以太网主站网关

PBM-ETH-3.0 产品手册

V1.0

北京鼎实创新科技股份有限公司

2015 年 9 月

第一章 产品概述.....1
1. 产品系列.....1
2. PBM-ETH-3.0 主要用途.....1
3. PBM-ETH-3.0 特点.....2
4. PBM-ETH-3.0 技术指标.....2
第二章 产品外观及指示灯.....5
1. 产品布局及指示灯正常工作时状态.....5
2. 产品结构尺寸.....9
3. 拨码开关的含义.....9
4. 网口的两种工作模式.....11
第三章 产品安装.....13
1. 导轨安装.....13
2. PROFIBUS 接口接插件及安装.....13
3. 电源安装.....14
4. 网线安装.....15
第四章 **PBM-ETH-3.0** 工作原理.....16
第五章 **PBM-ETH-3.0** 的运行.....17
第六章 配置软件 **PB-Confi** 的调试.....18
1. 通过 PB-Confi 进行离线配置.....19
1.1 新建项目.....19
1.2 更新设备目录.....20
1.3 添加主站.....21
1.4 添加从站.....22
1.5 设置总线参数.....25
1.6 设置软件连接的 IP 地址.....25
1.7 配置下载.....26
1.8 配置 PBM-ETH-3.0 网络参数.....26
1.9 保存以及加载 PBM-ETH-3.0 的配置文件.....27
2. 通过 PB-Confi 进行在线调试.....28
2.1 主站网关的主站操作.....28
2.2 主站网关的从站操作（DPV1 的操作）.....29
2.3 监控主站网关所连从站的状态.....29
2.4 PROFIBUS DPV0 IO 数据通信.....30
2.5 导出当前系统所有主站网关及从站状态.....30
2.6 更改从站地址（特殊从站）.....31
2.7 查看系统日志.....31
3. 固件升级.....32
第七章 实现 **PROFIBUS-DP** 从站的监控.....33
1. 输入寄存器数据区.....33
2. 保持寄存器数据区.....38
3. PBM-ETH-3.0 MODBUS 通信应答返回码.....40
4. PBM-ETH-3.0 Modbus DPV0 数据区操作.....41
4.1 DPV0 读数据操作.....41
4.2 DPV0 写数据操作.....44

5. PBM-ETH-3.0 Modbus DPV1 数据区操作.....45
5.1 DPV1C1 的读写请求及响应报文的含义.....46
5.2 DPV1C1 的读写请求报文案例.....48
5.3 DPV1C2 的读写请求及响应报文的含义.....48
5.4 DPV1C2 的读写请求报文案例.....50
5.5 DPV1C2 的异步事件.....51
5.6 利用主站网关的 DTM 使用 DPV1C2 功能.....53
6. PBM-ETH-3.0 Modbus DP 从站诊断数据区操作.....53
7. PBM-ETH-3.0 Modbus 系统日志区操作.....54
8. PBM-ETH-3.0 Modbus 寄存器区位功能定义详述.....56
第八章 基于 FDT/DTM 框架的 PA 通信实例.....61
1、 主站网关 PBM-ETH-3.0 的 PA 与 DTM 功能简介.....61
2、实例系统与相关软件.....63
3、PA 配置.....64
4、PROFIBUS PA 通信中的 DTM 应用.....65
附录一：术语.....75
附录二：常见故障排查（补充中）.....77
附录三：MODBUS/TCP 通信规范简介.....78
1. 概述.....78
1.1 面向连接.....78
1.2 数据编码.....79
1.3 参考编号的解释.....79
1.4 隐含长度基本原则.....80
2. 一致性等级概述.....80
2.1 等级 0.....80
2.2 等级 1.....80
2.3 等级 2.....81
2.4 机器/厂家/网络的特殊功能.....81
3. 协议结构.....82
4. 一致性等级的协议参考值.....83
4.1 等级 0 指令详述.....83
4.2 等级 1 指令详述.....85
4.3 等级 2 指令详述.....88
5. 异常代码.....93
6. MODBUS 存储区.....95
7. MODBUS 功能.....96
7.1 读取保存寄存器.....97
7.2 读取输入寄存器.....98
7.3 预置单寄存器.....99
7.4 预置多寄存器.....100
附录四 主站网关 2.0 与 3.0 的技术指标对比.....102
附录五 有毒有害物质表.....103

第一章 产品概述

1. 产品系列

北京鼎实主站网关系列产品包括 PBM-G-CANOPEN、PBM-G-MBS、PBM-G-PCI、PBMG-ETH-2 和 PBM-ETH-3.0 等。主站网关系列产品主要用于将 PROFIBUS-DP 从站设备接入到其他不同协议的工业网络中。其中 PBMG-ETH-2 用于将 PROFIBUS-DP 从站设备连接到工业以太网 MODBUS/TCP 上。

PBM-ETH-3.0 是 PBMG-ETH-2 的升级产品，在 PBMG-ETH-2 的功能基础上增加了 PROFIBUS-DPV1，诊断统计，固件升级，系统日志等功能。详细参见附录四。

本产品手册只适用于 PBM-ETH-3.0 。

2. PBM-ETH-3.0 主要用途

北京鼎实主站网关 PBM-ETH-3.0 用于实现 MODBUS/TCP 协议与 PROFIBUS 协议的转换。PBM-ETH-3.0 在 MODBUS/TCP 侧作为服务器，在 PROFIBUS 侧作为主站，将 DP 从站设备接入 MODBUS/TCP 网络中。

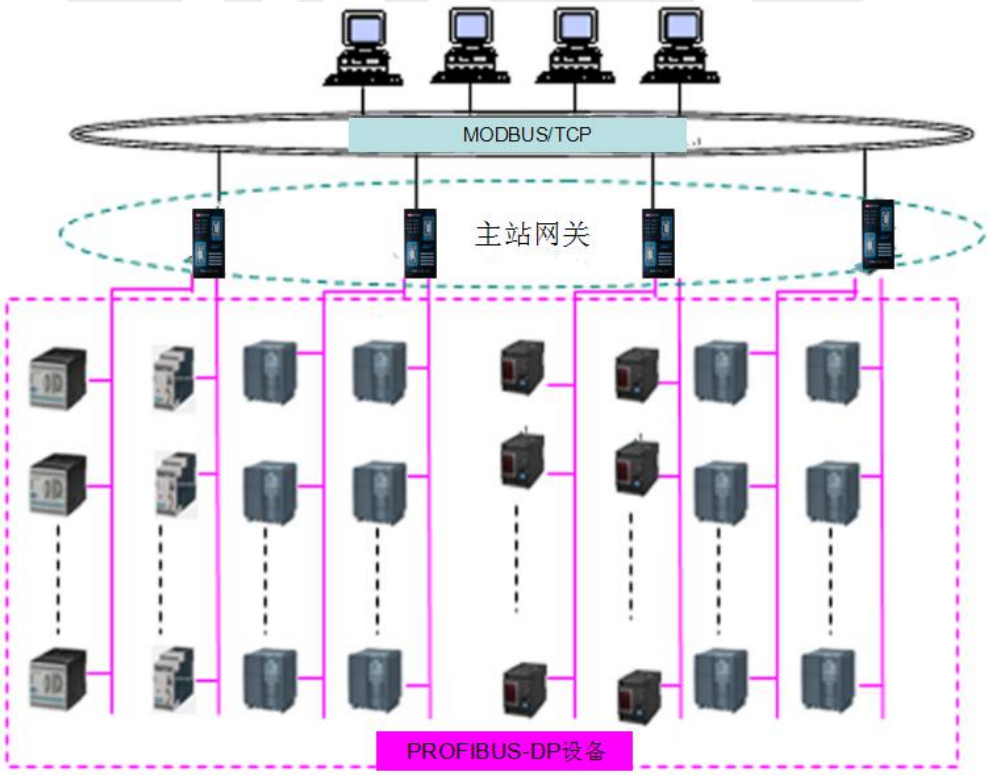


图 1-1

3. PBM-ETH-3.0 特点

- 应用简便

  用户不需了解 PROFIBUS 和 MODBUS/TCP 技术细节，只需参考本手册根据系统要求完成配置，即可在短时间内实现连接通信。

- 应用灵活

  以太网接口交换机，双网口两种工作模式，适合在不同的网络环境中应用。

- 性能卓越

  采用两颗独立的 CPU 分别作为 PROFIBUS 主站和 MODBUS/TCP 服务器，二者并行工作，PROFIBUS 通信和以太网通信互不影响，二者间通过双端口 RAM 共享数据。

- 丰富的诊断和统计功能

  通过前面板指示灯，附带的 PB-Confi 软件或设备 MODBUS 数据区对网关设备自身，PROFIBUS 主站，从站进行全面的运行监控，快速发现问题。

- 支持固件升级功能

  进行内嵌固件升级,不但可以快速修补漏洞，增强产品稳定性，还可以完善和扩充产品的功能。

- 支持系统日志功能

  通过系统日志，记录设备运行过程中的关键事件，便于进行系统维护。

4. PBM-ETH-3.0 技术指标

（1） PROFIBUS-DP 接口 Ethernet

- **连接器：**DB9 孔×2
- **电气隔离：**两个接口单独电气隔离，隔离电压 1kV
- **波特率：**9.6k, 19.2k,45.45k,93.75k,187,5k,500k, 1.5M, 3M, 6M（由配置软件设置）
- **通信协议：**PROFIBUS DPV0，DPV1C1，DPV1C2（IEC 61158-3、GB/T 20540-2006）
- **在线变更从站地址：**支持
- **单/多主站系统：**单主站系统
- **最大站点数：62**（2 个 DB9 接口，每个接口在不加中继器的情况下最多 31 个从站）
- **单从站最大数据量：**244 字节输入，244 字节输出
- **最大配置数据：**8k

- **最大诊断数据：**4k
- **最大输出数据：**8k
- **最大输入数据：8**k
- **每个从站最大 DPV0 模块数：**32
- **DPV1C2 同时支持的从站连接数：**1

（2）以太网接口

- **连接器：**RJ45×2
- **隔离电压：**1.0kV
- **网口特性：**10/100Mbps 自适应，支持自动线序识别
- **工作模式：**交换机，双网口模式
- **支持协议：**ARP，ICMP，IGMP，IP，TCP，UDP，MODBUS/TCP Server
- **流量限速：**支持
- **IP 冲突检测：**支持
- **推荐线缆：**推荐工业以太网专用线缆
- **工作模式：**MODBUS/TCP Server
- **连接数目：**交换机模式 4 个连接；双网口模式每个网络地址上 4 个连接
- **TCP 连接断开检测：**支持
- **支持的 MODBUS/TCP 功能码：**0x03，0x04，0x06，0x10
- **系统日志条目：**256

（3）配置软件

- **版本要求：** 3.8 及以上版本
- **解析从站 GSD 文件：**支持
- **运行状态监控：**支持
- **DPV0 IO 数据监控：**支持
- **固件升级：**支持
- **设备日志：**支持
- **系统报告：**支持
- **DPV1 C1/C2 功能：**支持

（4）支持 PROFIBUS-PA 及 FDT/DTM 功能

- 提供 PBM-ETH-3.0 配套通信 DTM 和网关 DTM；
- 具体使用参见第八章例程

（5）供电

- **连接器：**6 针端子
- **供电电压：**24V(±20%)
- **工作电流**: 152.95MA(24V，31 个从站设备）
- **额定功耗：**3.6708W
- **冗余电源：**支持

（6）防护等级

- **防护等级：**IP20

（7）环境条件

- **运输和存储温度：**-40℃ ～+70℃
- **工作温度：**-25℃ ～+55℃
- **工作相对湿度：**5～90% （无凝露）。

（8）机械特性

- **外壳：**塑料
- **尺寸：**宽：55mm × 深：103mm × 高：120mm

（9）EMC 等级

- **脉冲群:** IEC 61000-4-4 2KV（A 级性能判据）
- **浪涌：**IEC61000-4-5 CM：±2KV， DM：±1KV (A 级性能判据）

第二章 产品外观及指示灯

1.产品布局及指示灯正常工作时状态

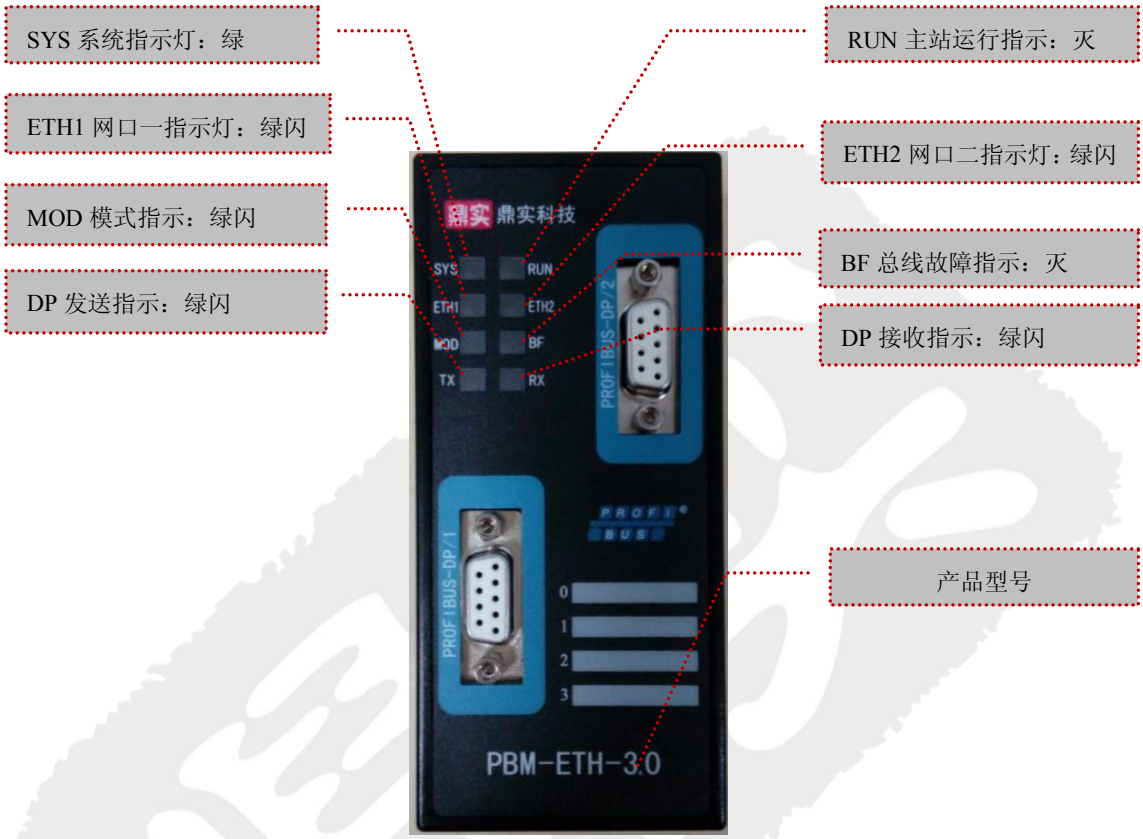


图 2-1 产品指示灯

表 2-1. 前面板接口

接口名称	功能
PROFIBUS-DP/1	PROFIBUS 标准 DP 接口，配合 PROFIBUS 专用插头使用
PROFIBUS-DP/2	PROFIBUS 标准 DP 接口，配合 PROFIBUS 专用插头使用

表 2-2. 前面板状态指示灯 1

LED 名称	颜色	状态	含义
SYS 系统指示	红绿双色	灭	设备未上电
		绿色常亮	工作模式下设备正常启动
			固件升级模式下更新固件前
			固件升级模式下更新固件成功
		绿色闪烁	固件升级模式下正在更新固件
			开启设备识别功能
		红色常亮	设备启动中
			固件升级模式下更新固件失败
			下载配置失败
		红色闪烁	正常工作模式下，工作固件启动失败
RUN 主站运行 指示	红黄双色	灭	主站工作在 RUN 状态
		黄色常亮	主站工作在 STOP 状态
		红色常亮	主站工作在 OFFLINE 状态
ETH1 网口 1 指示	红绿双色	红色常亮	网口 1 物理链路断开
		红色闪烁	网口 1 IP 冲突。与网口 1 相连的网络中存在相同 IP 地址的设备。
		绿色常亮	网口 1 运行正常
		绿色闪烁	网口 1 上有 MODBUS 报文通信
ETH2 网口 2 指示	红绿双色	红色常亮	网口 2 物理链路断开
		红色闪烁	网口 2 IP 冲突。与网口 2 相连的网络中存在相同 IP 地址的设备。
		绿色常亮	网口 2 运行正常
		绿色闪烁	网口 2 上有 MODBUS 报文通信

