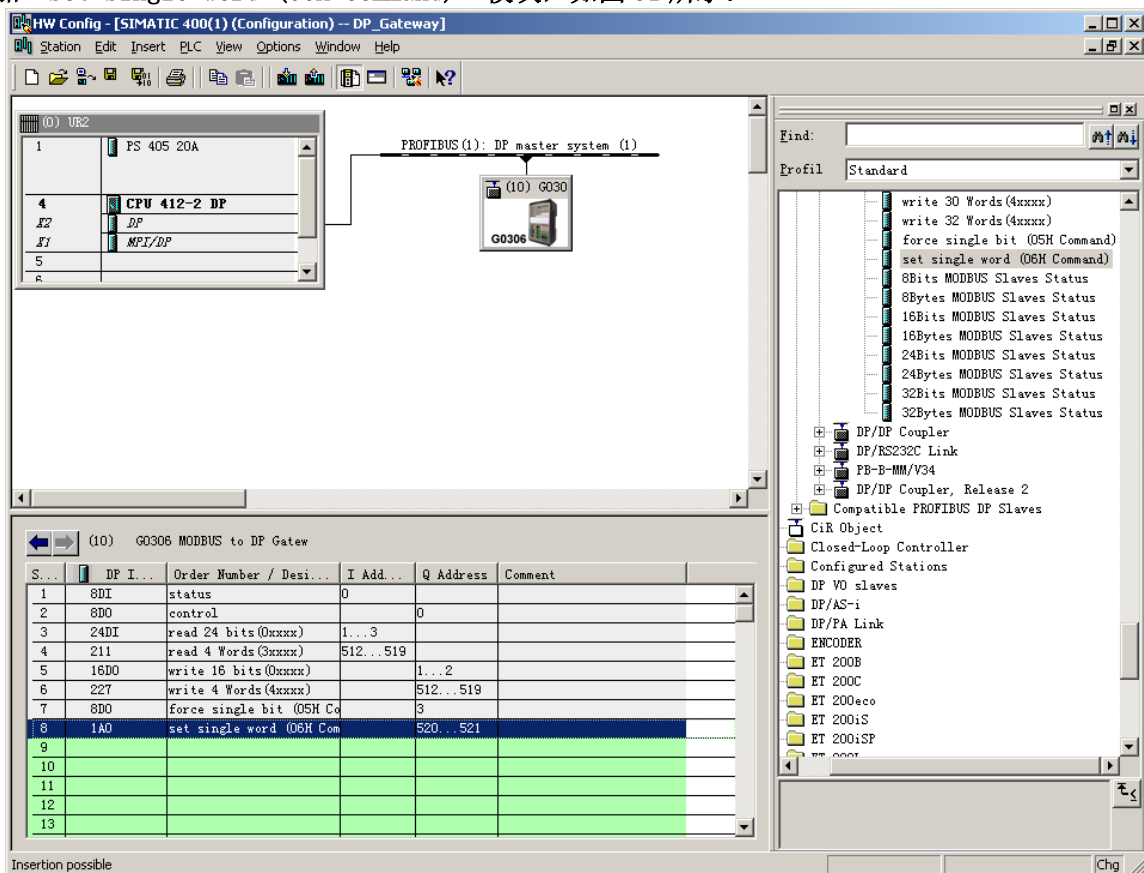


图 31 添加“set single word (06H Command)” 模块

以将此模块放入槽 8 为例，选中槽 8，双击“set single word (06H Command)” 模块。QB520...QB521 为 Profibus 主站为网关分配的输出数据地址，对应于 Modbus 写的 1 个字的寄存器(4xxxx)数据。

b) 配置“set single word (06H Command)”模块用户参数，如图 32 所示：

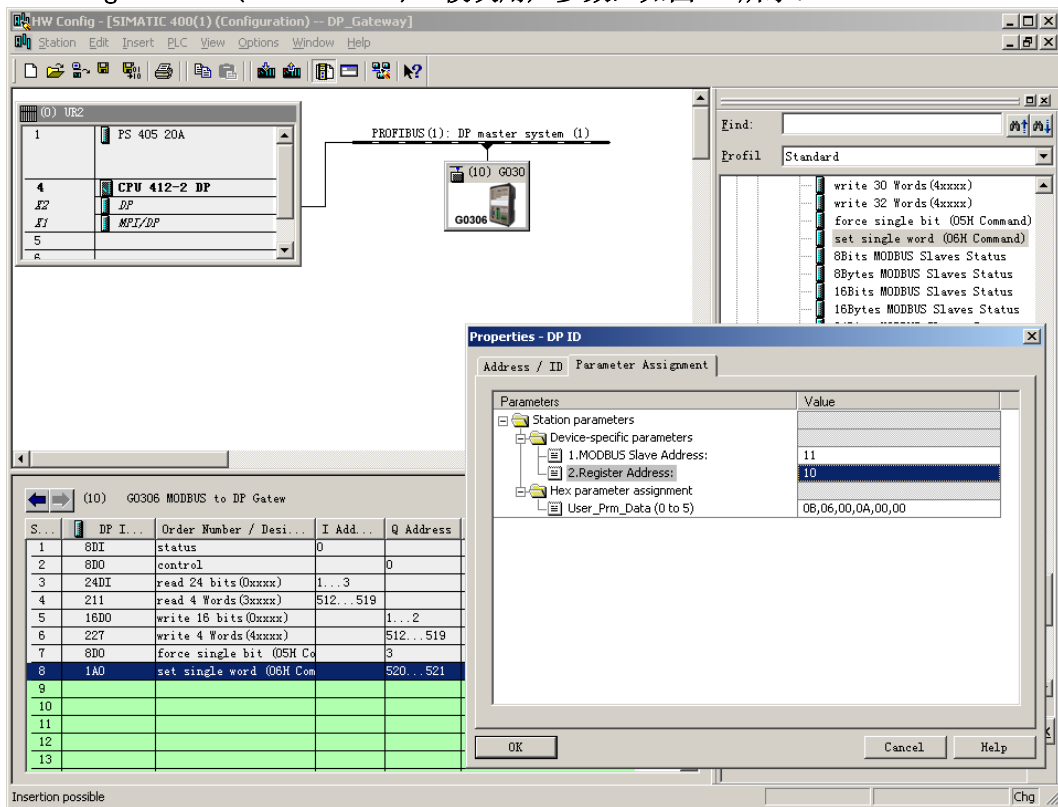


图 32 配置“set single word (06H Command)”模块用户参数

双击槽 8 中的“1AO”或“set single word (06H Command)”或“520...521”；选择“Parameter Assigement”，完成从站地址（MODBUS Slave Address）和输出地址（Register Address）的参数设定。

**从站地址：**指该 Modbus 通信模块发送到 Modbus 从站的地址，对应该 Modbus 报文的第一个字节。

**寄存器地址：**指要写入的 4xxxx 寄存器地址。注意：报文中线圈输出地址 40000 对应设备中 40001 地址，其他顺延。

“1. MODBUS Slave Address:” ⇒ 键入 Modbus 从站地址 11，如图 32。

“2. Register Address:” ⇒ 键入欲写入寄存器 4xxxx 的地址 40011，设置地址为 10 ⇒ “OK”，如图 32。

### c) PROFIBUS 地址与 Modbus 地址对应关系

如图 33 所示，其中 QB520...521 是 PROFIBUS 主站分配给这个 Modbus 模块的 PROFIBUS 输出数据地址共 2 字节，对应本 Modbus 报文写到 Modbus 设备中的 1 个字的寄存器 (4xxxx)。

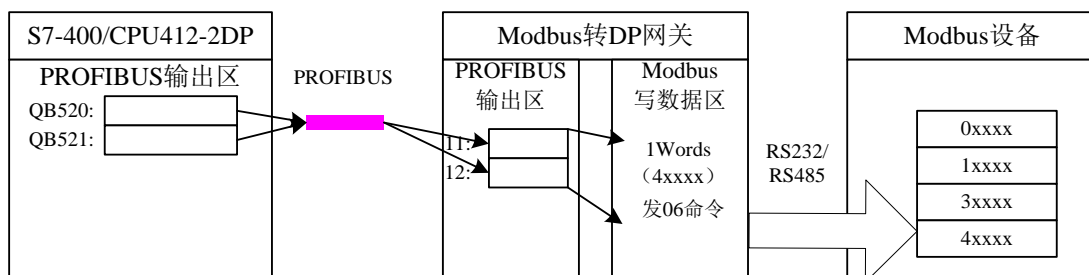


图 33 PROFIBUS 地址与 Modbus 地址对应关系

● 使用 xxx 位 Modbus 从站监测模块举例（模块 202、204、206、208）

a) 配置“3.MODBUS Slave Monitoring”设备用户参数，如图 34 所示：

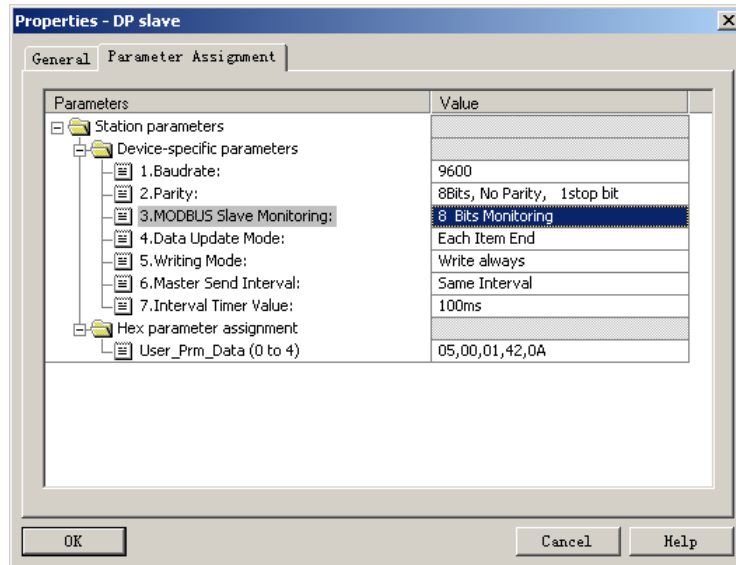


图 34 配置“3.MODBUS Slave Monitoring”设备用户参数

如图 34 所示，想要使用 xxx 位 Modbus 从站监测模块，则必须在设备用户参数中配置相对应的 Modbus 从站监测参数。本例配置“8 Bits Monitoring”，则对应应使用“8Bits MODBUS Slaves Status”模块。

b) 添加“8Bits MODBUS Slaves Status”模块，如图 35 所示：

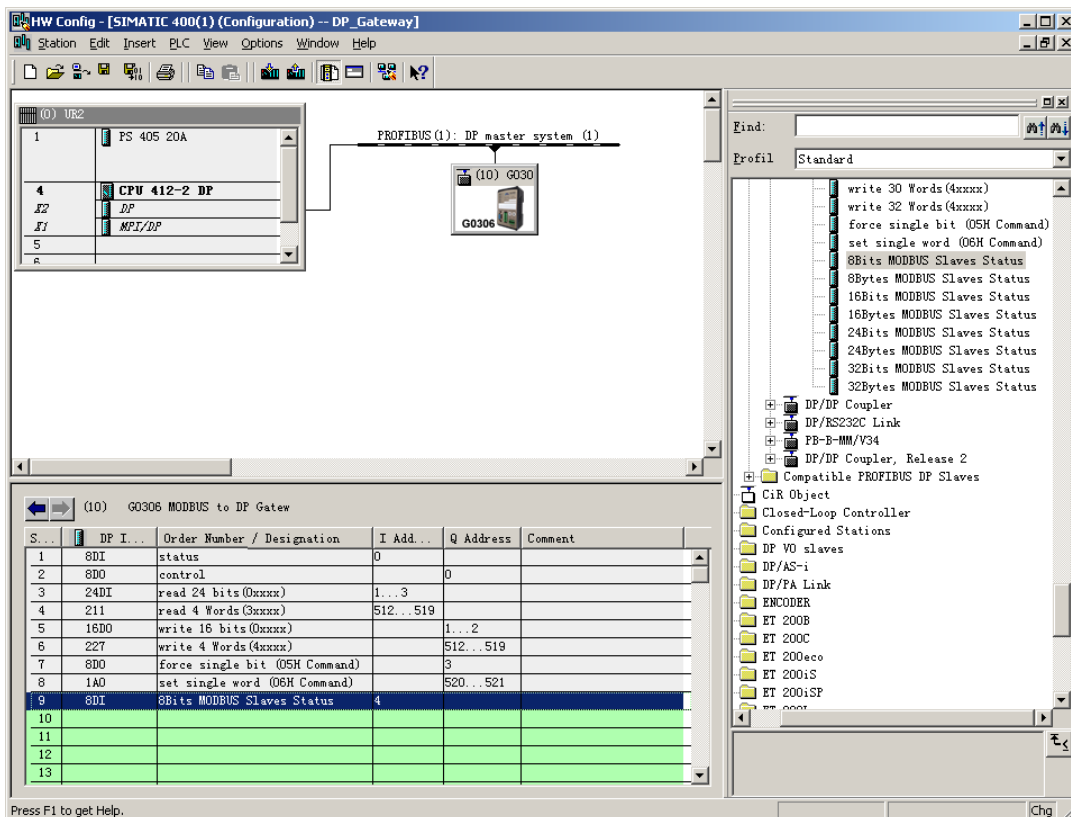


图 35 添加“8Bits MODBUS Slaves Status”模块

前文已描述过，此类模块必须放在所有 Modbus 通信模块之后，所以根据之前的例子槽 1-8 已有相应的模块，则“8Bits MODBUS Slaves Status”模块将填入到槽 9 中。选中槽 9，双击“8Bits MODBUS Slaves

Status” 模块。IB4 为 Profibus 主站为网关分配的输入数据地址共 1 个字节，每一位都对应于要监测的 Modbus 设备状态。

c) 配置“8Bits MODBUS Slaves Status” 模块用户参数，如图 36 所示：

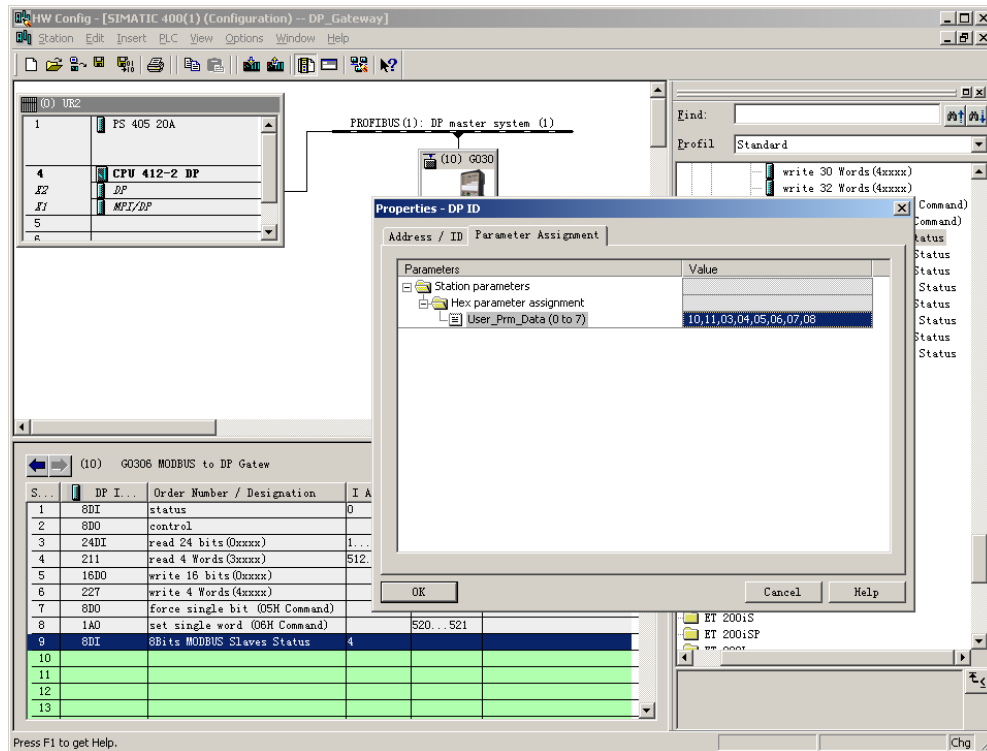


图 36 配置要监测的从站地址

如图 36 所示，每个设备对应于一个字节的模块用户参数。前例中，一共配置了两个从站 10、11，所以将这两个地址填入到模块用户参数中。

程序运行后，可在 PROFIBUS 地址 IB4 中，监测从站 10, 11 的状态，如下表所示：

表 18 IB4 中监测的 Modbus 从站状态

B7	B6	B5	B4	B3	B2	B1	B0
本例未使用	本例未使用	本例未使用	本例未使用	本例未使用	本例未使用	地址 11 通信状态	地址 10 通信状态
--	--	--	--	--	--	0: 有应答	0: 有应答
--	--	--	--	--	--	1: 无应答	1: 无应答

B0=0，表示网关根据当前配置，往地址为 10 的 Modbus 从站发送命令，网关能收到从站发送的正确响应报文。

B0=1，表示网关根据当前配置，往地址为 10 的 Modbus 从站发送命令，但从站超时没有响应或根本没连接地址为 10 的从站。

其他位的含义类似，只是监测的从站地址不同。

**注意：**如果从站数量小于检测数量，那么从站地址配置顺序为从低位到高位且配置的从站数量必须跟实际从站数量相同（例如在本例中有 2 个从站，但配置的模块可以监视 8 个从站，那么这两个从站的地址仅能配置在 B0 和 B1。地址顺序可以颠倒，例如 B1 监视地址 10，B0 监视地址 11）。