表 2-2. 前面板状态指示灯 2

LED 名称	颜色	状态	含义
MOD 模式指示	红绿双色	红色常亮	主站处于空闲状态
		绿色闪烁	主站处于工作状态
BF 总线故障指示	红黄双色	灭	所有配置从站都处于数据交换状态，且无报警
		黄色常亮	有从站产生高优先级报警，高优先级报警解除后才熄灭
		红色常亮	有配置从站未处于数据交换状态
		红黄同亮	既有从站掉线，又有从站产生高优先级报警
TX DP 发送指示	红绿色	灭	主站未向 DP 总线发送数据
		绿色闪烁	主站向 DP 总线发送数据
		红色	主站向 DP 总线发送报文错误
RX DP 接收指示	红绿色	灭	主站未收到来自 DP 总线的数据
		绿色闪烁	主站收到来自 DP 总线的数据
		红色	主站接收来自 DP 总线的报文错误

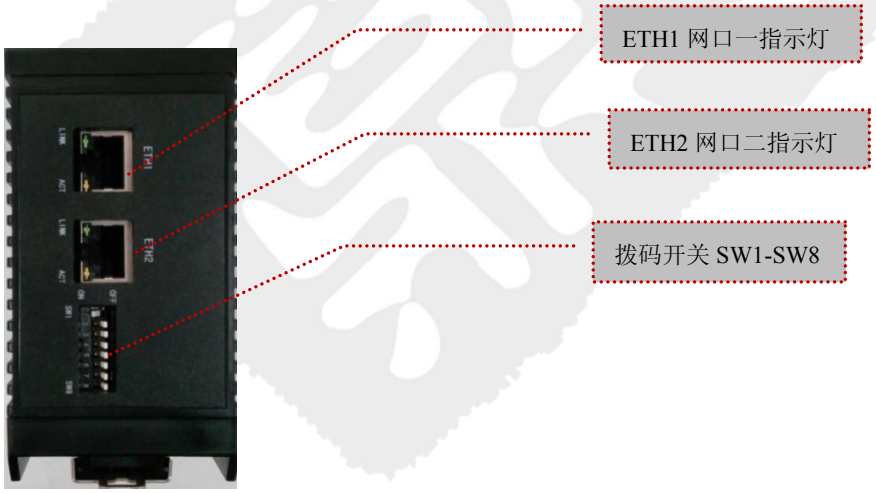


图 2-2 产品侧面图

表 2-3 网络接口

接口名称	功能
ETH1	快速以太网接口，绿色 LED 为物理链路联通指示，橙色 LED 为通信活动指示
ETH2	快速以太网接口，绿色 LED 为物理链路联通指示，橙色 LED 为通信活动指示

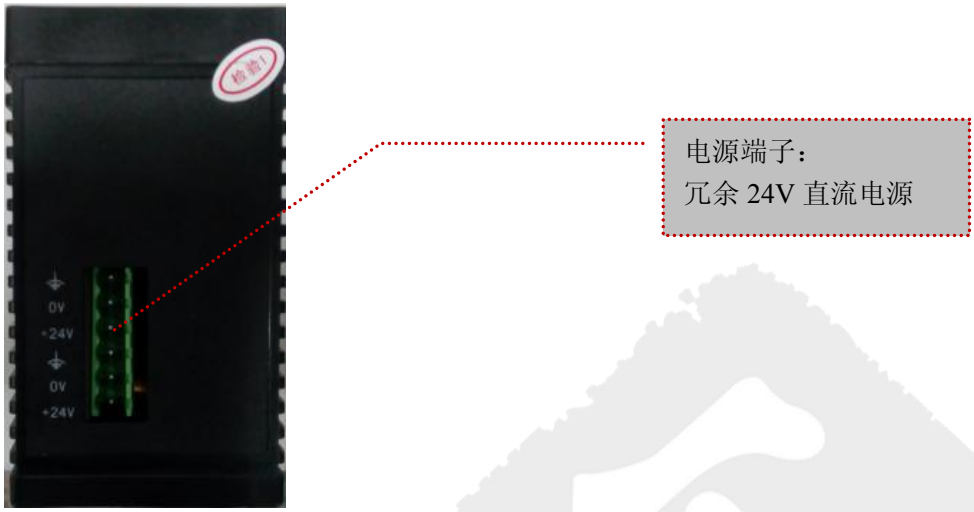


图 2-3 产品侧面图

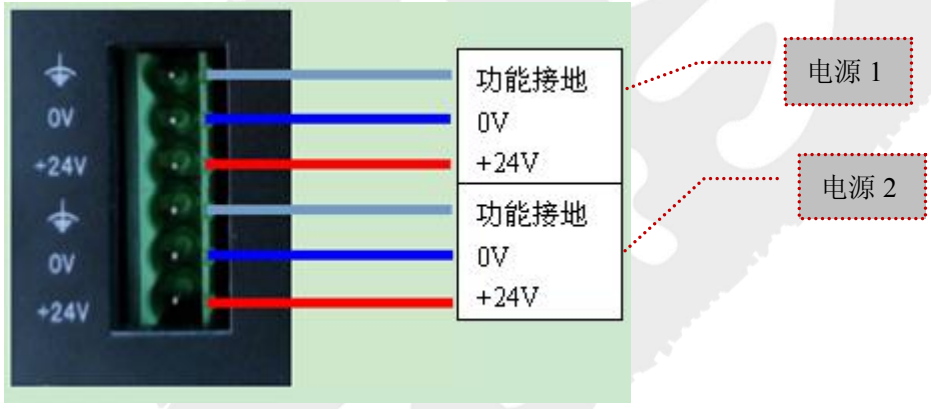


图 2-4 产品侧面电源图

表 2-4 电源接口

接口信号名称	功能描述
24V 电源 1	第一路直流 24V 电源正极输入。
24V 电源 2	第二路直流 24V 电源正极输入。
0V	两路直流 24V 电源的 0V。
功能接地	模块的接地

2. 产品结构尺寸

产品外形尺寸：55mm（宽） × 103mm（深） × 120mm（高），外形尺寸图如下图 2-5 所示。

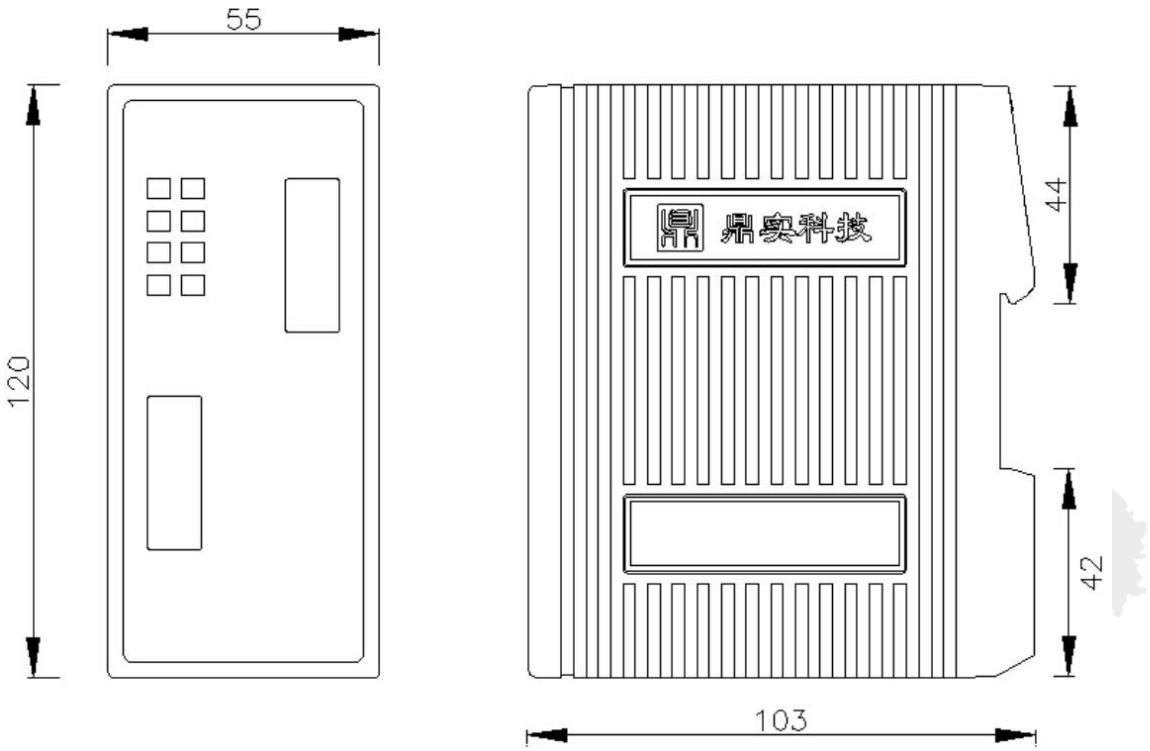


图 2-5、产品结构尺寸图

3. 拨码开关的含义

产品功能拨码开关 SW1-8，目前只使用 SW1~SW4 一位，其它拨码留作备用，见下图所示：

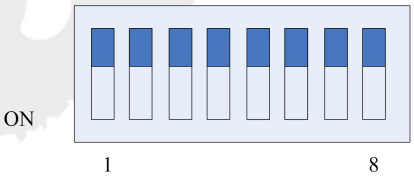


表 2-5 拨码开关

拨码开关位	功能	描述
Bit1	默认网络参数	为 ON 表示网络接口以默认网络参数启动，为 OFF 表示以用户配置的 IP 地址启动。

Bit2	reserved	
Bit3	**固件升级模式**	为 ON 表示主站网关运行在在固件升级模式，为 OFF 表示运行在正常工作模式。
Bit4	**离线模式**	为 ON 表示将主站置于离线模式，网关上电不利用本地配置启动主站，PROFIBUS 主站工作在离线状态，不向 DP 总线发送报文。若因本地配置异常导致网关无法启动时，可切换到该模式，并通过配置软件下载新的配置，之后再切换回正常工作模式。
Bit5~8	reserved	

注意：主站网关仅在上电时检测拨码开关的状态，之后确定工作模式，因此拨码开关的状态设置必须重新上电才有效。

默认网络参数

在用户没有设置网络参数或拨码开关置于“默认网络参数”模式时主站网关按以下网络参数启动：

表 2-6 默认网络参数

参数	默认值
网口工作方式	双网口模式
网口 1 IP 地址	192.168.1.10
网口 1 子网掩码	255.255.255.0
网口 1 网关地址	192.168.1.1
网口 2 IP 地址	192.168.2.10
网口 2 子网掩码	255.255.255.0
网口 2 网关地址	192.168.2.1

4. 网口的两种工作模式

PBM-ETH-3.0 以太网侧提供两个接口，可以工作在交换机模式也可以工作在双网口模式。用户利用产品附带的配置软件 PB-Confi 在对网关 PBM-ETH-3.0 进行配置的时候，选择其中一种工作模式即可。

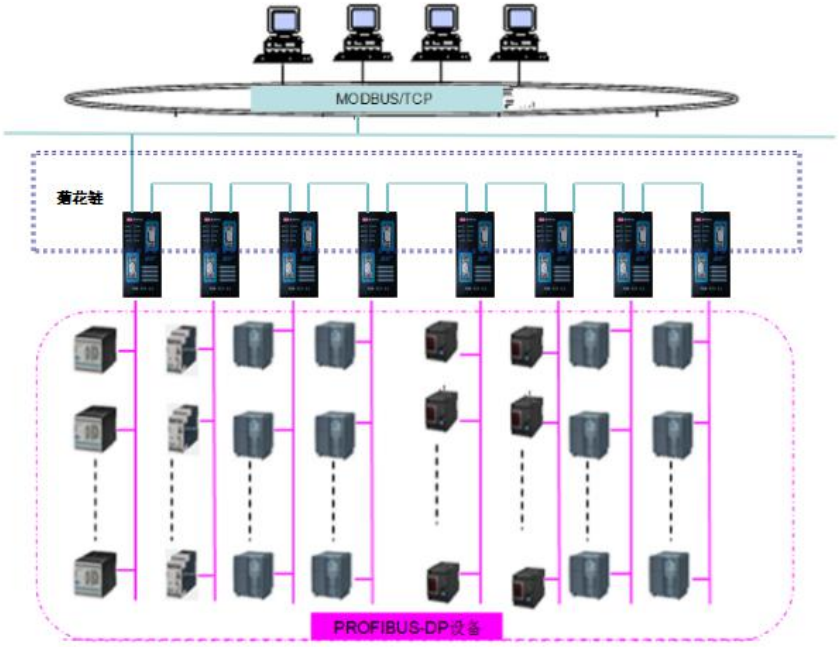


图 2-6 交换机模式的网络连接*（基于菊花链方式的拓扑结构，系统不需外置交换机）*

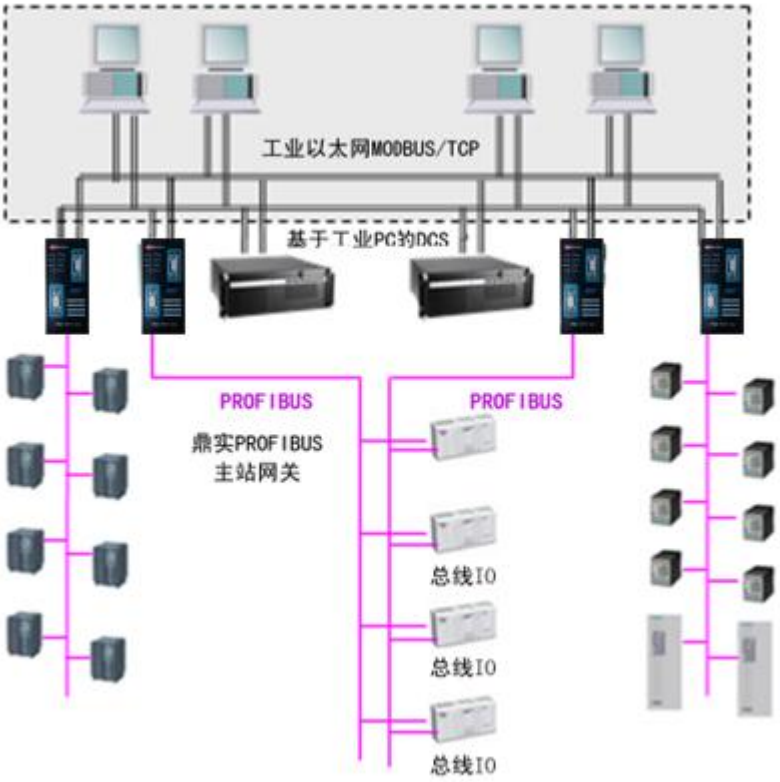


图 2-7 双网口模式的网络连接

第三章 产品安装

1. 导轨安装

使用标准 35mm DIN 导轨，导轨水平安装。器件的上下方至少留有 40mm 的空间便于散热。

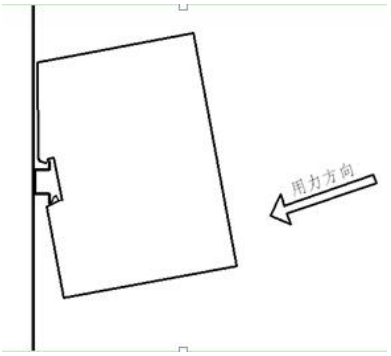


图 3-1 a.安装

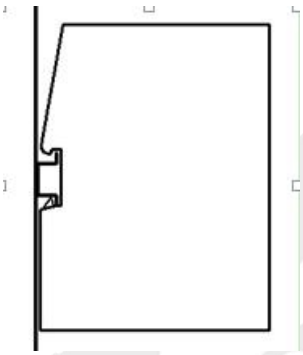


图 3-1 b.固定

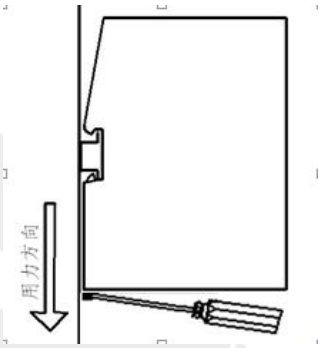


图 3-1c.拆卸

2. PROFIBUS 接口接插件及安装

PBM-ETH-3.0 总线桥的接口，采用标准 9 针 D 形 PROFIBUS 插座（孔）。建议用户使用标准 PROFIBUS 插头及标准 PROFIBUS 电缆,并在总线两端设置终端电阻。有关 PROFIBUS 安装规范请用户参照有关 PROFIBUS 技术标准，如下图 3-2 所示：