● 使用 xxx 字节 Modbus 从站监测模块举例（模块 203、205、207、209）

a) 配置“3.MODBUS Slave Monitoring”设备用户参数，如图 37 所示：

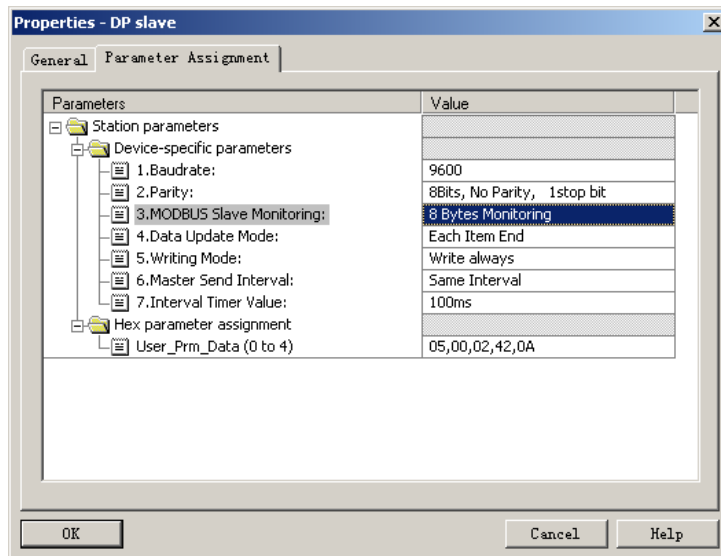


图 37 配置“3.MODBUS Slave Monitoring”设备用户参数

如图 37 所示，想要使用 xxx 字节 Modbus 从站监测模块，则必须在设备用户参数中配置相对应的 Modbus 从站监测参数。此例是基于前 6 个例子，将设备用户参数配置“8 Bytes Monitoring”，则对应应使用“8Bytes MODBUS Slaves Status”模块。

b) 添加“8Bytes MODBUS Slaves Status”模块，如图 38 所示：

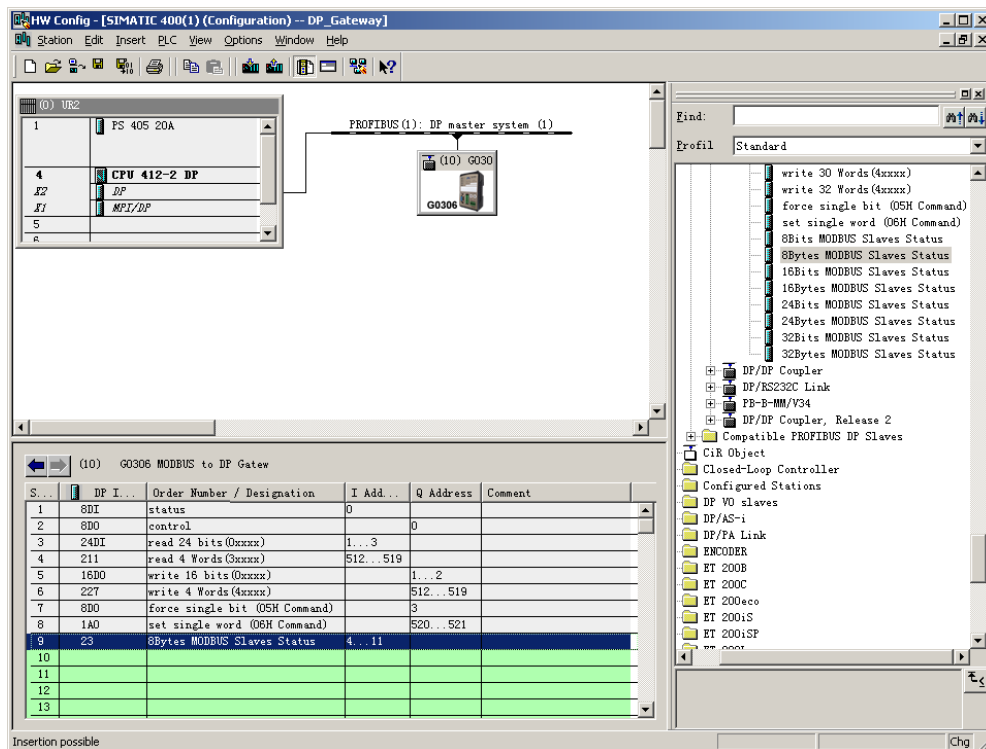


图 38 添加“8Bytes MODBUS Slaves Status”模块

前文已描述过，此类模块必须放在所有 Modbus 通信模块之后，所以根据之前的例子槽 1-8 已有相应的模块，则“8Bytes MODBUS Slaves Status”模块将填入到槽 9 中。选中槽 9，双击“8Bytes MODBUS Slaves



Status”模块。IB4...11 为 Profibus 主站为网关分配的输入数据地址共 8 个字节，每个字节都对应于要监测的 Modbus 设备状态。

c) 配置“8Bytes MODBUS Slaves Status”模块用户参数，如图 39 所示：

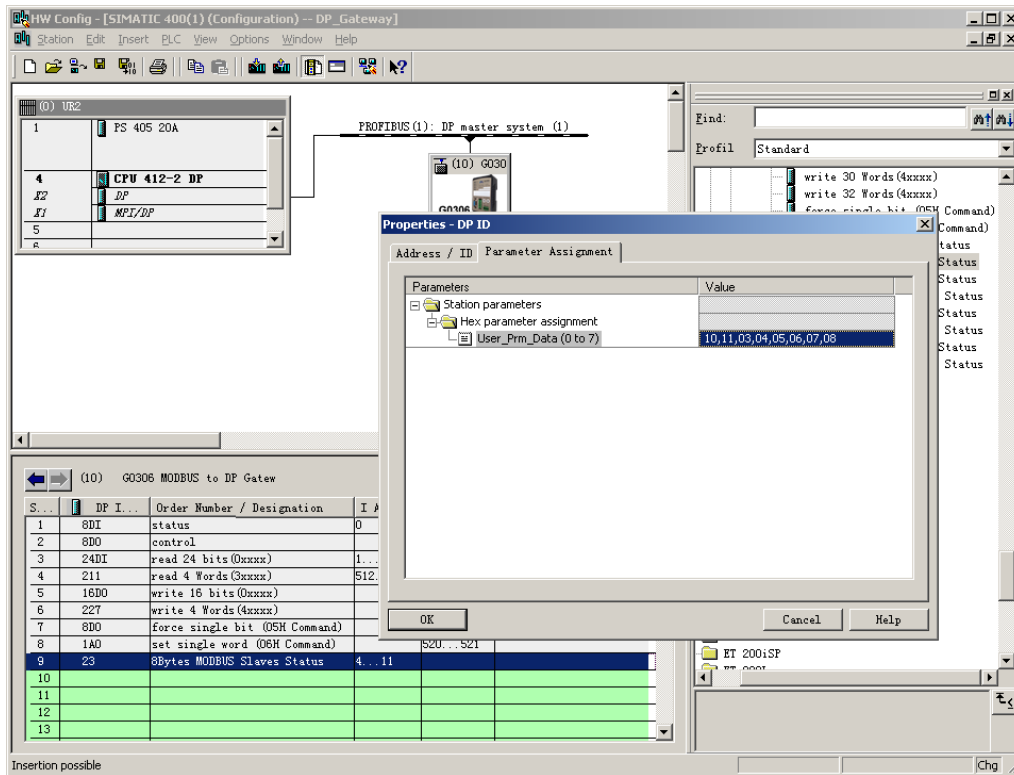


图 39 配置要监测的从站地址

如图 39 所示，每个设备对应于一个字节的模块用户参数。前例中，一共配置了两个从站 10、11，所以将这两个地址填入到模块用户参数中。

程序运行后，可在 PROFIBUS 地址 IB4...11 中，监测 8 个从站状态，由于本例仅有两个从站，则 IB4 为从站 10 的状态，IB5 为从站 11 的状态。

表 19 某一从站可被检测状态表

B7: 奇偶校验	B6: CRC 校验	B5: 保留	B4-B1: 异常响应码	B0: 响应超时
0: 当前从站奇偶校验正确	0: 当前从站 CRC 正确		详细见附录 A. 3	0: 当前从站响应未超时
1: 当前从站奇偶校验错误	1: 当前从站 CRC 错误			1: 当前从站响应超时

这部分不同于总状态模块，每个字节固定表示一个从站，可详细检测每一个从站的状态。

**注意：**如果从站数量小于检测数量，那么从站地址配置顺序为从低字节到高字节且配置从站数量必须跟实际从站数量相同（例如在本例中有 2 个从站，但配置的模块可以监视 8 个从站，那么这两个从站的地址仅能配置在前两个字节。地址顺序可以颠倒，例如 IB5 监视地址 10，IB4 监视地址 11）。

## (2) 如何使用 G0306-SS 的 GSD 文件

### ● 配置设备用户参数

在如图 13 界面，在网关设备上点右键，选择对象属性→参数分配。

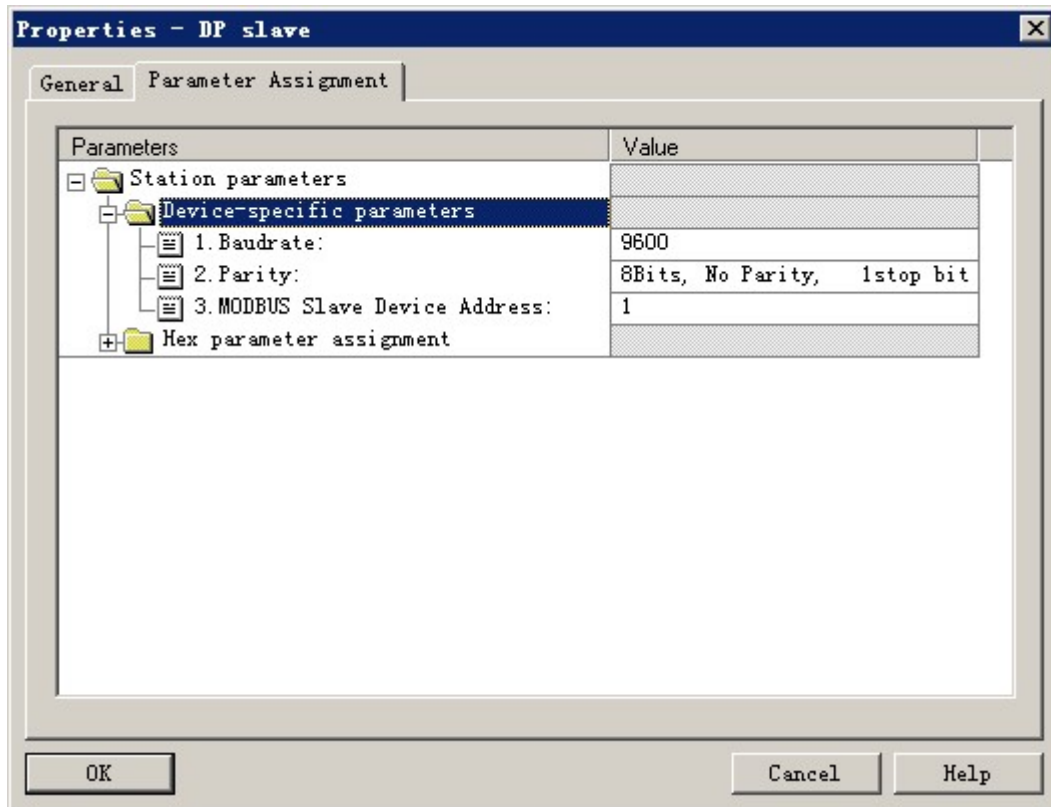


图 40 G0306-SS 设备用户参数配置界面

在这里可以修改表 14 中提到的所有参数。用户要根据实际情况进行修改。可配置网关作为 Modbus 从站的波特率、校验、以及 Modbus 从站地址等。

### ● 配置网关模块简介

在 4.3.1 章 (2) 中已经介绍过，本网关 GSD 中包含 20 个槽，67 个模块，最多支持 237 个用户参数，每个模块选项的具体含义见表 13。

其中，槽 1 固定为总状态模块（模块 2），槽 2 固定为控制模块（模块 3），其余 20 个槽可根据需求任意配置。

以配置“Input:24 bits(0xxxx)”模块（模块 6）放入槽 3 举例，选中槽 3，在右侧设备列表中，双击“Input:24 bits(0xxxx)”模块即可将该模块添加到槽 3 中。

本网关根据用户实际配置的模块顺序，形成 Modbus 存储区。往下将详细介绍各个模块如何使用。

### ● 总状态模块（模块 2）

此模块实时显示网关报文发送接收状态以及检测接收的报文是否存在异常。异常不会自动消除，直至清除错误标记为止。清错误标记方法见控制模块（模块 3）。

B7: 奇偶校验	B6: CRC 校验	B5: 保留	B4-B1: 异常响应码	B0: 发送/接收
0: 当前从站奇偶校验正确	0: 当前主站 CRC 正确	不用	详细见附录 A.3	0: 发送报文或等待接收
1: 当前从站奇偶校验错误	1: 当前主站 CRC 错误	不用		1: 接收或处理报文

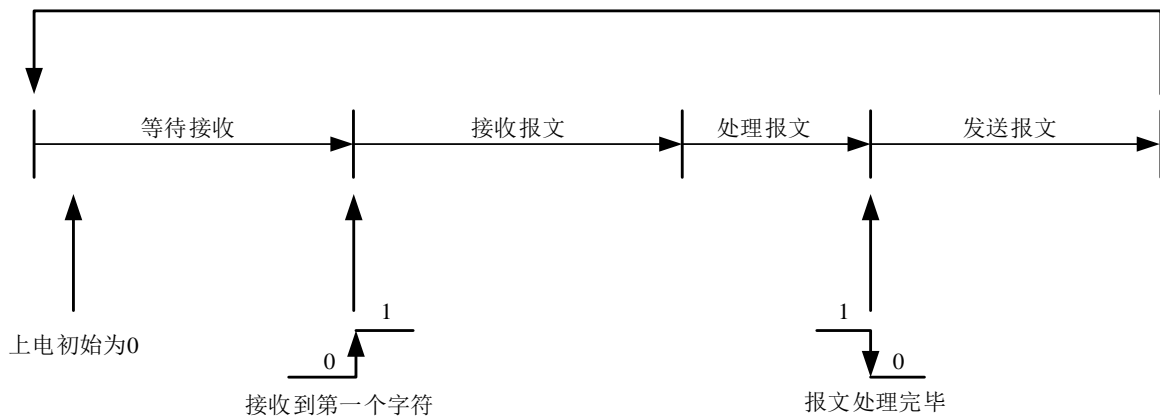
**a) B0:发送/接收**


图 41 发送接收状态转换图

由于 G0306-SS 是从站，所以，网关上电后自动进入等待接收状态。

**b) B4-B1:异常响应码**

当网关接收到主站发送的报文后，没有传输错误，但网关无法正确执行主站命令或无法作出正确应答，网关将以“异常响应码”回答。详细见附录 A. 3。

**c) B6:CRC 校验**

当网关接收到主站发送的报文有 CRC 校验出现错误时，将此位置 1。此时，网关认为此报文数据不可靠、不执行命令，不响应报文。

**d) B7:奇偶校验**

当网关接收数据发现字符奇偶校验错误时，将此位置 1。此时，网关认为 MODBUS 响应数据不可靠，不执行命令，不响应报文。

**● 控制模块（模块 3）**

此模块主要用作控制 Profibus 输出以及清除错误标记。

表 20 控制模块格式

B7:清除错误标记	B6-B1:保留	B0:Profibus 输出使能
0:无清除操作	——	0:禁止 Profibus 输出数据进入 Modbus 1xxxx 和 3xxxx
1:清除错误标记 B7~B1	——	1:使能 Profibus 输出数据进入 Modbus 1xxxx 和 3xxxx

**a) B0: Profibus 输出使能**

控制 Profibus 输出数据是否进入 Modbus 的 1xxxx 和 3xxxx 存储区。初始存储区数据均为 0。

**b) B7:清除错误标记**

该位置 1，则清除总状态模块中的 B7-B1 位。当该位置 0 后，才重新检测是否收到异常报文。

**● 使用输入 xxx 位模块举例（模块 4-19）**

使用这些模块可以将 Modbus 存储区 0xxxx 的数据对应到 Profibus 输入区 Ix.y。用户可使用功能码 1、5、15 对 Modbus 存储区 0xxxx 进行操作。