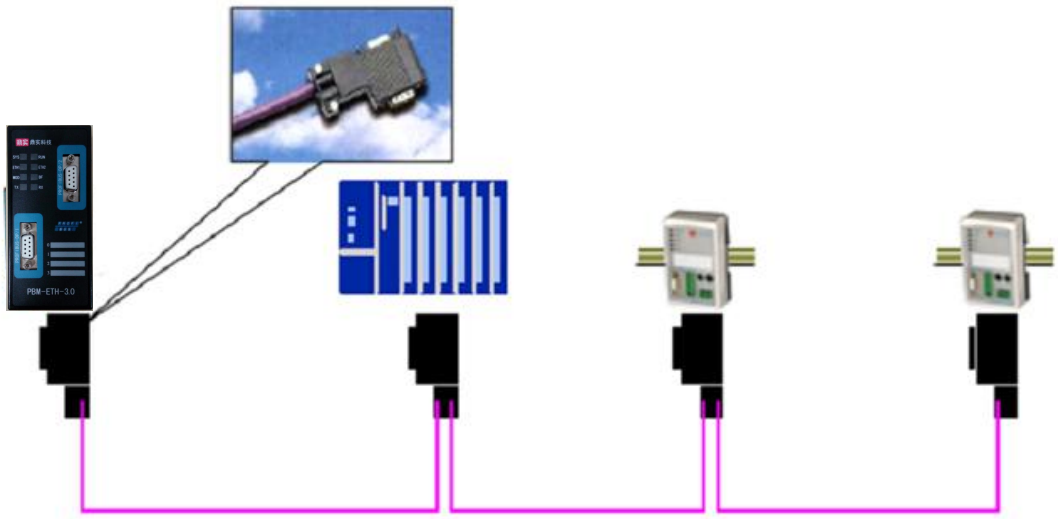


图 3-2 PROFIBUSB 标准接线

3. 电源安装

单独 24V（±20%）直流电源供电接法

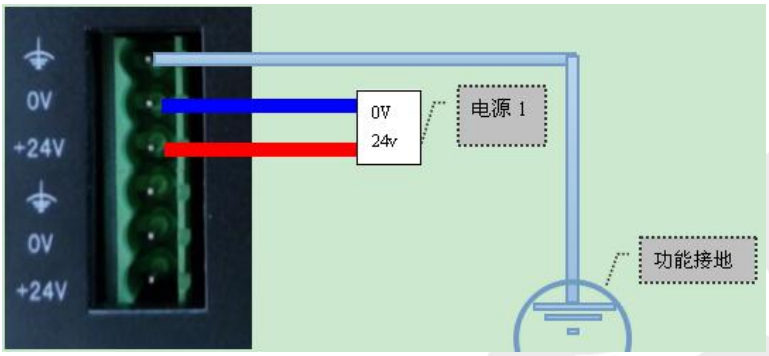


图 3-3a　单独连接一路电源

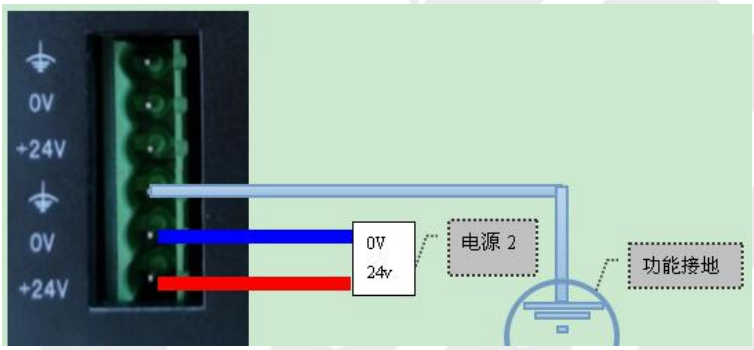


图 3-3b　单独连接一路电源

冗余 24V（±20%）直流电源供电接法

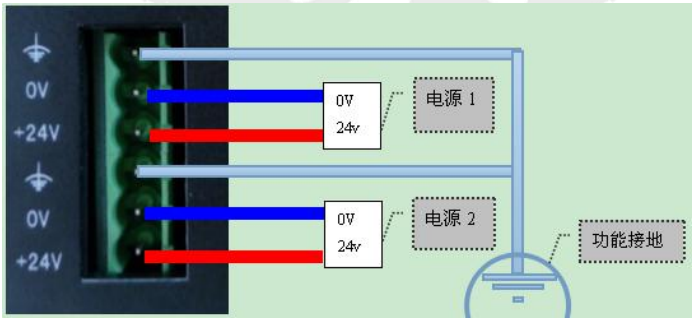


图 3-4　冗余电源标准接线

4. 网线安装

以太网端口：RJ45 接头，平行线、交叉线自适应。如果想得到更加稳定的通讯保障， 获得更强的抗干扰能力，建议使用工业以太网网线。工业以太网网线的基本构造为四芯铜线，带有屏蔽层，具有很强的屏蔽外界信号抗干扰的能力，使用这种网线能够大大提升通讯系统的稳定性。

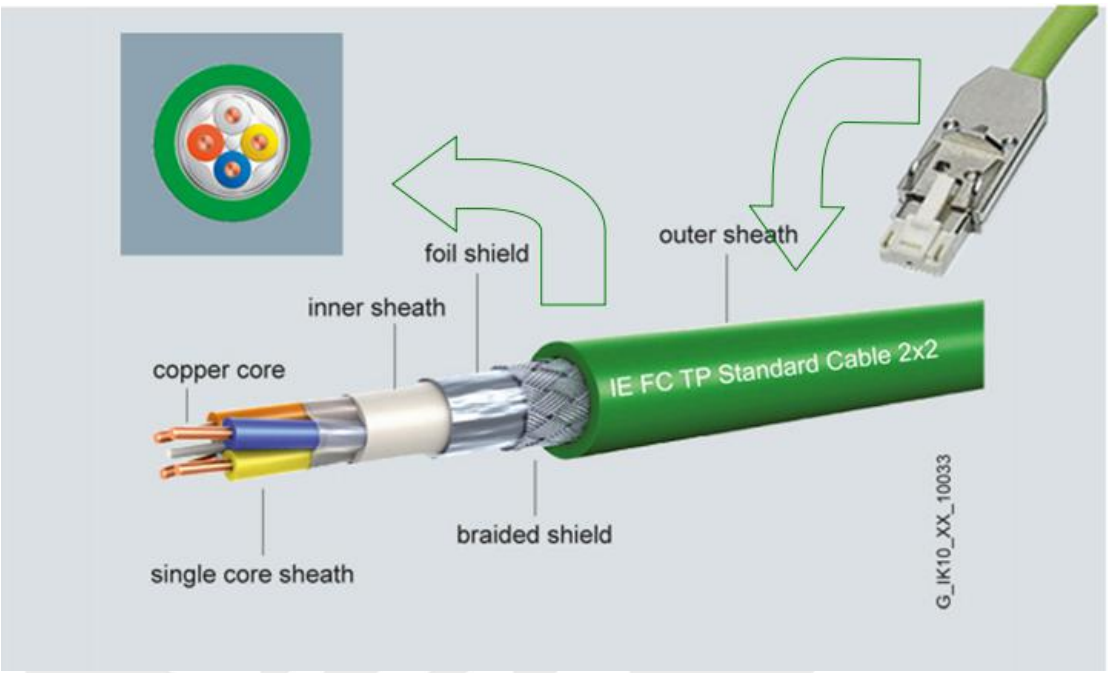


图 3-5 工业以太网网线

更多 PROFIBUS-DP 安装知识详见《PROFIBUS 现场总线安装指导手册》，该手册鼎实网站 www.c-profibus.com.cn 上可以下载。

第四章 PBM-ETH-3.0 工作原理

PBM-ETH-3.0 内置 MODBUS/TCP 服务器，用户通过 MODBUS 数据区实现对 PROFIBUS-DP 从站设备的控制，诊断和 DP 数据通信等功能。支持 MODBUS 功能码为 0x03、0x04、0x06 和 0x10。

PBM-ETH-3.0 主站网关通过 PROFIBUS 循环/非循环数据及主站网关内部数据到 MODBUS 存储区的映射，实现对主站网关的监控及 MODBUS 与 PROFIBUS 的数据共享，内置 MODBUS/TCP 客户端的用户设备可以通过对 MODBUS 三、四区的读写操作，实现对 PROFIBUS 循环/非循环数据的读写。

下图为主站网关内部数据映射共享示意图：

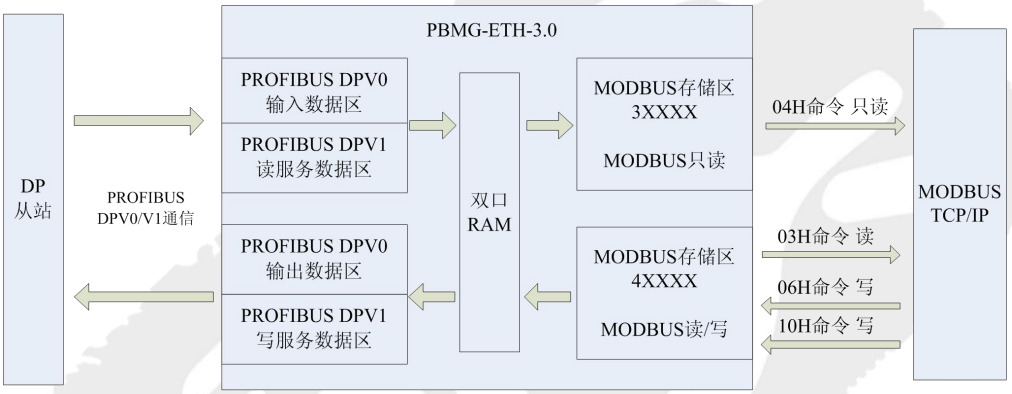


图 4-1 映射关系示意图

PROFIBUS-DP 从站的输入输出数据位于 DPRAM 中，运行 PROFIBUS 主协议栈的 CPU 负责与 DP 从站进行 IO 通信，从 DPRAM 输出数据区取 DP 从站的输出数据并发给 DP 从站，从 DP 从站获取的输入数据写入到 DPRAM 的输入数据区。

以太网侧 CPU 负责处理 MODBUS/TCP 服务请求，对于 MODBUS/TCP 写请求按照配置的从站数据映射关系写入到 DPRAM 输出数据区的相应地址，对于 MODBUS/TCP 读请求按照配置的从站数据映射关系从 DPRAM 输入数据区的相应地址取出数据回复给 MODBUS/TCP 客户端。

第五章 PBM-ETH-3.0 的运行

用标准的 PROFIBUS 电缆将主站网关 PBM-ETH-3.0 的 DP 接口与 PROFIBUS-DP 从站设备的 DP 接口连接起来。建议使用工业以太网网线将主站网关 PBM-ETH-3.0 的网口与控制器相连接。

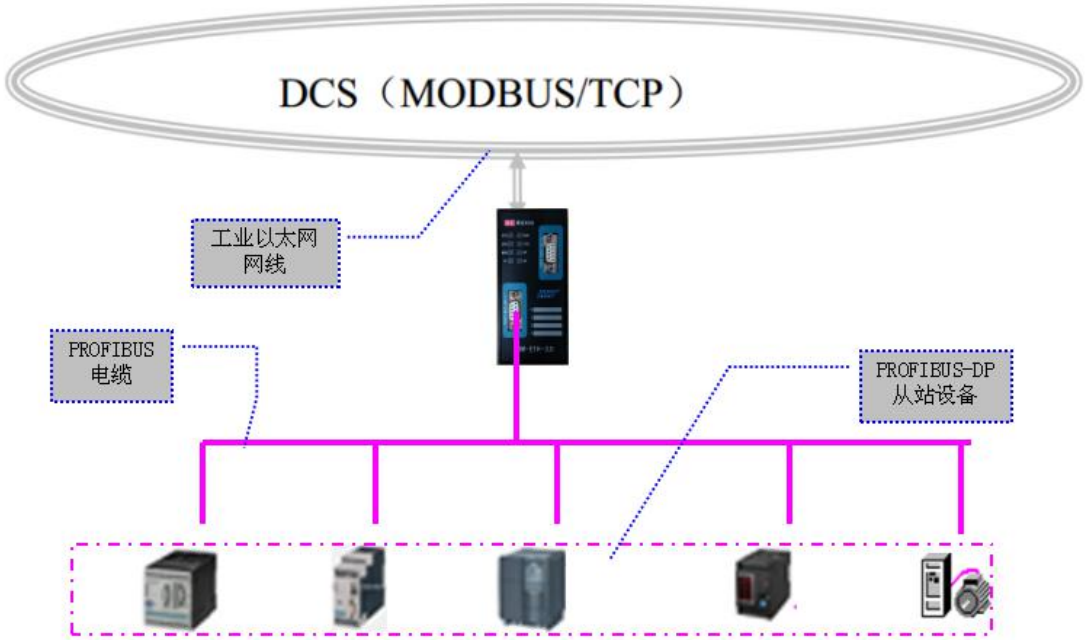


图 5-1 工作状态

PBM-ETH-3.0 内置 PROFIBUS-DP 主站协议栈和 MODBUS/TCP 服务器，在经过软件 PB-Confi 配置后，PBM-ETH-3.0 的 PROFIBUS 侧主站协议栈就可以和 PROFIBUS-DP 从站进行数据交换了；以太网侧 MODBUS/TCP 服务器也可以和 MODBUS/TCP 客户端进行数据交换了。它们之间的映射关系，参见第四章。

下章中将介绍如何使用软件 PB-Confi 下载配置。

第六章 配置软件 PB-Confi 的调试

本章主要介绍配置软件 PB-Confi 的功能和 PBM-ETH-3.0 的配置方法。

配置软件 PB-Confi 的功能：

- 配置和下载　　配置 PBM-ETH-3.0 相关参数，通过以太网 MODBUS/TCP 服务器接口下载配置。
- 在线监测　　通过内置 MODBUS/TCP 服务器接口获取 DP 从站 IO 数据，进行 DPV1C1/C2 通信，获取系统（主站及所连从站）诊断信息，通过内置系统日志功能记录系统运行关键事件。
- 固件升级　　通过内置设备固件升级功能快速进行功能升级和缺陷修复。

PBM-ETH-3.0 的配置方法：

下载配置时，建议网关 PBM-ETH-3.0 的 DP 口连接 PROFIBUS-DP 从站设备（方便后面 PB-Confi 进行在线调试）；另一侧网口连接已经安装配置软件 PB-Confi 的电脑，先不要连接 MODBUS/TCP 的控制器，待配置下载或者调试完毕后，再连接控制器。示意图如下所示

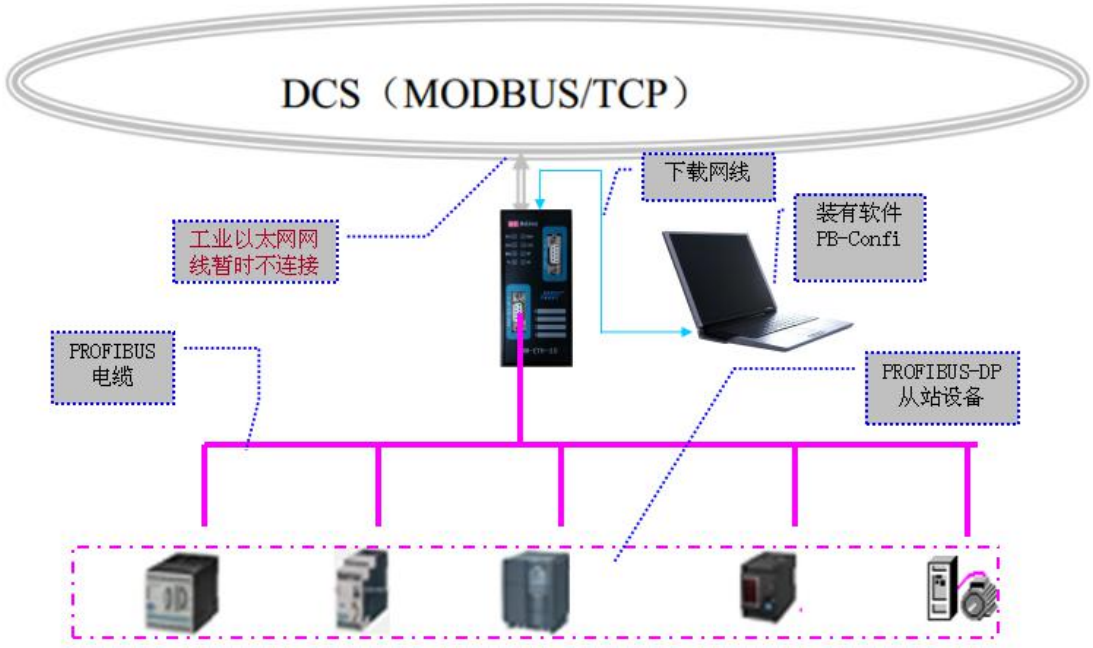


图 6-1 下载配置示意图

1. 通过PB-Confi进行离线配置

本产品使用需要和 PB-Confi 配合使用。PBM-ETH-3.0 使用的是 PB-Confi 软件的以太网下载功能。这里以一个应用实例配置为例。具体配置如下：

表 6-1 实例配置表

实例配置				
序号	设备名称	型号及技术指标	数量	备注
1	网关设备	PBM-ETH-3.0	1	本产品
2	PROFIBUS 从站	PB-DSDPV1	1	其它从站皆可
3	MODBUS/TCP 客户端	电脑	1	模拟 MODBUS/TCP 客户端
		软件 ModScan32.exe	1	
4	DP 电缆（带有 DP 插头）	标准 PROFIBUS 电缆	1	连接 PROFIBUS 侧
5	网线（带有水晶头）	普通网线	1	连接以太网侧

1.1 新建项目

点击配置软件 PB-Confi 图标，进入 PB-Confi 的页面。在打开软件配置窗口后进入如下界面。

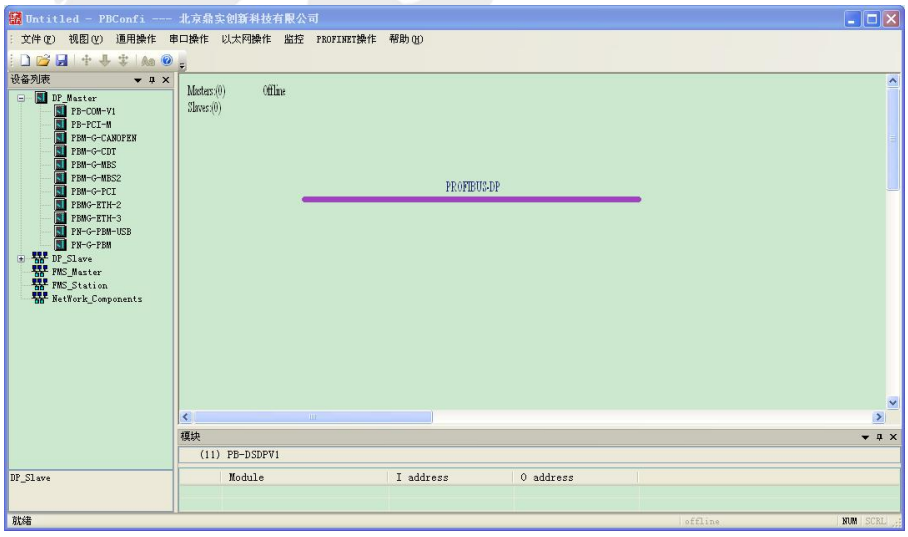


图 6-2 新建项目

1.2 更新设备目录

如果用户所需配置的从站设备的 GSD 文件还没有放入 PB-Confi 软件相应的目录下，可以点击“视图” →“工作目录”→“GSD 目录”。将从站设备 GSD 文件拷贝入打开的 GSD 文件夹中。

放入从站设备 GSD 文件后，需要对当前设备目录进行更新。点击“文件” →“重读 GSD”，如图所示，即可更新软件窗口右边的设备目录。此时，相应的从站设备应该出现在左方设备目录中的“DP-slave”目录中。

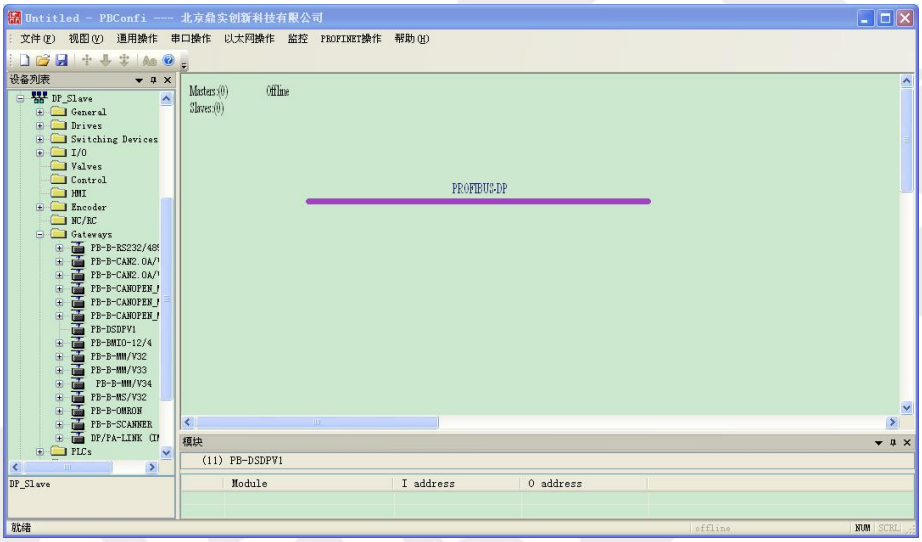


图 6-3 设备目录更新

1.3 添加主站

点击软件界面右侧的硬件设备栏，点击“DP-Master” →“PBM-ETH-3.0”，软件将自动添加 PBM-ETH-3.0 主站。

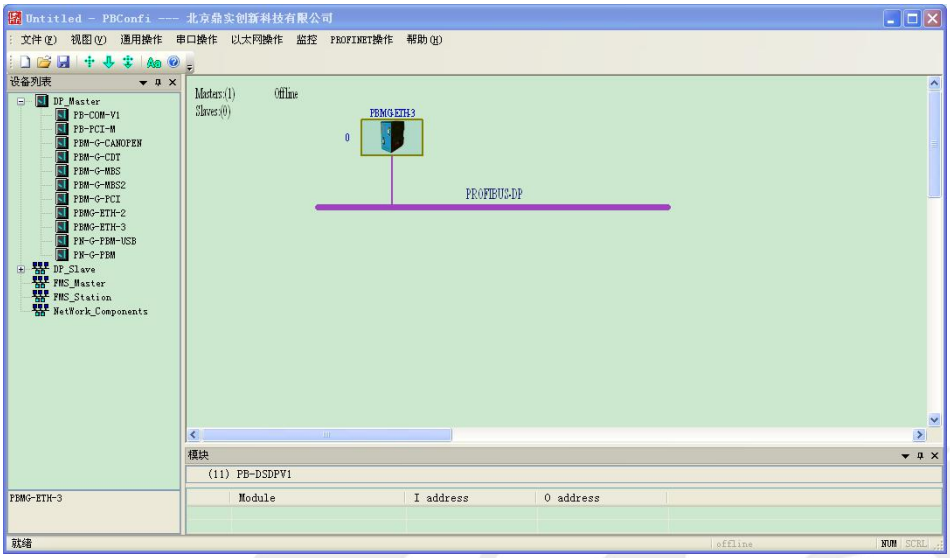


图 6-4 添加主站

双击界面中主站图标，会弹出 PROFIBUS 主站相关属性定义窗口，可以对主站地址，总线波特率等相关信息进行定义。

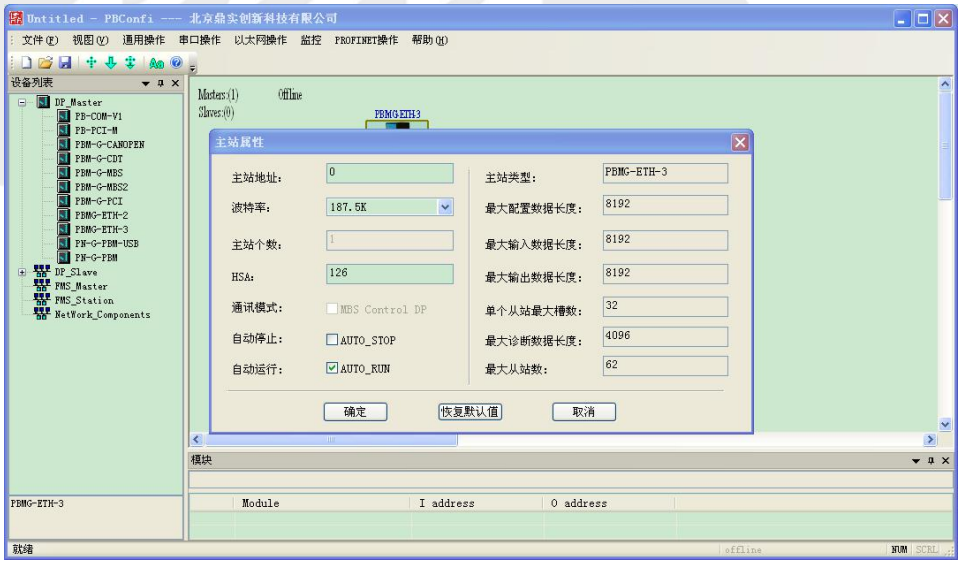


图 6-5 主站属性设定

表 6-2 主站工作模式

设置项名称	功能
自动停止 AUTO STOP	若使能，当有配置了的 DP 从站不在数据交换状态，主站自动切换到 STOP 状态，不管是否使能 AUTO RUN 功能，此时在 STOP 模式下拒绝用户手动切换到 RUN 状态的操作。之后若所有从站都回到数据交换状态，如果未使能 AUTO RUN 功能，主站会维持在 STOP 状态，需要用户手动切换到 RUN 状态，如果使能 AUTO_RUN 功能，主站会自动回到 RUN 状态。
自动运行 AUTO RUN	若使能，主站上电自动运行到 RUN 状态。若禁止，主站上电运行到 STOP 状态。需要用户手动切换到 RUN 状态。当同时开启 AUTO STOP 和 AUTO RUN 功能，AUTO STOP 优先级更高，有配置了的从站不在数据交换状态，主站运行在 STOP 状态，当所有从站都回到数据交换状态，主站自动回到 RUN 状态。使能 AUTO RUN 主站工作在 RUN 状态时，若用户手动将主站切换到 STOP 状态，主站会维持在 STOP 状态 50ms，之后又自动跳回到 RUN 状态。

1.4 添加从站

点击软件界面右侧的硬件设备栏，点击“DP-Slave” →“gateway”，双击在下拉菜单中所选中从站 PB-DSPBV1 就可以将其添加到界面中。

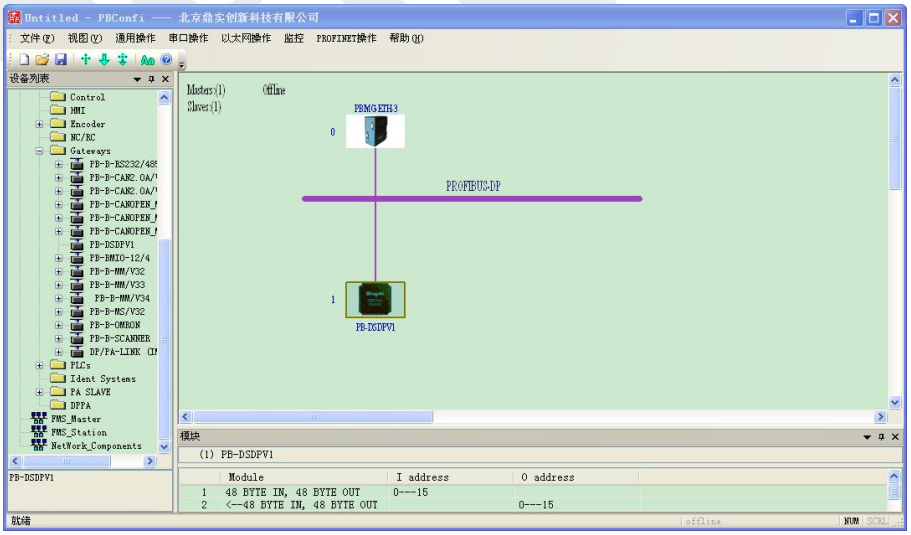


图 6-6 从站添加

双击界面中的从站图标，从弹出的窗口中可以对从站站地址，用户参数，是否支持 WD 看门狗等相关信息进行配置。

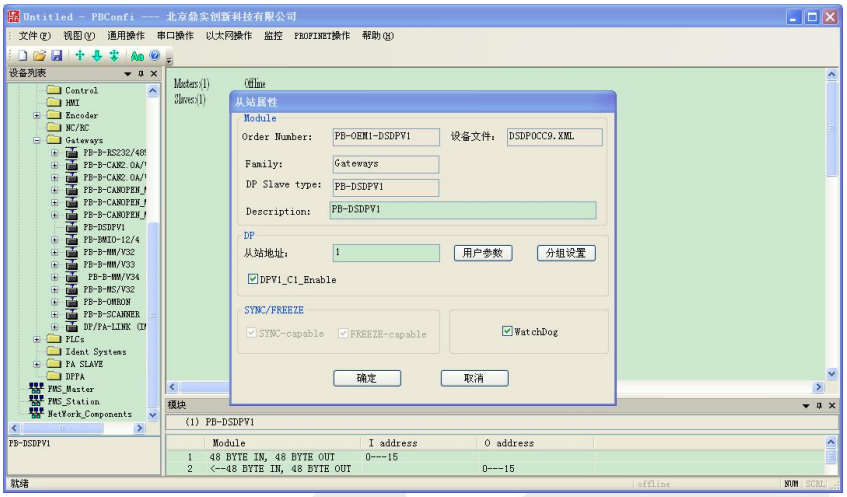


图 6-7 从站属性

◆ 配置 PROFIBUS DPV1 功能

对于支持 DPV1 功能的从站（GSD 文件中包含描述 DPV1_Slave= 1），在从站属性窗口中默认 DPV1_Enable 选项是勾选的，如果不打算使用该从站的 DPV1C1/C2 功能，可以不选择 DPV1_Enable 勾选项（有些 DPV1 从站这样设置可能会导致 DPV0 不通）。对于不支持 DPV1 功能的从站，DPV1_Enalbe 勾选项默认是不选中且无法设置的状态。

◆ 设置 Watchdog

从站可用看门狗（ Watchdog）监测总线通信，以确认主站处于工作状态，过程数据值依然被更新。通过参数报文从站获得一个用于看门狗的时间值。如果由于总线繁忙而导致从站不能重新触发看门狗，从站状态跳转至 Wait_Prm 状态并将输出设置为安全状态。安全状态依应用而不同，且不能被指定。

◆ 设置从站用户参数

从站的用户参数大多不相同。有的从站的用户参数是无法修改的，有的从站提供可以选择的用户参数。

◆ 同步冻结、分组设置

同步模式下，所编址的从站输出数据锁定在当前状态下。在这之后的用户数据传输周期中，从站存储接收到输出的数据，但它的输出状态保持不变；当接收到下一同步命令时，所存储的输出数据才发送到外围设备上。用户可通过非同步命令退出同步模式。