以“Input:32 bits(0xxxx)”模块为例，此模块将 Modbus 存储区 0xxxx 的 32 个线圈对应到 Profibus

输入区中。

a) 添加“Input:32 bits(0xxxx)”模块，如图 42 所示：

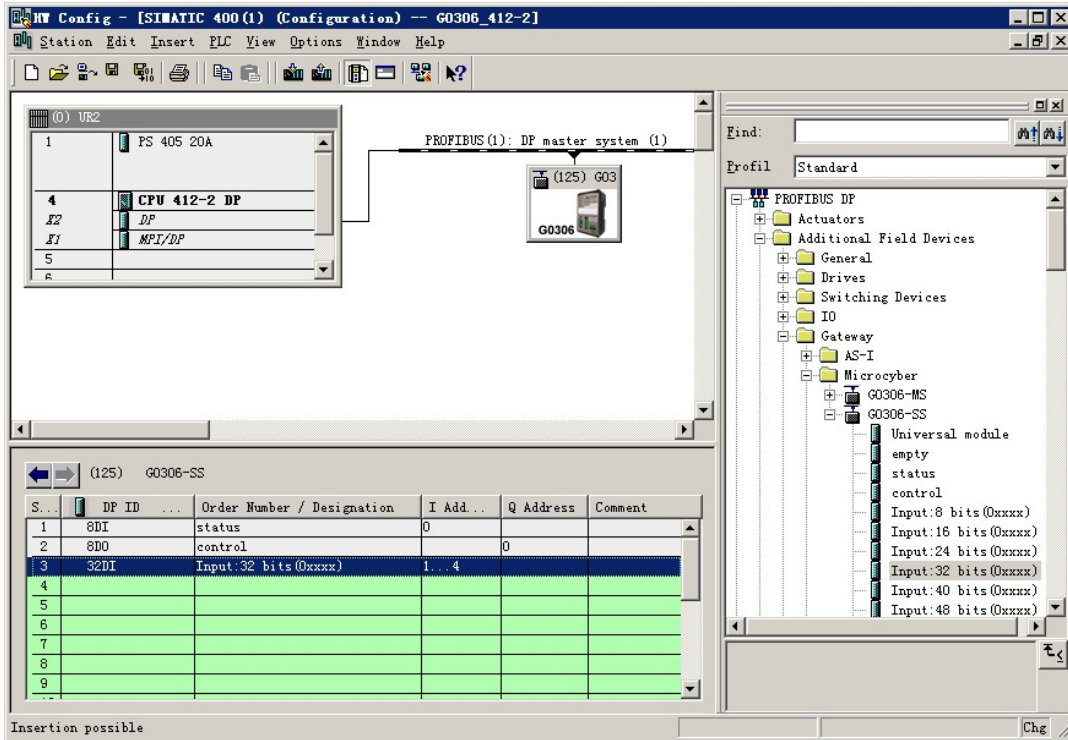


图 42 添加“Input:32 bits(0xxxx)”模块

以将此模块放入槽 3 为例，选中槽 3，双击“Input:32 bits(0xxxx)”模块。IB1-IB4 为 Profibus 主站为网关分配的输入数据地址，对应于 Modbus 线圈 00001-00032。

b) Modbus 存储区 0xxxx 与 Profibus 输入区的对应关系

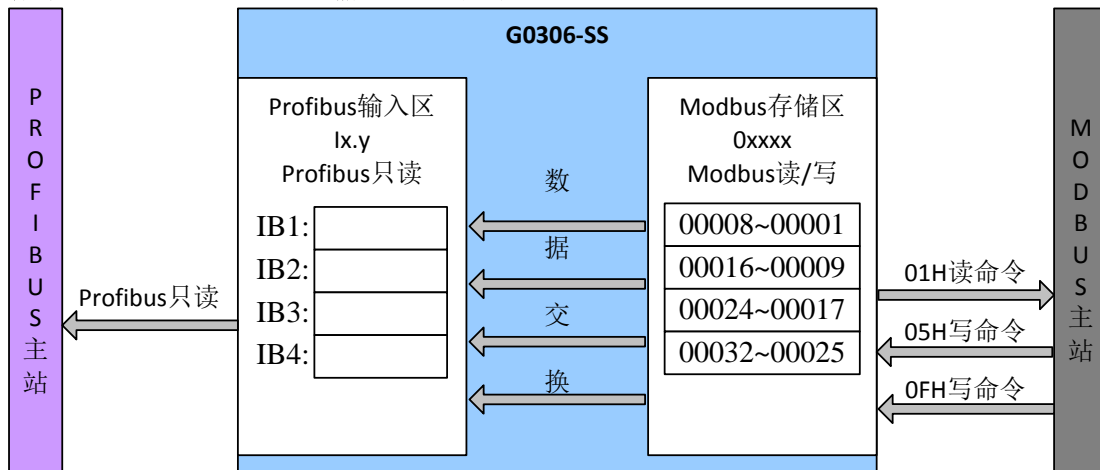


图 43 Modbus 存储区 0xxxx 与 Profibus 输入区的对应关系

**注意：**IB0 对应的是总状态模块。Modbus 一侧线圈地址一定是从 00001 开始的。当再插入一个输入 xxx 位模块时，Modbus 线圈地址顺序连续分配。例如：再插入一个“Input:32 bits(0xxxx)”模块，则地址顺序连续分配为 00033-00064，对应于 Profibus 的 IB5-IB8。

#### ● 使用输出 xxx 位模块举例（模块 36-51）

使用这些模块可以将 Profibus 输出区 Qx.y 的数据对应到 Modbus 存储区 1xxxx。用户可使用功能码 2 对 Modbus 存储区 1xxxx 进行操作。

以“Output:32 bits(1xxxx)”模块为例，此模块将Profibus输出区4个字节数据写到Modbus存储区1xxxx的32个线圈中。

a) 添加“Output:32 bits(1xxxx)”模块，如图44所示：

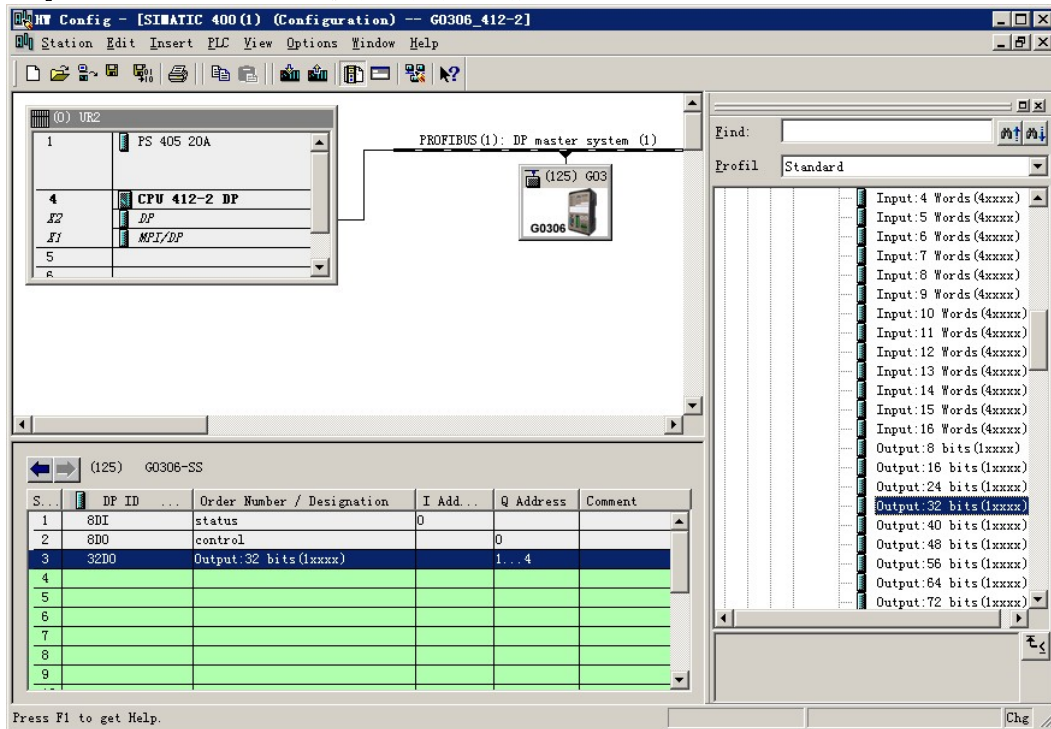


图44 添加“Output:32 bits(1xxxx)”模块

以将此模块放入槽3为例，选中槽3，双击“Output:32 bits(1xxxx)”模块。QB1-QB4为Profibus主站为网关分配的输出数据地址，对应于Modbus线圈10001-10032。

b) Profibus输出区与Modbus存储区1xxxx的对应关系

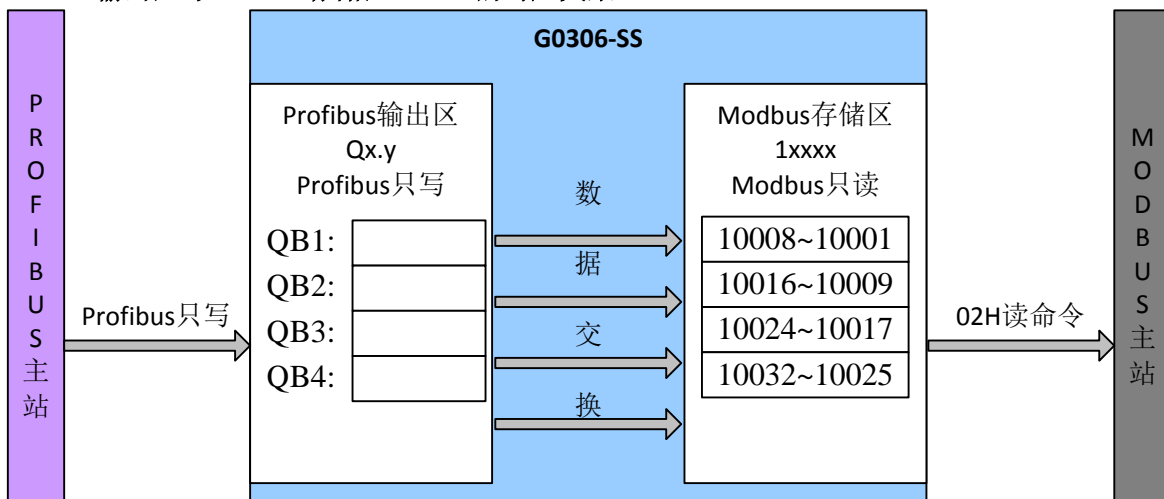


图45 Profibus输出区与Modbus存储区1xxxx的对应关系

**注意：**QB0对应的是控制模块。Modbus一侧线圈地址一定是从10001开始的。当再插入一个输出xxx位模块时，Modbus线圈地址顺序连续分配。例如：再插入一个“Output:32 bits(1xxxx)”模块，则地址顺序连续分配为10033-10064，对应于Profibus的QB5-QB8。