冻结模式将从站的输入数据锁定在当前状态下，直到主站发送下一个冻结命令时才可以

更新。用户可以通过非冻结命令退出锁定模式。

同步或冻结操作通过向主站特定一个或多个组发送标准 DP 广播报文来实现。标准共定义 8 个组，用广播报文中一个字节的每个位来表示一个组。使用同步冻结功能要在 PRFIBUS 系统配置阶段分别定义 8 个组的功能，之后再将各个从站可选地加入到相应的组中。

PBM-ETH-3.0 支持 PRFIBUS 标准中的同步冻结功能，设置方法如下。

先在“分组设置”窗口的“分组信息”标签中定义每个组的功能，任意一个组都可以设置为同步组，冻结组，同步冻结组，禁止几种方式。

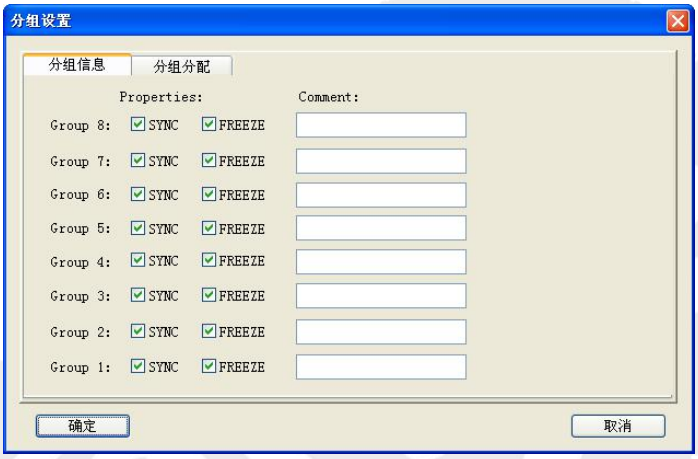


图 6-8 分组信息

再在分组分配标签下将从站加入到组中。可能的添加方式为加入同步组，加入冻结组，加入同步冻结组，不加入任何组。从站只允许加入到在“分组信息”标签中设置使能了的组。

图 6-9 分组分配

1.5 设置总线参数

双击总线，出现下图，有时隙时间，Gap，Retry 得到 Tid，Ttr，WD 时间。

图 6-10 总线参数

- Tslot_Init 决定主站给从站发送报文后等待从站应答的超时时间（tbit） 。
- Max.Tsdr 用来结算 Watchdog 时间和 Ttr。
- Gap 是决定每隔多少个 Token 发送一次 FDL 报文 。
- Retry 就是报文重发次数

1.6 设置软件连接的IP地址

“以太网操作”->“访问参数设置

使用 PB-confi 时，需要将软件的访问 IP 设置成与端口 IP 一致。（默认软件的连接 IP 为 192.168.1.10。PBM-ETH-3.0 的默认 IP 分别为: ETH1 是 192.168.1.10; ETH2 是 192.168.2.10）

图 6-11 访问参数设置

1.7 配置下载

点击菜单中的“通用操作”→“编译并下载”，或者直接点击工具栏中的“编译并下载”按钮，就可以将现有配置通过网口下载到网关中。

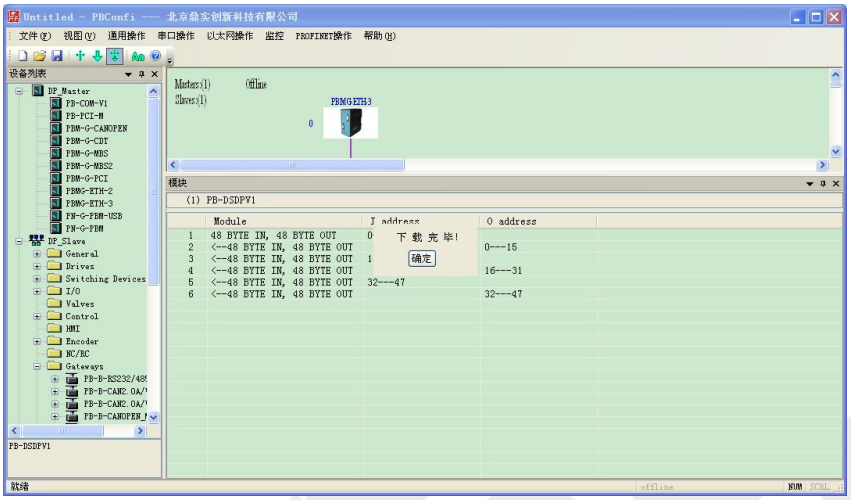


图 6-12 下载完毕

1.8 配置PBM-ETH-3.0网络参数

“以太网操作”→“网络参数设置”，选择模式和修改 IP 地址。下载完成后，将 SW1 拨到 OFF，重新给模块上电后，新模式和新 IP 生效。

图 6-13 修改网络配置

注：在双网口模式，两个网口的 IP 地址不能配置在一个网段。

主站网关的交换机工作模式

主站网关在交换机工作模式下对外呈现一个网络接口，一个 IP 地址，两个 RJ45 可认为是交换机的两个端口。通过两个网络接口都可以与主站网关进行通信。交换机工作模式还可用来组建菊花链型网络。

主站网关的双网口工作模式

主站网关在交换机工作模式下对外呈现两个独立的网络接口，两个 IP 地址，且不能在同一网段。两个网络接口分别接入不同的网段。交换机工作模式可用来组建独立冗余双网。

1.9 保存以及加载PBM-ETH-3.0的配置文件

点击菜单中的“文件”→“保存”，给文件命名后，点击保存，如下图所示。

图 6-14 保存配置

2. 通过PB-Confi进行在线调试

操作方法：通用操作→设备操作。设备操作窗口用来查看设备基本信息，修正网关系统时间，监控网关运行环境，设置网关设备名称和设备描述。

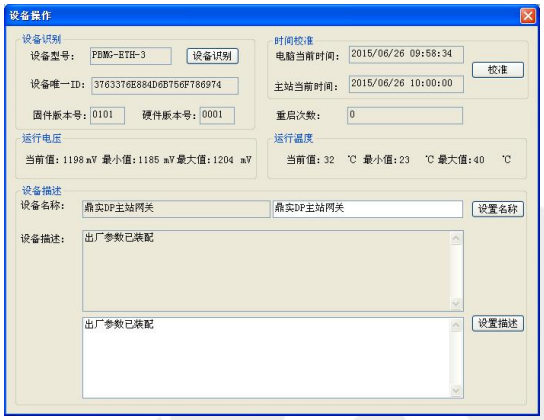


图 6-15 设备操作

2.1 主站网关的主站操作

操作方法：通用操作→主站操作。该窗口可监控主站运行状态，设置主站参数，控制主站工作模式等。

图 6-16 主站操作

通过“RUN”，“STOP”按钮切换主站的 RUN/STOP 状态。

2.2 主站网关的从站操作（DPV1的操作）

操作方法：通用操作→从站操作。该窗口显示从站工作状态，诊断信息，对 DPV1 的操作。

图 6-17 从站操作

2.3 监控主站网关所连从站的状态

获取主站和各个从站的运行状态，不论这些从站是否被配置，都可以获得到它们的状态。点击“监控→启动”可见如下界面。

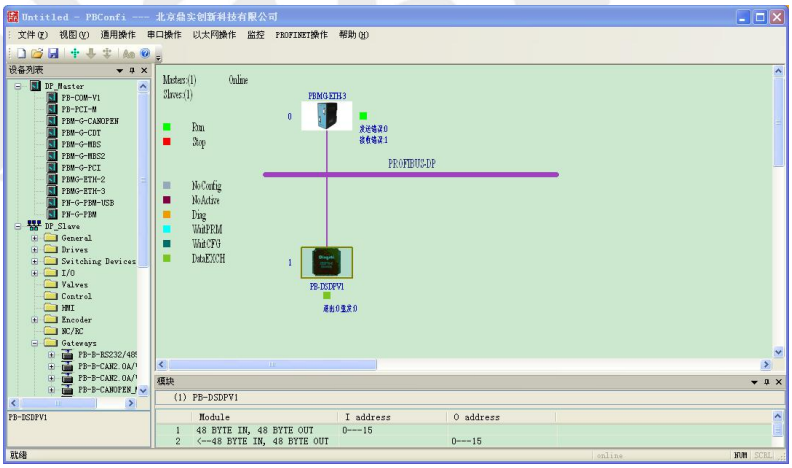


图 6-18 监控

通过不同的色块图标可知主站和从站的运行状态。主站图标下包含发送报文错误次数和接收报文错误次数，从站图标下包含对该从站的重发报文次数和该从站退出数据交换次数。

2.4 PROFIBUS DPV0 IO数据通信

操作方法：通用操作→IO 数据映射/在线监控。

图 6-19 在线监控

选择要监控的从站，相应从站站号前多了个“*”，且“当前从站:”指示当前选择的从站，点击“启动监测”或将该从站的输入数据和输出数据消失在 PB-Input 和 PB-Output 数据区中，选择 PB-Output 数据区中的数据，修改并点击“数据下发”可将修改的数据下发给相应的从站。

2.5 导出当前系统所有主站网关及从站状态

操作：通用操作→总线运行报告。

导出当前当前网关的设备状态，主站状态，及其所连从站的状态。

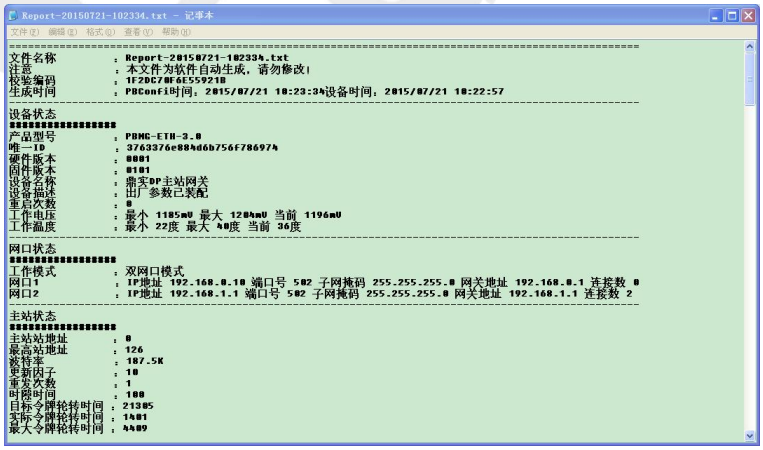


图 6-20 总线运行报告

2.6 更改从站地址（特殊从站）

有些 DP 从站不提供拨码开关设置站地址，而是通过设置站地址报文来为其设置从站地址。通常这些从站的出厂默认地址为 125，设置的站地址从站会保存在自身的非易失性存储中，下次上电设置的站地址不会丢失。PB-Confi 软件支持设置从站地址功能。

操作方法：通用操作-→设置从站地址

图 6-21 从站地址更

2.7 查看系统日志

通过 PB-Confi 可以查看系统日志。“通用操作→网关系统日志”可见以下窗口。

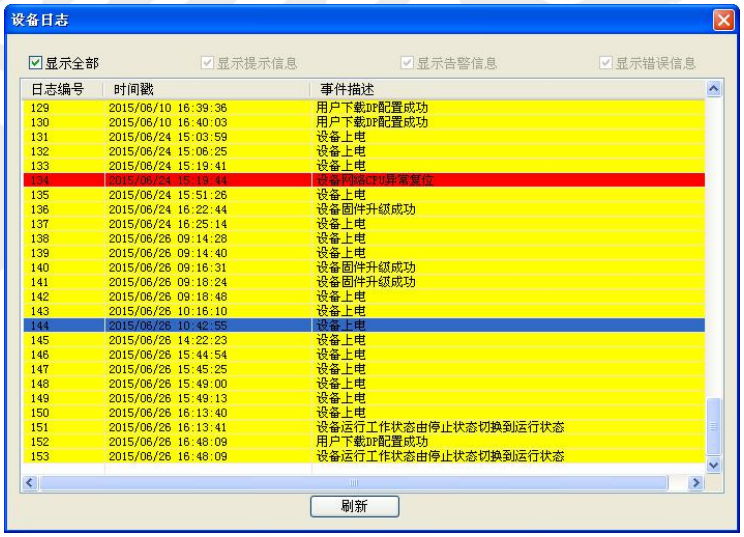


图 6-22 系统日志

日志条目过滤功能。

事件 ID 小于 0x0013 称为关键事件，这些事件会被保存在网关的非易失性存储中，掉电不会丢失。网关最多可同时存储 256 条系统日志，当系统日志条目数超过 256 时，最新的日志条目会覆盖最早的日志条目。

3. 固件升级

为及时修复网关内部的软件缺陷或对产品功能进行升级，PBM-ETH-3.0 提供通过以太网进行固件升级的功能。

使用固件升级功能，要求主站网关运行在固件升级模式。通过拨码开关“固件升级”位 SW3 设置到固件升级模式(SW3=1)，对主站网关重新上电。若以太网链路连通，则 SYS 指示器会由红色常亮状态切换为绿色常亮状态，否则 SYS 指示器保持红色常亮状态直到以太网链路连通。

运行 PB-Confi 软件，通过菜单“通用操作”→“固件升级”打开固件升级窗口，下拉菜单选择欲升级的固件版本，点击“升级”按钮启动固件升级。进度条持续前进表明固件升级正在进行中。

固件升级过程中 SYS 指示灯处于绿色闪烁状态，升级成功配置软件进度条完成，并给出提示，同时 SYS 指示灯为绿色常亮。升级结束后将拨码开关拨回到正常工作模式，并对设备重新上电。

若固件升级成功，设备会以最新固件启动运行，SYS 指示灯为绿色常亮状态。因为某些原因（关闭 PB-Confi 软件，网线脱落，网关断电等原因）导致固件升级失败，切换回正常模式启动后，SYS 指示灯为红色闪烁状态，表明工作固件启动失败。此时需要回到固件升级模式重新更新设备固件。

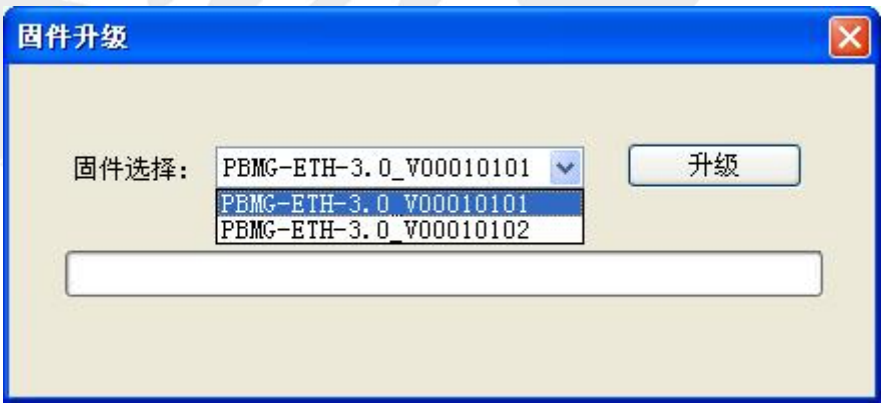


图 6-23 固件升级

第七章 实现 PROFIBUS-DP 从站的监控

本章主要介绍 MODBUS/TCP 的客户端如何通过主站网关 PBM-ETH-3.0 来实现对 PROFIBUS-DP 从站的监控。由前几章，我们可以知道这一切是通过对 modbus 寄存器读写来实现的。我们首先需要了解 modbus 的数据区，PBM-ETH-3.0 的 modbus 数据区的含义如下表所示。

表 6-1 modbus 数据区

MODBUS 数据区	数据名称	操作属性	功能码	数据功能
MODBUS 三区	输入寄存器	只读	0x04:读输入寄存器	● PROFIBUS DPV0 输入数据 ● PROFIBUS DPV1 读数据 ● PROFIBUS 从站诊断数据 ● 主站网关系统日志数据 ● 主站网关状态寄存器
MODBUS 四区	保持寄存器	可读可写	0x03:读保持寄存器 0x06:写单寄存器 0x10:写多寄存器	● PROFIBUS DPV0 输出数据 ● PROFIBUS DPV1 写数据 ● 主站网关控制寄存器

1. 输入寄存器数据区

MODBUS 三区的数据区分为 DPV0 输入数据区，DPV1 应答数据区，DP 诊断数据区，系统日志数据区，网关状态寄存器区。每次 MODBUS 读请求只能访问一个数据区，不能跨区访问。PBM-ETH-3.0 的 MODBUS 三区数据地址功能如表所示。