### ● 使用输入 xxx 字节模块举例（模块 20-35）

使用这些模块可以将 Modbus 存储区 4xxxx 的数据对应到 Profibus 输入区 IWx.y。用户可使用功能码 3、6、16 对 Modbus 存储区 4xxxx 进行操作。

以“Input:4 Words(4xxxx)”模块为例，此模块将 Modbus 存储区 4xxxx 的 4 个寄存器对应到 Profibus 输入区中。

#### a) 添加“Input:4 Words(4xxxx)”模块，如图 46 所示：

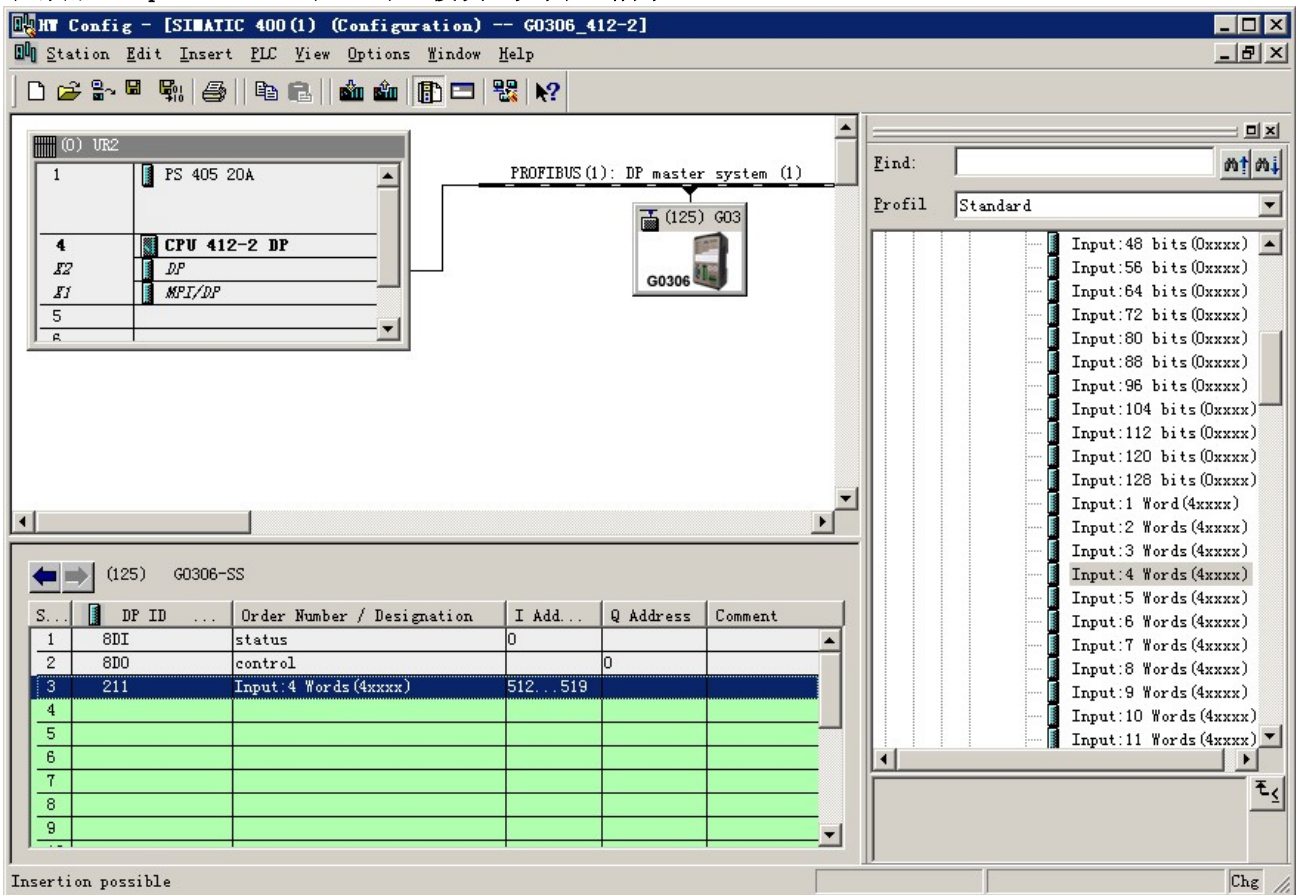


图 46 添加“Input:4 Words(4xxxx)”模块

以将此模块放入槽 3 为例，选中槽 3，双击“Input:4 Words(4xxxx)”模块。IW512- IW519 为 Profibus 主站为网关分配的输入数据地址，对应于 Modbus 寄存器 40001-40004。

## b) Modbus 存储区 4xxxx 与 Profibus 输入区的对应关系

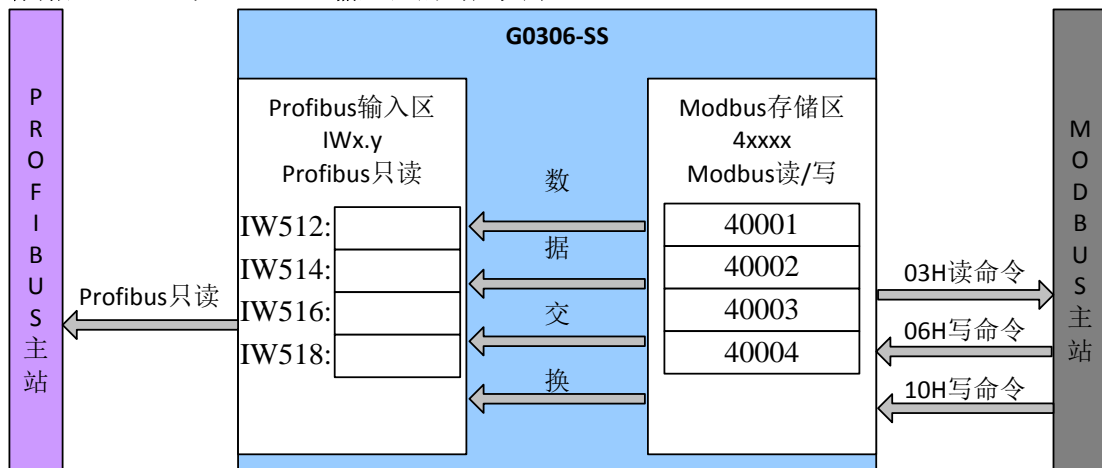


图 47 Modbus 存储区 4xxxx 与 Profibus 输入区的对应关系

**注意：**Modbus 一侧寄存器地址一定是从 40001 开始的。当再插入一个输入 xxx 字节模块时，Modbus 寄存器地址顺序连续分配。例如：再插入一个“Input:4 Words(4xxxx)”模块，则地址顺序连续分配为 40005-40008，对应于 Profibus 的 IW520-IW527。

## ● 使用输出 xxx 字节模块举例（模块 52-67）

使用这些模块可以将 Profibus 输出区 QWx.y 的数据对应到 Modbus 存储区 3xxxx。用户可使用功能码 4 对 Modbus 存储区 3xxxx 进行操作。

以“Output:4 Words(3xxxx)”模块为例，此模块将 Profibus 输出区 8 个字节数据写到 Modbus 存储区 3xxxx 的 4 个寄存器中。