表 6-2 三区数据地址功能

类型	名称	地址	长度（字）	说明
DPV0 输入数据区	DPV0_IDATA	0x0000~0x0FFF (0~4095)	4k	PROFIBUS DPV0 输入数据
DPV1C1 应答数据区	DPV1_C1RSP	0x2000~0x207F (8192~8319)	128	PROFIBUS DPV1C1 请求应答报文
DPV1C2 应答数据区	DPV1_C2RSP	0x3000~0x307F (12288~12415)	128	PROFIBUS DPV1C2 请求应答报文
DP 诊断数据区	SLAVE_DIAGRSP	0x4000~0x407F (16384~16511)	128	PROFIBUS DIAG 数据
系统日志数据区	SYSLOG	0x5000~0x55FF (20480~22015)	1280	系统日志数据，最多存储 256 条日志信息

表 6-3 系统状态寄存器区(一)

类型	名称	地址	长度（字）	说明
系统状态寄存器区(一)		0x8000 (32768)	1	产品 ID，取值为 0x06FA
		0x8001 (32769)	6	设备唯一 ID，每台设备具有唯一的 ID
		0x8007 (32775)	1	硬件版本号
		0x8008 (32776)	1	固件版本号，高字节为主版本号，低字节次版本号
		0x8009 (32777)	1	系统状态寄存器*
		0x800A (32778)	1	系统重启次数寄存器，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。
		0x800B (32779)	1	系统日志区中系统日志条目数
		Reserved		
		0x8015 (32789)	1	本次上电过程中设备供电电压当前值，以 mV 为单位
		0x8016 (32790)	1	本次上电过程中设备供电电压最小值，以 mV 为单位
		0x8017 (32791)	1	本次上电过程中设备供电电压最大值，以 mV 为单位
		0x8018 (32792)	1	本次上电过程中设备工作温度当前值的补码，以摄氏度为单位
		0x8019 (32793)	1	本次上电过程中设备工作温度最小值的补码，以摄氏度为单位
		0x801A (32794)	1	本次上电过程中设备工作温度最大值的补码，以摄氏度为单位
		Reserved		
		0x801F (32799)	1	当前配置的 CRC 校验值
		0x8020 (32800)	2	主站网关网络接口 1 用户配置 IP 地址。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节

表 6-4 系统状态寄存器区(二）

类型	名称	地址	长度（字）	说明
系统状态寄存器区(二）		0x8022 (32802)	2	主站网关网络接口 1 用户配置子网掩码。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节
		0x8024 (32804)	2	主站网关网络接口 1 用户配置默认网关地址。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节
		0x8026 (32806)	1	主站网关网络接口 1 用户配置 MODBUS/TCP 服务端口号
		0x8027 (32807)	1	主站网关网络接口 1 TCP 连接数
		0x8028 (32808)	2	主站网关网络接口 2 用户配置 IP 地址。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节
		0x802A (32810)	2	主站网关网络接口 2 用户配置子网掩码。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节
		0x802C (32812)	2	主站网关网络接口 2 用户配置默认网关地址。首字的高字节对应网络地址的最低字节，尾字的低字节对应网络地址的最高字节
		0x802E (32814)	1	主站网关网络接口 2 用户配置 MODBUS/TCP 服务端口号
		0x802F (32815)	1	主站网关网络接口 2 TCP 连接数
		Reserved		

表 6-5 主站状态寄存器区

类型	名称	地址	长度（字）	说明
主站状态寄存器区		0x8040 (32832)	1	主站站地址及最高站地址，低字节为最高站地址，高字节为主站站地址
		0x8041 (32833)	1	主站波特率。取值含义为：1:9.6k, 2:19.2k, 3:45.45k, 4:93.75k, 5:187,5k 6:500k, 7:1.5M, 8:3M, 9:6M
		0x8042 (32834)	1	GAPG 及 RETRY，高字节为 GAP（每多少个 Token 发送一次 FDL 报文），低字节为重发次数。
		0x8043 (32835)	1	主站时隙时间
		0x8044 (32836)	1	主站目标令牌轮转时间高字
		0x8045 (32837)	1	主站目标令牌轮转时间低字
		Reserved		
		0x8047 (32839)	1	主站自动模式寄存器*
		0x8048 (32840)	1	主站配置寄存器*
		0x8049 (32841)	1	主站配置状态寄存器*
		0x804A (32842)	1	主站实际令牌轮转时间高字
		0x804B (32843)	1	主站实际令牌轮转时间低字
		0x804C (32844)	1	主站最大令牌轮转时间高字（最大令牌轮转时间不能超过 Ttr）
		0x804D (32845)	1	主站最大令牌轮转时间低字（最大令牌轮转时间不能超过 Ttr）
		Reserved		
		0x8051 (32849)	1	**主站发送 DP 报文错误计数器**，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。
		0x8052 (32850)	1	**主站接收 DP 报文错误计数器**，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。

表 6-6 从站状态寄存器区

类型	名称	地址	长度(字)	说明
		Reserved		
从站状态寄存器区		0x805B (32859)	1	从站配置数目寄存器
		0x805C (32860)	1	设置从站站地址状态寄存器
		0x805D (32861)	1	从站 0 状态寄存器*
		……		
		0x80DA (32986)	1	从站 125 状态寄存器
		0x80DB (32987)	1	从站 0 退出数据交换次数寄存器，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。
		……		
		0x8158 (33112)	1	从站 125 退出数据交换次数寄存器，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。
		0x8159 (33113)	1	从站 0 重发次数统计寄存器，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。
		……		
		0x81D6 (33238)	1	从站 125 重发次数统计寄存器，最高位为溢出位，bit14~0 为计数位，若计数溢出，则溢出位一直为 1。

注意：

（1） 以上地址为 MODBUS 报文中的数据地址，从 0 开始寻址，若利用 ModScan 工具，填写的地址为上面的地址加 1。

（2） 带“ * ”号的具体含义参见本章 8 PBM-ETH-3.0 Modbus 寄存器区位功能定义详述

2. 保持寄存器数据区

MODBUS 四区的数据区分为 DPV0 输出数据区，DPV1 请求数据区，控制寄存器区。

每次 Modbus 请求只能访问一个数据区，不能跨区访问。PBM-ETH-3.0 的 Modbus 四区数据地址功能如表所示。

表 6-7 四区数据地址功能

类型	名称	地址	长度（字）	说明
DPV0 输出数据区	DPV0_ODATA	0x0000~ 0x0FFF(0~4095)	4k	PROFIBUS DPV0 输出数据
DPV1C1 请求数据区	DPV1_C1REQ	0x2000~ 0x207F (8192~8319)	128	PROFIBUS DPV1C1 请求报文
DPV1C2 请求数据区	DPV1_C2REQ	0x3000~ 0x307F (12288~12415)	128	PROFIBUS DPV1C2 请求报文
系统控制寄存器区	RUNTIME_YEAR	0x8000 (32768)	1	设备运行时间年*
	RUNTIME_MONDAY	0x8001 (32769)	1	设备运行时间月日*
	RUNTIME_HOURMIN	0x8002 (32770)	1	设备运行时间时分*
	RUNTIME_MSEC	0x8003 (32771)	1	设备运行时间毫秒*
	DEVICE_CTRL	0x8004(32772)	1	设备控制寄存器，bit2 为 1 开启设备识别，SYS 指示灯为绿色闪烁状态，bit2 为 0 关闭设备识别。
		Reserved		
	DEVICE_NAME	0x8010~0x802F (32784~32815)	32	设备名称，写入后掉电不丢失
	DEVICE_DESCRIP	0x8030~0x80AF (32816~32943)	128	设备描述，写入后掉电不丢失

表 6-8 控制寄存器区

类型	名称	地址	长度（字）	说明
主站控制寄存器区	MASTER_OPCTRL	0x80B0 (32944)	1	主站状态机寄存器*
		Reserved		
	MASTER_C2RSPTOUT	0x80B2 (32946)	1	主站 DPV1C2 响应超时时间寄存器。写入后掉电不丢失。该寄存器和合法取值范围为 100~3000。对应实际超时时间为该值*10ms。该寄存器的取值应比 C2 从站 GSD 文件中的 C2_Response_Timeout 属性值要大
	MASTER_COMCNTCLR	0x80B3 (32947)	1	主站通信计数清除寄存器*
		Reserved		
从站控制寄存器区	SLAVE_SYNFRZCTRL	0x80C0 (32960)	1	从站同步冻结控制寄存器*
	SLAVE_COMCNTCLR	0x80C1 (32961)	1	从站通信计数清除寄存器*
	SLAVE_SETSADDR_ADDR	0x80C2 (32962)	1	设置从站站地址寄存器，高字节为从站当前地址，低字节为从站目标地址
	SLAVE_SETSADDR_IDNUM	0x80C3 (32963)	1	设置从站站地址 Ident Number 寄存器
	SLAVE_SETSADDR_NOCHG	0x80C4 (32964)	1	设置是否允许再次变更从站站地址寄存器，为 0 表示允许再次变更，非零表示不允许再次变更

注意：

（1） 以上地址为 MODBUS 报文中的数据地址，从 0 开始寻址，若利用 ModScan 工具，填写的地址为上面的地址加 1。

（3） 带“ * ”号的具体含义参见本章 8 PBM-ETH-3.0 Modbus 寄存器区位功能定义详述。

3. PBM-ETH-3.0 MODBUS通信应答返回码

网关对来自客户端的 MODBUS/TCP 访问请求进行判断，若服务请求有错误或网关无法完成该服务请求会利用 MODBUS 应答返回相应的错误码。网关可能返回的错误码及其含义如下表所示。

表 6-9 应答码值

MODBUS 应答码名称	应答码值	含义
MBSRET_INVALIDFC	0x01	非法的 MODBUS 功能码
MBSRET_OFFSETERR	0x02	非法的数据地址
MBSRET_VALUEERR	0x03	非法的数据值
MBSRET_AREA_INVALID	0x10	MODBUS 访问区域无效
MBSRET_AREA_CROSS	0x11	重叠访问两个 MODBUS 功能区
MBSRET_SERVIC_BUSY	0x12	设备服务忙
MBSRET_SETTIME_FAIL	0x20	设置主站系统时间失败
MBSRET_GETLOG_FAIL	0x21	获取系统日志失败
MBSRET_USRCONF_ERR	0x40	主站用户配置错误
MBSRET_NOTPMASTER_ER R	0x41	当前主站不是工作 P 主站
MBSRET_REDUSW_FAIL	0x42	冗余主站切换错误
MBSRET_RUNSTOPSW_FAIL	0x43	主站 RUN/STOP 切换失败
MBSRET_HIGH_DIAG	0x60	从站高优先级报警
MBSRET_SLAVE_OFFLINE	0x61	访问的从站掉线（主站向其发送 SD2 报文无应答）
MBSRET_SLAVE_NDEX	0x62	访问的从站不在数据交换状态
MBSRET_V0_UNREADY	0x63	访问的从站 DPV0 数据未就绪
MBSRET_SYNFRZ_FAIL	0x64	从站同步冻结操作失败
MBSRET_V1_FAIL	0x65	从站 DPV1 操作请求失败
MBSRET_V1_UNREADY	0x66	从站 DPV1 应答未就绪
MBSRET_V1_NOTSUPP	0x67	从站不支持 DPV1 功能
MBSRET_SETSADDR_FAIL	0x68	设置从站站地址失败

4. PBM-ETH-3.0 Modbus DPV0数据区操作

MODBUS/TCP 客户端通过读取主站网关 Modbus 三区的 DPV0 输入数据，可以获得从站设备的 DPV0 输入数据。通过写主站网关 Modbus 四区的 DPV0 输出数据，可以更新从站设备的 DPV0 输出数据。

4.1 DPV0 读数据操作

本处仅以表格形式说明 PROFIBUS DPV0 输入数据在 MODBUS 数据区的中映射方式，具体的地址映射关系则由 PB-Confi 配置软件生成的地址映射表提供。

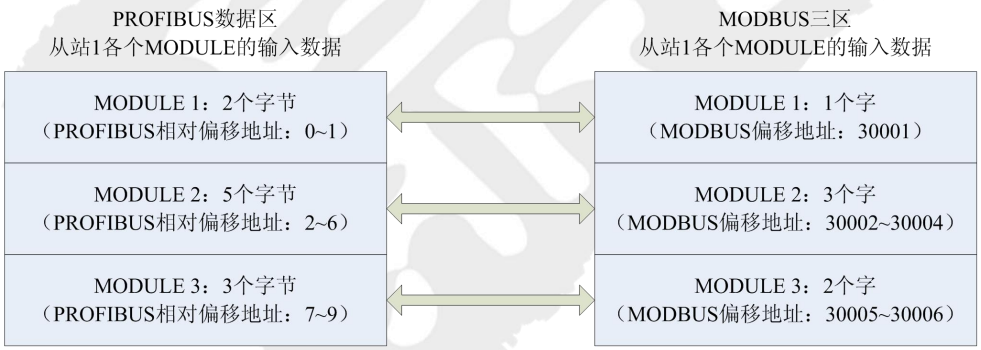
表 6-10 地址映射表

相对偏移地址（字）	类型	数据说明	附加说明
0000	配置从站 1 的 DPV0 输入数据	本从站 Module 1 的输入数据	从站设备通常包含一个或多个 module，因此从站设备的 DPV0 输入数据也由多个 Module 的输入数据组成。 当 Module 数据的长度为奇数时，MODBUS 数据区中此 Module 输入数据的最后一个字： ● 高字节为有效输入数据； ● 低字节为零。
……		本从站 Module 2 的输入数据	
……		……	
n		本从站 Module x 的输入数据	
n + 0001	配置从站 2 的 DPV0 输入数据	本从站 Module 1 的输入数据	
……		本从站 Module 2 的输入数据	
……		……	
m		本从站 Module x 的输入数据	
m + 0001	配置从站 3 的 DPV0 输入数据	……	

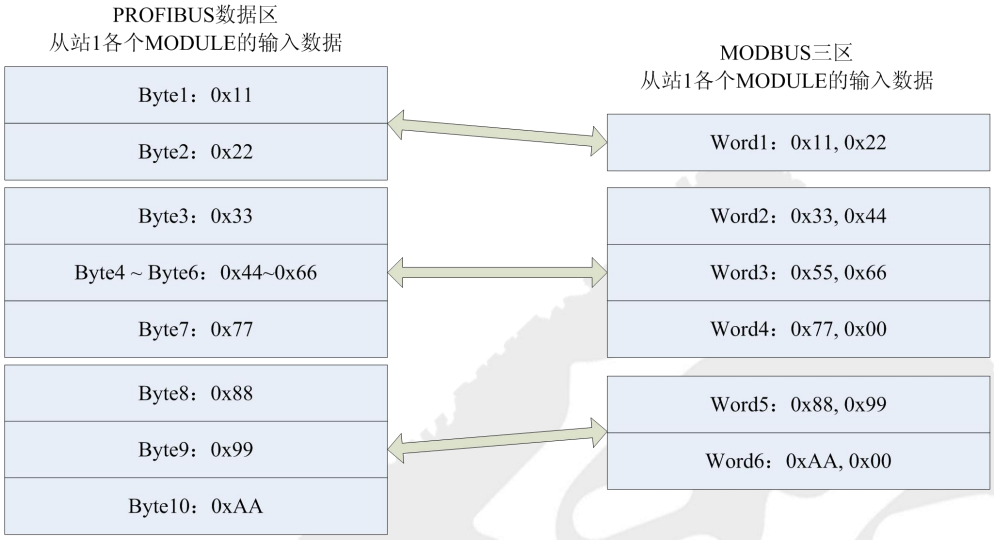
从站设备可能由一个或多个 Module 组成，下图简单介绍了从站各个 Module 的输入数据在 PROFIBUS 数据区与 MODBUS 三区中的映射关系。

【eg】从站 1 共有 10 个字节的输入数据，从站由三个 Module 组成，分别含有 2 个字节、5 个字节和 3 个字节。

- Module 1 带有 2 个字节的输入数据，在 PROFIBUS 数据区的相对偏移地址为 0~1 两个字节，在 MODBUS 三区的地址为 30001 一个字；
- Module 2 带有 5 个字节的输入数据，在 PROFIBUS 数据区的相对偏移地址为 2~6 五个字节，在 MODBUS 三区的地址为 30002~30004 三个字；
- Module 3 带有 3 个字节的输入数据，在 PROFIBUS 数据区的相对偏移地址为 7~9 三个字节，在 MODBUS 三区的地址为 30005~30006 两个字；



下图说明了各个 Module 内的数据在 PROFIBUS 数据区与 MODBUS 数据区内的映射关系。



MODBUS/TCP 客户端进行 PROFIBUS DPV0 数据读操作可能的应答信息如下所示。

- 正常数据响应
- MBSRET_AREA_CROSS
- MBSRET_USRCONF_ERR
- MBSRET_NOTPMASTER_ERR
- MBSRET_HIGH_DIAG
- MBSRET_SLAVE_NDEX
- MBSRET_SLAVE_DURDY

4.2 DPV0 写数据操作

用户可以通过写 MODBUS 四区修改 DPV0 输出数据。

在规定的地址范围内，用户每次MODBUS写四区请求的偏移地址与写入长度没有限制，可以一次写一个或多个从站的输出数据。起始偏移地址不需要是某个从站的 MODBUS 起始地址。

在主从 DP 通信正常，从站已经进入数据交换状态的情况下，用户向 MODBUS 四区写入的 DPV0 输出数据是否生效受主站网关工作状态与是否为 P 主站的影响。

仅在主站 RUN 状态下，用户向 MODBUS 四区写入的数据会成为有效输出数据。

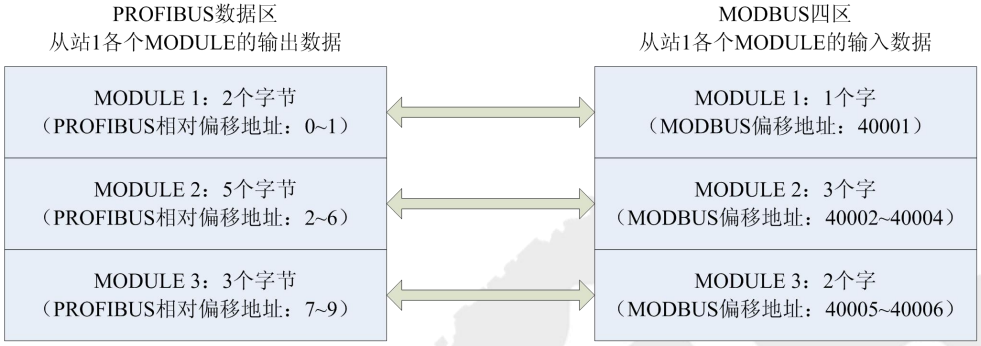
本文档仅以表格形式说明 PROFIBUS DPV0 输出数据在 MODBUS 数据区的中映射方式，具体的地址映射关系则由 PB-Confi 配置软件生成的配置下载文件提供。

表 6-11 相对偏移地址

相对偏移地址（字）	类型	数据说明	附加说明
0000	配置从站 1 的 DPV0 输出数据	本从站 Module 1 的输出数据	从站设备通常包含一个或多个 module，因此从站设备的 DPV0 输出数据也由多个 Module 的输出数据组成。 当 Module 数据的长度为奇数时，MODBUS 数据区中此 Module 输入数据的最后一个字： ● 高字节为有效输入数据； ● 低字节为零。
……		本从站 Module 2 的输出数据	
……		……	
n		本从站 Module x 的输出数据	
n + 0001	配置从站 2 的 DPV0 输出数据	本从站 Module 1 的输出数据	
……		本从站 Module 2 的输出数据	
……		……	
m		本从站 Module y 的输出数据	
m + 0001	配置从站 3 的 DPV0 输出数据	……	

从站设备可能由一个或多个 Module 组成，下图简单介绍了从站各个 Module 的输出数据在 PROFIBUS 数据区与 MODBUS 四区中的映射关系。

由于输出数据的数据映射方式与输入数据一致，在此不再细述。



MODBUS/TCP 客户端进行 PROFIBUS DPV0 数据读操作可能的应答信息如下所示。

- 正常数据响应
- MBSRET_AREA_CROSS
- MBSRET_USRCONF_ERR
- MBSRET_HIGH_DIAG
- MBSRET_SLAVE_NDEX
- MBSRET_SLAVE_DURDY

5. PBM-ETH-3.0 Modbus DPV1数据区操作

主站网关支持 DPV1C1 和 DPV1C2 主站功能。用户通过写主站网关 Modbus 四区中的 DPV1 请求数据区发起 DPV1 请求。**仅能通过写入 DPV1 请求数据区首地址 0x2000 开始的区域才能发起 DPV1 请求操作**，主站网关在收到 DPV1 请求后会向相应从站设备发送 DPV1 请求。

由于 DPV1 通信为非循环通信，主站网关将在数个总线周期后才能获得有效的从站响应。主站网关收到从站的 DPV1 响应后会将其放到 Modbus 三区的 DPV1 应答数据区。用户通过读取 Modbus 三区的 DPV1 应答数据区来查询应答是否到来及获取应答数据。**仅能通过读取 DPV1 应答数据区首地址 0x2000 开始的区域才能获取 DPV1 应答数据，主站网关会将上一次 DPV1 请求的应答结果返回给用户。**

与从站的 DPV1 通信仅在主站工作于 RUN 状态。用户每次只能对一个从站的一个槽-索引进行操作，且在本次读操作确定成功/失败之前，拒绝进行其它 DPV1 服务请求。

对于 DPV1C1 操作还要求相应从站处于数据交换状态。因此仅能与主站配置了的，参数化报文中使能 DPV1 功能，且处于数据交换状态的从站进行 DPV1C1 通信。

而对于 DPV1C2 通信，则可以与当前总线让任何支持 DPV1C2 的从站进行通信，即便该从站不是网关站配置的从站。

5.1 DPV1C1 的读写请求及响应报文的含义

主站网关在 MODBUS 四区中的 DPV1 请求数据区支持的 DPV1C1 请求报文及其可能的响应报文的格式如下表所示。

表 6-12 DPV1C1 的读写请求及响应报文

<table>
<tr><th>操作类型</th><th>请求报文</th><th>请求报文可能返回的 Modbus 异常码</th><th>应答报文</th></tr>
<tr><td rowspan="2">Read（对 DPV1C1 从站的特定槽索引进行读操作）</td><td rowspan="2">● OPTIONID（2 字节）
● SLAVE_ADDR:RSV
● FUNC_NUM(0x5E):SLOT
● INDEX:LENGTH</td><td rowspan="4">MBSRET_V1_FAIL：
DPV1 服务请求操作失败。
MBSRET_V1_BUSY：
主站网关 DPV1 服务请求忙。
MBSRET_V1_NOTSUPP：
请求的从站不支持或未使能 DPV1 功能。</td><td>● OPTIONID（2 字节）
● SLAVE_ADDR: RSV
● FUNC_NUM(0x5E):SLOT
● INDEX:LENGTH
● DATA
……（DATA 字段用 0 补齐为偶数字节）</td></tr>
<tr><td>● OPTIONID（2 字节）
● SLAVE_ADDR: RSV
● FUNC_NUM(0xDE):ERR_DECODE
● ERR_CODE1:ERR_CODE2
● REQ_RESULT（2 字节）</td></tr>
<tr><td rowspan="2">Write（对 DPV1C1 从站的特定槽索引进行写操作）</td><td rowspan="2">● OPTIONID（2 字节）
● SLAVE_ADDR: RSV
● FUNC_NUM(0x5F):SLOT
● INDEX:LENGTH
● DATA
……
（DATA 字段若为奇数字节长，最后一个字节为位于 MBS 字单元的高字节，低字节值任意）</td><td>● OPTIONID（2 字节）
● SLAVE_ADDR: RSV
● FUNC_NUM(0x5F):SLOT
● INDEX:LENGTH</td></tr>
<tr><td>● OPTIONID
● SLAVE_ADDR: RSV
● FUNC_NUM(0xDF):ERR_DECODE
● ERR_CODE1:ERR_CODE2
● REQ_RESULT（2 字节）</td></tr>
</table>

其中各个字段的含义如下。

表 6-13 DPV1C1 字段含义

字段名称	字段含义
OPTIONID	DPV1 服务请求操作 ID，为区分每次 DPV1 操作，建议用户在每次 DPV1 服务操作后将该字段值加 1，初值为 0。DPV1 服务响应报文中该字段的值与服务请求报文中该字段的值一致。
RSV	保留字段
SLAVE_ADDR	DPV1 操作的从站地址
DPV1_CLASS	DPV1 操作类别，1 表示 DPV1C1 操作。
FUNC_NUM	DPV1 操作功能号，0x5E 为 DPV1C1 读，0x5F 为 DPV1C1 写。若响应报文中该字段为 0 表明从站的 DPV1C1 应答尚未到来。
SLOT	DPV1 操作从站槽号。
INDEX	DPV1 操作从站索引号。
LENGTH	DPV1 操作数据长度，以字节为单位。
DATA	DPV1 操作数据字段。
ERR_DECODE ERR_CODE1 ERR_CODE2	DPV1 操作错误编码
REQ_RESULT	主站网关返回的 DPV1 操作请求异常结果。 0x0000: 未检测到错误。 0x0001: 本次 DPV1 服务请求因超时未获得响应（poll 有应答，但未获得服务响应） 0x0002: DPV1 报文应答超时（请求或 poll 报文无响应） 0x0003: DPV1 应答帧错误 0x0004:DPV1C2 连接已关闭 0x0005:操作从站未处于数据交换状态而导致 DPV1C1 通信失败 0x0006:主站未处于 RUN 状态 0x0007:主站未处于 P 主站状态

5.2 DPV1C1 的读写请求报文案例

DPV1C1 通过 MBS 数据区进行读写请求及获取应答的报文示例如下所示。

表 6-14 DPV1C1 的读写请求报文案例

报文名称	报文格式
对站地址为 7 的从站的槽 0 索引 1 进行 240 字节的 DPV1C1 读操作	
DPV1C1 读请求	00 00 00 00 00 0F 00 **10 20 00 00 04 08 00 01 07 00 5E 00 01 F0**
对站地址为 7 的从站的槽 1 索引 2 进行 30 字节的 DPV1C1 写操作	
DPV1C1 写请求	00 00 00 00 00 2D 00 **10 20 00 00 13 26 00 01 07 00 5F 01 02 1E 01 01 00 00 CD CC 8C 3F 00 00 B0 40 E6 00 00 00 00 00 C8 42 E6 00 00 05 00 00 BE 42 B8 0B**
读取 MODBUS 三区 DPV1C1 应答数据区 32 字节长度	
DPV1C1 获取应答	00 00 00 00 00 06 00 **04 20 00 00 10**

5.3 DPV1C2 的读写请求及响应报文的含义

主站网关在 MODBUS 四区中的 DPV1 请求数据区支持的 DPV1C2 请求报文及其可能的响应报文的格式如下表所示。

表 6-15 DPV1C2 从站 Initiate 报文

报文类型	报文格式	可能的应答报文格式
Initiate (与特定 DPV1C2 从站建立连接)	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x57):RSV1 ● RSV2:RSV3 ● RSV4: RSV5 ● FEATURE_SUPT1:FEATURE_SUPT2 ● PROFILE_FEATURE_SUPT1: PROFILE_FEATURE_SUPT2 ● PROFILE_ID_NUM（2 字节） ● S_TYPE:SLEN ● D_TYPE:DLEN ● S_API:S_SCL ● S_NETADDR:S_MACADDR ● D_API:D_SCL ● D_NETADDR:D_MACADDR	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x57):MAX_LEN_DUNT ● FEATURE_SUPT1:FEATURE_SUPT2 ● PROFILE_FEATURE_SUPT1: PROFILE_FEATURE_SUPT2 ● PROFILE_ID_NUM（2 字节） ● S_TYPE:SLEN ● D_TYPE:DLEN ● S_API:S_SCL ● S_NETADDR:S_MACADDR ● D_API:D_SCL ● D_NETADDR:D_MACADDR
		● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0xD7):ERR_DECODE ● ERR_CODE1:ERR_CODE2 ● REQ_RESULT（2 字节）
		● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0xD8):LOCAL_GENERATE ● SUBNET:INSTANCE_REASON_CODE ● ABORT_DETAIREQ_RESULT（2 字节）

表 6-16 DPV1C2 从站 Read 报文

报文类型	报文格式	可能的应答报文格式
Read（对 DPV1C2 从站的特定槽索引进行读操作）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x5E):SLOT ● INDEX:LENGTH	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x5E):SLOT ● INDEX:LENGTH ● DATA ……（DATA 用 0 补齐为偶数字节
		● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0xDE):ERR_DECODE ● ERR_CODE1:ERR_CODE2 ● REQ_RESULT（2 字节）
Write（对 DPV1C2 从站的特定槽索引进行写操作）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x5F):SLOT ● INDEX:LENGTH ● DATA ……（DATA 用 0 补齐为偶数字节）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x5F):SLOT ● INDEX:LENGTH
		● OPTIONID（2 字节） ● RSV1: RSV ● FUNC_NUM(0xDF):ERR_DECODE ● ERR_CODE1:ERR_CODE2 ● REQ_RESULT（2 字节）
Trans（对 DPV1C2 从站的特定槽索引进行数据传输操作）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x51):SLOT ● INDEX:LENGTH ● DATA ……（DATA 用 0 补齐为偶数字节）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x51):SLOT ● INDEX:LENGTH ● DATA ……（DATA 用 0 补齐为偶数字节）
		● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0xD1):ERR_DECODE ● ERR_CODE1:ERR_CODE2 ● REQ_RESULT（2 字节）
Abort (与特定 DPV1C2 从站关闭连接)	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x58):SUBNET(0x00) ● INSTANCE_REASON_CODE(0x20):0x00	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x58/0xD8):LOCAL_GENERATE ● SUBNET:INSTANCE_REASON_CODE ● ABORT_DETAIL ● REQ_RESULT（2 字节）
Reset（复位 DPV1C2 主站状态机）	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x61): 0x00 ● 0x00:0x00	● OPTIONID（2 字节） ● SLAVE_ADDR: RSV ● FUNC_NUM(0x0x61):0x00 ● REQ_RESULT（2 字节）

其中各个字段的含义基本与 DPV1C1 一致，不一致的字段如下。

表 6-17 DPV1C1 **字段名称**

字段名称	字段含义
RSV1~5	保留字段，取值任意。
FUNC_NUM	DPV1 操作功能号，0x57 为 DPV1C2 建立连接，0x51 为 DPV1C2 数据传输，0x58 为 DPV1C2 关闭连接，0x61 为 DPV1C2 复位主站状态机。若响应报文中该字段为 0 表明从站的 DPV1C1 应答尚未到来。
SADDR	DPV1 操作目标从站站地址。
DPV1_CLASS	DPV1 操作类别， 2 表示 DPV1C2 操作。
LOCAL_GENERATE	主站自身检测到的错误该字段置 1，否则置 0
ABORT_DETAIL	非 0 表示 C2 从站的 RM 应答报文中的 Send Timeout 时间值
……	

5.4 DPV1C2 的读写请求报文案例

DPV1C1 通过 MODBUS 数据区对站地址为 7 的从站进行读写请求及获取应答的报文示例如下所示。

表 6-18 DPV1C2 的读写请求报文案例

报文名称	报文格式
DPV1C2 连接请求	00 00 00 00 00 23 00 **10 20 00 00 0E 1C 00 01 07 00 57 00 00 00 00 00 00 00 00 00 00 00 00 02 00 02 00 00 00 00 00 00 00 00**
DPV1C2 读请求	00 00 00 00 00 0F 00 **10 20 00 00 04 08 00 01 07 00 5E 00 01 F0**
DPV1C2 写请求	00 00 00 00 00 2D 00 **10 20 00 00 13 26 00 01 07 00 5F 01 02 1E *01 01 00 00 CD CC 8C 3F 00 00 B0 40 E6 00 00 00 00 00 C8 42 E6 00 00 05 00 00 BE 42 B8 0B***
DPV1C2 数据传输请求	00 00 00 00 00 2D 00 **10 20 00 00 13 26 00 01 07 00 51 04 01 1E *01 01 00 00 CD CC 8C 3F 00 00 B0 40 E6 00 00 00 00 00 C8 42 E6 00 00 05 00 00 BE 42 B8 0B***
DPV1C2 关闭请求	00 00 00 00 00 0F 00 **10 20 00 00 04 08 00 01 07 00 58 00 20 00**
DPV1C2 复位请求	00 00 00 00 00 0F 00 **10 20 00 00 04 08 00 01 07 00 61 00 00 00**
DPV1C2 获取应答	00 00 00 00 00 06 00 04 20 00 00 10