## a) 添加“Output:4 Words(3xxxx)”模块，如图 48 所示：

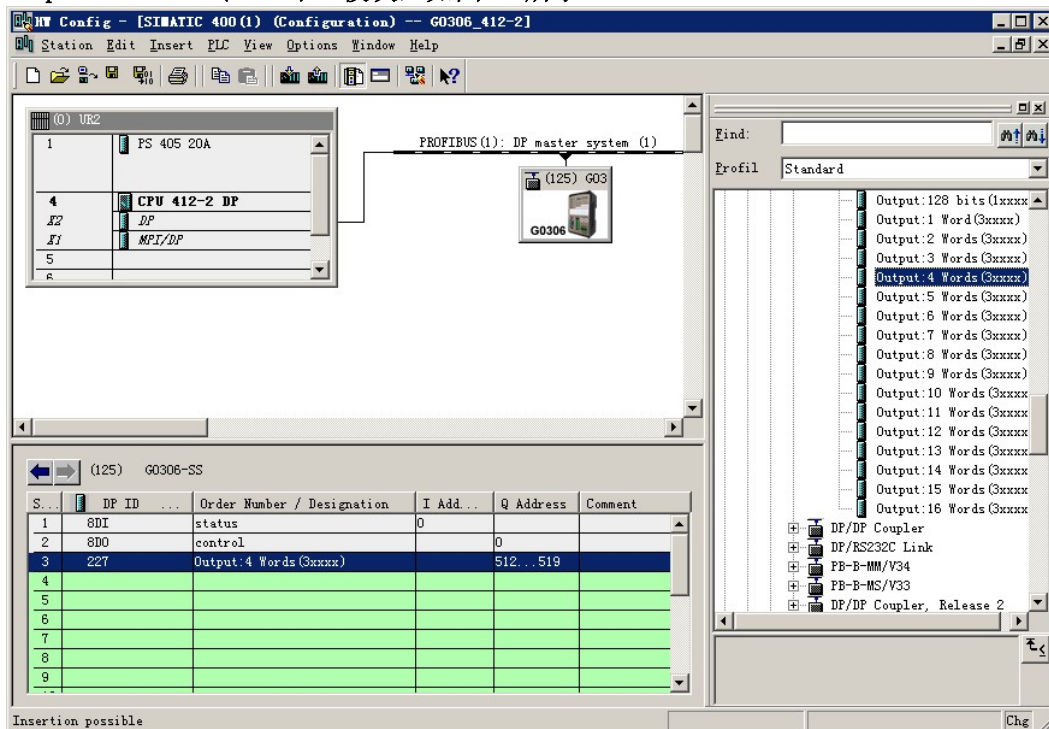


图 48 添加“Output:4 Words(3xxxx)”模块

以将此模块放入槽 3 为例，选中槽 3，双击“Output:4 Words(3xxxx)”模块。QW512-QW519 为 Profibus

主站为网关分配的输出数据地址，对应于 Modbus 寄存器 30001-30004。

#### b) Profibus 输出区与 Modbus 存储区 3xxxx 的对应关系

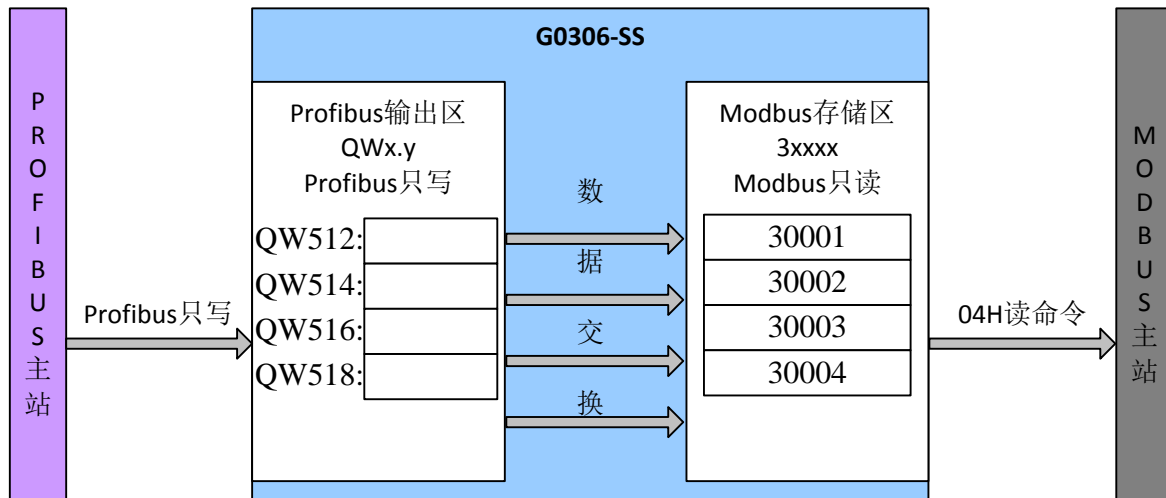


图 49 Profibus 输出区与 Modbus 存储区 3xxxx 的对应关系

**注意：**Modbus 一侧寄存器地址一定是从 30001 开始的。当再插入一个输出 xxx 字节模块时，Modbus 寄存器地址顺序连续分配。例如：再插入一个“Output:4 Words (3xxxx)”模块，则地址顺序连续分配为 30005-30008，对应于 Profibus 的 QW520-QW527。

#### 4.3.4 使用注意事项

使用 G0306 Modbus 转 DP 网关时，有如下几点容易出错的地方，请用户在使用时重点关注：

1. G0306-MS 和 G0306-SS 功能切换后，必须要给设备重新上电才能生效。
2. 地址拨码开关虽然有一个是 16 位的，但是是按照 10 进制进行计算的。  
例如：16 位旋钮为 0xB，10 位旋钮为 5，则地址为  $11(0xB) * 10 + 5 * 1 = 115$ 。
3. G0306-MS 的详细诊断功能是通过配置设备用户参数“MODBUS 从站状态监测”以及网关模块“xxx 位/字节 Modbus 从站监测模块”实现的。如果配置的“MODBUS 从站状态监测”参数非 0 时，则必须要所有配置的模块最后的位置上，配置相应的“xxx 位/字节 Modbus 从站监测模块”。





## 第5章 维护

- 简单维护

表 21 LED 指示灯状态表

LED 指示灯	颜色	正常状态	异常状态	异常原因	纠正方法
Power	绿	常亮	灭	供电故障	检查供电电源及连接
				内部故障	联系技术支持
Online	黄	常亮	灭	组态错误	检测硬件组态是否存在异常或未组态
				地址错误	检测地址是否与组态匹配
				环境故障	检测 DP 总线连接是否正确，终端匹配是否正确
				内部故障	联系技术支持
Offline	红	灭	亮	组态错误	检测硬件组态是否存在异常或未组态
				地址错误	检测地址是否与组态匹配
				环境故障	检测 DP 总线连接是否正确，终端匹配是否正确
				内部故障	联系技术支持
TxD	绿	闪烁	灭	未接 Modbus 设备	正确连接 Modbus 设备
				配置错误	检测是否正确配置模块参数
				供电故障	检查供电电源及连接
				内部故障	联系技术支持
RxD	黄	闪烁	灭	未接 Modbus 设备	正确连接 Modbus 设备
				配置错误	检测是否正确配置模块参数
				供电故障	检查供电电源及连接
				内部故障	联系技术支持

- 日常维护只限于清洁设备。
- 故障维修：发现故障，请返厂维修。
- 配置错误：以下配置错误，不会导致设备在 DP 端掉线，但 Modbus 通信会异常。

表 22 配置错误检测表

序号	异常现象	异常原因	纠正方法
1	部分 Modbus 命令发送错误	总状态模块配置错误	总状态模块仅允许配置在第 1 个槽中，不要将其配置在其他槽中
2	部分 Modbus 命令发送错误	控制模块配置错误	控制模块仅允许配置在第 2 个槽中，不要将其配置在其他槽中
3	部分 Modbus 命令发送错误	G0306-MS 的从站监测模块没有配置到最后	请将“MODBUS 从站状态监测”参数所对应的从站监测模块配置到最后一个有效的槽中，不要配置在通信模块中间。
4	部分 Modbus 命令发送错误	G0306-MS 的“MODBUS 从站状态监测”参数与所配置的从站监测模块不匹配	请使用“MODBUS 从站状态监测”参数所指定的从站监测模块。如“MODBUS 从站状态监测”参数为没有从站监测模块，那么，请不要配置从站监测模块。
5	发送完所有配置的 Modbus 命令后，还会发送几个字节数据	G0306-MS 的“MODBUS 从站状态监测”参数与所配置的从站监测模块不匹配，且所配置的从站监测模块长度大于“MODBUS 从站状态监测”参数长度	请将 从站监测模块 配置的与“MODBUS 从站状态监测”参数一致

## 第6章 技术规格

### 6.1 基本参数

工作电压	24VDC (±20%)
额定电流	$I_{24V} : \leq 60\text{mA}$
工作温度	-20℃~70℃
贮存温度	-40℃~70℃
湿度范围	5%~95%RH
Modbus 物理接口	RS485 (可配置终端) / RS232
Modbus 字符传输模式	RTU 模式

### 6.2 性能指标

防护等级	外壳防护等级达到IP20
电磁兼容	符合 GB/T 18268.1-2010《测量、控制和实验室用的电设备 电磁兼容性要求 第1部分:通用要求》中工业场所的抗扰度要求 FF 端口测试方法采用 GB/T 18268.23-2010《测量、控制和实验室用的电设备 电磁兼容性要求 第23部分:特殊要求 带集成或远程信号调理变送器的试验配置、工作条件和性能判据》

### 6.3 物理特性

重量	0.2kg
结构材料	壳体: ABS; 卡子: POM; 涂层: 聚脂环氧树脂。

### 6.4 默认通信参数

<b>通用默认通信参数</b>	
波特率	9600
数据位	8
停止位	1
校验	NO
<b>G0306-MS 默认通信参数</b>	
MODBUS 从站 状态监测	无
数据更新模式	在全部 MD 响应后
写入模式	一直写
主站发送间隔	从站应答发送
间隔时间值	500ms
槽	槽 1: 总状态模块; 槽 2: 控制模块; 槽 3-39: 没有模块
<b>G0306-SS 默认通信参数</b>	
Modbus 从站地址	1

### 6.5 支持 Modbus 功能码

1	读线圈
2	读离散量输入
3	读保持寄存器值
4	读输入寄存器值
5	写单个线圈
6	写单个寄存器
15	写多个线圈
16	写多个寄存器值



表 23 字符传输模式表

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: 1BIT	起始位: 1BIT
数据位	数据位: 8BITS	数据位: 7BITS
校验位	奇偶校验位(可选): 1 位	奇偶校验位(可选): 1 位
停止位	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, 从站不再继续通信, 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 主站在一定时间过后仍未收到从站应答, 即做出“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

表 24 Modbus 报文 RTU 格式表

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

### A.3 Modbus 异常响应

1) 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做出正确应答, 从站将以“异常响应”回答之。

## 2) 异常响应报文格式

例: 主站发请求报文, 功能码 01, 读 1 个 0x04A1 线圈值。

表 25 主站发送的请求报文(十六进制)

从站地址	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

由于从站的最高线圈地址为 0x0400, 则 0x04A1 超地址上限, 从站做出异常响应如下(注意: 功能码最高位置 1):

表 26 从站发送的响应报文(十六进制)

从站地址	功能码	异常码	CRC
0A	81	02	XXXX

## 3) 异常响应码

表 27 Modbus 异常响应码

异常码	名称	含义
0x01	非法功能	所收到的报文功能对于被编址从站是不允许执行的。若有询问命令发出, 则本码表示在此之前无编程功能。
0x02	非法数据地址	数据字段中的地址对于被编址的从站是禁止的。
0x03	非法数据	数据字段中的值对于被编址的从站是禁止的。
0x04	从站设备故障	当服务器(或从站)正在设法执行请求的操作时, 产生不可重新获得的差错。

## 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；

表 28 Modbus 存储区

存储区标识	名称	类型	读/写	存储单元地址（十进制）
0xxxx	线圈	位	读/写	00001~0xxxx xxxx: 与设备有关
1xxxx	离散量输入	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~xxxx: xxxx 与设备有关

## A. 5 Modbus 功能码

Modbus 协议共有三类 Modbus 功能码：公共功能码、用户定义功能码、保留功能码。

### 1) 公共功能码

- 是较好地定义的功能码
- 保证是唯一的
- MODBUS 组织可改变的
- 公开证明的
- 具有可用的一致性测试
- MB IETF RFC 中证明的
- 包含已被定义的公共指配功能码和  
未来使用的未指配保留供功能码

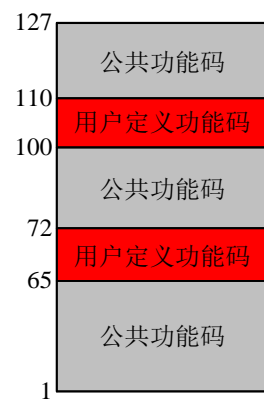


图 51 Modbus 功能码

### 2) 用户定义功能码

- 有两个用户定义功能码的定义范围，即 65 至 72 和 100 至 110
- 用户没有 MODBUS 组织的任何批准就可以选择和实现一个功能码
- 不能保证被选功能码的使用是唯一的
- 如果用户要重新设置功能作为一个公共功能码，那么用户必须启动 RFC，以便将改变引入公共分类中，并且指配一个新的公共功能码

### 3) 保留功能码

- 一些公司对传统产品通常使用的功能码，并且对公共使用是无效的功能码

### A. 5.1 01 (0x01) 读线圈举例

表 29 主站请求报文格式（十六进制）

从站地址	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	01	00	13	00	25	xxxx

功能：读从站线圈 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 17 (0x11) 号从站线圈，起始地址=0x0013=19，对应设备中的地址 00020；线圈数=0x0025=37；

末地址=00020+37-1=00056。

因此，本请求报文功能是：读 17 (0x11) 号从站的线圈 00020—00056，共 37 个线圈状态。

表 30 从站响应报文格式（十六进制）

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：从站返回线圈 0xxxx 状态。

本例：0xCD=11001101，对应 00020—00027；0x6B=01101011，对应 00028—00035；

0xB2=10110010，对应 00036—00043；0x1B=00011011，对应 00052—00056。

#### A. 5. 2 02 (0x02) 读离散量输入举例

表 31 主站请求报文格式（十六进制）

从站地址	功能码	高位起始地址	低位起始地址	离散量输入数高位	离散量输入数低位	CRC
11	02	00	C4	00	16	xxxx

功能：读从站离散量输入 1xxxx 状态。

注意：报文中离散量输入起始地址 00000 对应设备中 10001 地址，其他顺延。

本例：读 17(0x11)号从站离散量输入，起始地址=0x00C4=196，对应地址 10197；离散量输入数=0x0016=22，末地址=10197+22-1=10218。

因此，本请求报文功能是：读 17 (0x11) 号从站离散量输入 10197—10218，共 22 个离散量输入。

表 32 从站响应报文格式（十六进制）

从站地址	功能码	字节计数	离散量输入 10197-10204	离散量输入 10205-10212	离散量输入 10213-10218	CRC
11	02	03	AC	DB	35	xxxx

功能：从站返回离散量输入 1xxxx 状态。

#### A. 5. 3 03 (0x03) 读保持寄存器举例

表 33 主站请求报文格式（十六进制）

从站地址	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	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 17 (0x11) 号从站保持寄存器值，起始地址=0x006B=107，对应地址 40108；寄存器数=0003；末地址=40108+3-1=40110。

因此，本请求报文功能是：读 17 (0x11) 号从站 3 个保持寄存器 40108—40110 的值。

表 34 从站响应报文格式（十六进制）

从站地址	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)=0x022B，(40109)=0x0106，(40110)=0x2A64。

#### A. 5. 4 04 (0x04) 读输入寄存器举例

表 35 主站请求报文格式（十六进制）

从站地址	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 17 (0x11) 号从站输入寄存器值，起始地=0x0008=0008，对应地址 30009；寄存器数=0001；末地址=30009。

因此，本请求报文功能是：读 17 (0x11) 号从站 1 个保持寄存器 30009 的值。

表 36 从站响应报文格式（十六进制）

从站地址	功能码	字节计数	输入寄存器高位	输入寄存器低位	CRC
11	04	02	01	01	xxxx

功能：从站返回输入寄存器 30009 的值；(30009)=0x0101。

#### A. 5. 5 05 (0x05) 写单个线圈举例

表 37 主站请求报文格式（十六进制）

从站地址	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	FF	00	xxxx

功能：写 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=0xFF00，置线圈 ON。

断通标志=0x0000，置线圈 OFF。

本例：起始地址=0x00AC=172，对应设备中的地址为 00173。

因此，本请求报文功能是：写 17 号从站线圈 00173 为 ON 状态。

表 38 从站响应报文格式（十六进制，原文返回）

从站地址	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：写 17 号从站线圈 0173 为 ON 后，原文返回。

#### A. 5. 6 06 (0x06) 写单个寄存器举例

表 39 主站请求报文格式（十六进制）

从站地址	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：写单个保持寄存器 4xxxx 值。报文中寄存器起始地址 00000 对应设备中 40001 地址，其它顺延。

本例：写 17 号从站单个保持寄存器 40136 值=0x039E。

表 40 从站响应报文格式（十六进制，原文返回）

从站地址	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：写 17 号从站单个保持寄存器 40136 值=0x039E 后，原文返回。

#### A. 5. 7 15 (0x0F) 写多个线圈举例

表 41 主站请求报文格式（十六进制）

从站地址	功能码	线圈地址高位	线圈地址低位	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 写为 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：写 17(0x11)号从站多个连续线圈，线圈起始地址=0x0013=19，对应地址 00020；线圈数=0x000A=10；

末地址=00020+10-1=00029。

因此，本请求报文功能是：写 17 (0x11) 号从站 10 个线圈 00020—00029 的值；其中，00020—00027 地址写入 0xCD，00028—00029 地址写入 0x00。

表 42 从站响应报文格式（十六进制）

从站地址	功能码	线圈地址高位	线圈地址低位	线圈数高位	线圈数低位	CRC
11	0F	00	13	00	0A	xxxx

功能：返回线圈地址和线圈数。

#### A.5.8 16 (0x10) 写多个寄存器

表 43 主站请求报文格式（十六进制）

地址	功能码	寄存器地址高位	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	13	00	0A	02	CD	00			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 17 (0x11) 号从站多个保持寄存器值，寄存器起始地址=0x0087=135，对应地址 40136，线圈数=0x0002=2，末地址=40135+2-1=40137；

因此，本请求报文功能是：预置 17 (0x11) 号从站 2 个保持寄存器值；40136 地址写入 0x0105；40137 地址写入 0x0A10。

表 44 从站响应报文格式（十六进制）

从站地址	功能码	寄存器地址高位	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

功能：返回寄存器地址和寄存器数。



**附录B G0306 Modbus 转 DP 网关选型代号表**

GW-MODB-DP	G0306 Modbus 转 DP 网关	
	代号	Modbus 物理接口
	RS485	RS485 接口
	RS232	RS232 接口
GW-MODB-DP - RS485 —— 选型示例		



中国科学院沈阳自动化研究所  
沈阳中科博微科技股份有限公司  
[Http://www.microcyber.cn](http://www.microcyber.cn)  
地址：中国·沈阳·浑南新区文溯街17-8号  
邮编：110179  
电话：0086-24-31217295 / 31217296  
传真：0086-24-31217293  
EMAIL: [sales@microcyber.cn](mailto:sales@microcyber.cn)