5.5 DPV1C2 的异步事件

在 DPV1C2 状态机运行过程中，主站会监测到一些通信异常状况，主站网关通过异步事件发向 MODBUS 的 DPV1 应答数据区，异步事件的格式如下所示。

表 6-19 异步事件格式

异步事件名称	字段含义
Reject	● OPTIONID(0x0000)（2 字节） ● SLAVE_ADDR:RSV ● FUNC_NUM(0xF1):REASON_CODE ● REQ_RESULT（2 字节）
Abort	● OPTIONID（2 字节） ● SLAVE_ADDR:RSV ● FUNC_NUM(0x58/0xD8):LOCAL_GENERATE ● SUBNET:INSTANCE_REASON_CODE ● ABORT_DETAIL ● REQ_RESULT（2 字节）

Reject 异步事件中 REASON_CODE 字段取值含义如下表

表 6-20 REASON_CODE 字段取值含义

字段名称	字段取值	字段含义
REJ_LE	0x09	Max_Len_Data_Unit overflow
REJ_PS	0x0A	number of parallel service requests exceeded

Abort 异步事件中 SUBNET 字段取值含义如下表所示：

表 6-21 SUBNET 字段取值含义

字段名称	字段取值	字段含义
SUBNET_NO	0	没有子网
SUBNET_LOCAL	1	本地子网
SUBNET_REMOTE	2	远端子网
SUBNET_FALSE	3	子网信息错误

通过 INSTANCE_REASON_CODE 字段返回主站网关监测到的异步事件。INSTANCE_REASON_CODE 字段取值含义如下表所示：

表 6-22 INSTANCE_REASON_CODE 字段取值含义

字段名称	字段取值	字段含义
事件源 Bit[7:4]	INSTANCE_DLL 0x10	数据链路层
	INSTANCE_MS2 0x20	DPV1C2 主站层
	INSTANCE_USER 0x30	用户层
事件码 Bit[3:0] 当故障源 Bit[7:4]为 INSTANCE_DLL 时	UE 1	Remote-DMPM / DL interface error
	RR 2	Resources of the remote-DL Entity not sufficient or not available
	RS 3	Service or remote-address at remote-DLSAP or remote-DLSAP not activated - remote-station is no DP -Station - remote-station is not yet ready for these Service - remote-station is associated with an other Requester - optional service not available
	NR 9	No Response data
	DH 10	Positive acknowledgement for sent data, reply data with high priority available
	RDL 12	Response data low and no resource for sent data
	RDH 13	Response data high and no resource for sent data
	NA 15	Negative ack, no reaction from remote station
故障码 Bit[3:0] 当故障源 Bit[7:4]为 INSTANCE_MS2 时	ABT_SE(=1)	sequence error
	ABT_FE(=2)	invalid request APDU received
	ABT_TO(=3)	connection timed out
	ABT_RE(=4)	invalid response APDU received
	ABT_IV(=5)	invalid service from the User
	ABT_STO(=6)	**requested value of Send_Timeout was too short**
	ABT_IA(=7)	invalid additional address information
	ABT_OC(=8)	S-Timer expired, response APDU has not been sent yet

5.6 利用主站网关的 DTM 使用 DPV1C2 功能

主站网关 MODBUS 接口提供的 DPV1C2 功能的设计原则主要是考虑配合 DTM 使用，而且 DPV1C2 使用之前不需要通过 PB-Confi 进行配置，所有的设置都通过 DTM 来完成。DTM 通过主站网关的 MODBUS 接口中的 DPV1 数据区使用 DPV1C2 功能。（DTM 使用可参见第八章）

6. PBM-ETH-3.0 Modbus DP从站诊断数据区操作

MODBUS 三区中每个从站诊断数据的格式

用户通过读取 MODBUS 三区诊断数据区获取其配置的所有 DP 从站的诊断数据及其发生时间戳，设置 MODBUS 报文的单元标识符（MODBUS/TCP 报文的第七个字节）为要获取诊断数据的从站地址，**读取 MODBUS 数据区获取从站诊断数据时读取数据的起始地址必须为 DP 诊断数据区首地址 0x4000**。每个从站的诊断数据在其相应区域中的数据结构如表所示。

表 6-23 诊断数据的数据结构

相对偏移地址(字)	数据功能
0x00	诊断数据时戳年
0x01	诊断数据时戳月日，月为第一字节，日为第二字节
0x02	诊断数据时戳时分，时为第一字节，分为第二字节
0x03	诊断数据时戳毫秒
0x04	实际诊断数据长度，以字节为单位
0x05	实际诊断数据首字
……	……
	实际诊断数据尾字，若为单字节，高字节有效，低字节为零

在从站诊断数据结构中，诊断数据时间戳表明主站接收到从站诊断应答报文的时间，由于从站实际回复的诊断数据长度可能小于最大诊断数据长度，实际诊断数据长度字段反应诊断数据结构中实际有效诊断数据的长度。若用户读取诊断数据长度超过从站返回的实际诊断数据长度，超出部分的数据无效。

7. PBM-ETH-3.0 Modbus系统日志区操作

为了便于进行系统故障分析，PBM-ETH-3.0 支持系统日志功能，通过系统日志功能可以记录系统运行过程中的关键事件。用户通过 MODBUS 三区的日志数据区可以读取到日志事件。**读取 MODBUS 数据区获取从站诊断数据时读取数据的起始地址必须为 DP 诊断数据区首地址 0x5000**。

系统日志事件分关键日志事件和非关键日志事件。PBM-ETH-3.0 会将关键日志事件写入非易失性存储，掉电之后也能保存，便于进行设备维护。

系统日志格式

MODBUS 三区系统日志区共 3kB，每条日志条目占 10 字节，最多可存储 256 条日志信息。非易失性存储中最多可掉电保存 256 条关键日志事件。每个日志条目的数据格式如下：

表 6-24 日志条目的数据格

相对偏移地址（字）	内容
0x00	日志条目时戳年
0x01	日志条目时戳月日，在 MODBUS 报文中月字节在前，日字节在后
0x02	日志条目时戳时分，在 MODBUS 报文中小时字节在前，分钟字节在后
0x03	日志条目时戳毫秒，在 MODBUS 报文中毫秒的高字节在前，低字节在后
0x04	日志条目 ID，在 MODBUS 报文中日志条目 ID 高字节在前

其中日志时戳占 8 个字节，格式为“年：月日：时分：毫秒”，表示记录的该系统事件的发生时间，时间基准为 PBM-ETH-3.0 内部的时间。

若希望采用绝对时间进行系统事件的记录，用户需要在 PBM-ETH-3.0 每次上电时通过 MODBUS 四区的系统时间寄存器来设置 PBM-ETH-3.0 的系统时间。

日志条目 ID 表示记录的日志事件的类型，占 2 个字节，每种事件类型都有唯一的 ID 值。通过“系统日志区中系统日志条目数”寄存器可以获取当前日志区的日志条目数。

系统日志 ID

目前 PBM-ETH-3.0 支持的系统事件 ID 如表所示。

表 6-25 系统日志 ID

日志事件 ID 名称	日志事件 ID 值	日志事件描述
SYSLOG_SYS_PWRUP	0x0001	设备上电
SYSLOG_SYS_PBMWTGRESET	0x0002	DP 主站 CPU 看门狗重启
SYSLOG_SYS_ETHWTGRESET	0x0003	网络 CPU 看门狗重启
SYSLOG_SYS_PBMCPUEXCEPT	0x0006	主站 CPU 异常复位
SYSLOG_SYS_ETHCPUEXCEPT	0x0007	网络 CPU 异常复位
SYSLOG_SYS_TEMPUPLIMIT	0x0008	设备环境温度超上限
SYSLOG_SYS_TEMPLOWLIMIT	0x0009	设备环境温度超下限
SYSLOG_SYS_VOLTUPLIMIT	0x000A	设备工作电压超上限
SYSLOG_SYS_VOLTLOWLIMIT	0x000B	设备工作电压超下限
SYSLOG_SYS_ETH1IPCRASH	0x000E	网络接口 1 IP 地址冲突
SYSLOG_SYS_ETH2IPCRASH	0x000F	网络接口 2 IP 地址冲突
SYSLOG_SYS_USRLOADCONFOK	0x0010	用户下载配置成功
SYSLOG_SYS_USRLOADCONFERR	0x0011	用户下载配置失败
SYSLOG_SYS_FIRMWAREUPDATEOK	0x0012	设备固件升级成功
SYSLOG_SYS_FIRMWAREUPDATEERR	0x0013	设备固件升级失败
前面的日志事件为关键日志事件，事件发生时会被写入非易失性存储，掉电不丢失。		
SYSLOG_SYS_ETH1CONNECOFF	0x0021	网络接口 1 网络连接断开
SYSLOG_SYS_ETH2CONNECOFF	0x0022	网络接口 2 网络连接断开
SYSLOG_MASTER_P2IDLE	0x0040	设备冗余工作状态由主用状态切换到空闲状态
SYSLOG_MASTER_B2IDLE	0x0041	设备冗余工作状态由备用状态切换到空闲状态
SYSLOG_MASTER_P2B	0x0042	设备冗余工作状态由主用状态切换到备用状态
SYSLOG_MASTER_B2P	0x0043	设备冗余工作状态由备用状态切换到主用状态
SYSLOG_MASTER_IDLE2B	0x0044	设备冗余工作状态由空闲状态切换到备用状态
SYSLOG_MASTER_STOP2RUN	0x0045	设备运行工作状态由停止状态切换到运行状态
SYSLOG_MASTER_RUN2STOP	0x0046	设备运行工作状态由运行状态切换到停止状态
SYSLOG_SLAVE0_LEAVDEXCH	0x0060	站地址为 0 的从站退出数据交换状态
……		
SYSLOG_SLAVE125_LEAVDEXCH	0x00DD	站地址为 125 的从站退出数据交换状态
SYSLOG_SLAVE0_HALARM	0x00DE	站地址为 0 的从站产生高优先级报警
……		
SYSLOG_SLAVE125_HALARM	0x015B	站地址为 125 的从站产生高优先级报警

其中对系统日志区的读操作不要求必须以日志条目的整数倍进行读取，读取的首地址也不要求必须是日志条目的首地址。若读取日志数据长度超过当前日志条目总长度，以 0 补齐长度进行应答。

8. PBM-ETH-3.0 Modbus寄存器区位功能定义详述

系统状态寄存器 输入寄存器 0x8009(32777)

表 6-26 系统状态寄存器

位编号	名称	功能
Bit3	TOO_HIGH_TEMP	为 1 表示工作温度过高
Bit2	TOO_LOW_TEMP	为 1 表示工作温度过低
Bit1	TOO_HIGH_VLT	为 1 表示工作电压过高
Bit0	TOO_LOW_VLT	为 1 表示工作电压过低

主站状态机寄存器操作 保持寄存器 0x80B0 (32944)

读状态含义为：

表 6-27 主站状态机寄存器读状态含义

位编号	名称	功能
Bit2:0	主站运行状态	001：主站处于离线状态 010：主站处于配置状态 011：主站处于停止（STOP）状态 100：主站处于运行（RUN）状态

写操作含义为：

表 6-28 主站状态机寄存器读状态含义

位编号	名称	功能
Bit2:0	主站运行控制	001：无效 010：无效 011：将主站置为停止（STOP）状态 100：将主站置为运行（RUN）状态

从站状态寄存器操作 输入寄存器 0x805D(32861)~0x80DA(32986)表示从站 0 到从站 125 的状态

每个站地址的从站都有唯一的从站状态寄存器。寄存器格式如下：

表 6-29 从站状态寄存器

位编号	名称	功能
Bit15	SLAVE_WITHINCONF	为 1 表示当前配置包含该从站
Bit14	SLAVE_ONLINE	从站在线（活动从站，FDL 报文有应答）
Bit13~12	SLAVE_FSMSTATE	从站状态机状态 00：诊断状态 01：参数化状态 10：配置状态 11：数据交换状态
Bit11	WTG1MS_ENABLE	从站使用 1ms 而非 10ms 的 Watchdog 时基
Bit10	DEXCH_HALARM	数据交换应答从站产生高优先级报警
Bit9	DIAGRESP_NOTSUPPORT	诊断应答从站不支持配置的某些功能
Bit8	DIAGRESP_STATIONNTRDY	诊断应答从站未就绪
Bit7	DIAGRESP_PARAMCONFERR	诊断应答从站参数或配置错误
Bit6	DIAGRESP_NEEDPARAM	诊断应答从站需要参数化
Bit5	DIAGRESP_EXTERNDIAGN	诊断应答扩展诊断有效
Bit4	DIAGRESP_STATICDIAGN	诊断应答静态诊断有效
Bit3	DIAGRESP_SLAVELOCKED	诊断应答从站已被其它主站锁定
Bit2	DIAGRESP_INVALIDMADDR	诊断应答主站地址错误
Bit1	DIAGRESP_INVALIDSID	诊断应答从站 ID 错误
Bit0	DIAGRESP_LENOVERRUN	诊断应答长度超限

系统控制寄存器操作 保持寄存器

系统控制寄存器目前提供的功能如表所示。

表 6-30 系统控制寄存器

系统控制寄存器功能	操作方式
修正系统时间 **0x8000~0x8003** **(32768~32771)**	系统时间年，月日，时分，毫秒四个字段每个字段占一个字，可一起或单独对每个字段进行时间修正。小时字段为 24 小时计时制。
设置设备名称 **0x8010~0x802F** **(32784~32815)**	64 字节掉电不丢失的数据存储区，为系统中主站网关定义设备名称。
设置设备描述 **0x8030~0x80AF** **(32816~32943）**	256 字节掉电不丢失的数据存储区，为系统中主站网关建立设备在系统中的描述信息。

主站通信计数清除寄存器 保持寄存器 0x80B3 (32947)

表 6-31 主站通信计数清除寄存器

位编号	名称	功能
Bit1	COMCNTCLR_TX	为 1 表示主站接收错误计数器清零
Bit0	COMCNTCLR_RX	为 1 表示主站发送错误计数器清零

主站自动模式寄存器　输入寄存器 0x8047(32839)

表 6-32 主站自动模式寄存器

位编号	名称	功能
Bit1	AUTO_RUN	为 1 表示网关上电自动进入 RUN 状态
Bit0	AUTO_STOP	为 1 表示网关使能自动停止功能，当由配置的从站不在数据交换状态时，主站自动切换到安全输出状态。

主站配置寄存器 输入寄存器 0x8048(32840)

表 6-33 主站配置寄存器

位编号	名称	功能
Bit3	CONFCTRL_PREPM	为 1 表示网关为优选 P 主站，非冗余模式下，该位恒定为 1
Bit2	CONFCTRL_REDUN	为 1 表示双机冗余工作模式，否则为非冗余工作模式。

主站配置状态寄存器 输入寄存器 0x8049(32841)

表 6-34 主站配置状态寄存器

位编号	名称	功能
Bit3:2	CONFSTAT	00:配置主站未完成 01:配置主站失败 10:配置主站成功

设置从站站地址状态寄存器 输入寄存器 0x805C(32860）

表 6-35 从站站地址状态寄存器

位编号	名称	功能
Bit1:0	SET_SADDR_RSLT	00:设置从站站地址未就绪 01:设置从站站地址成功 10:设置从站站地址响应超时 11: 设置从站站地址被拒绝

从站同步冻结控制寄存器 保持寄存器 0x80C0 (32960）

表 6-36 从站同步冻结控制寄存器

位编号	名称	功能
Bit11	SYNC_ENABLE	为 1 表示同步使能
Bit10	SYNC_DISABLE	为 1 表示同步禁止
Bit9	FREEZE_ENABLE	为 1 表示冻结使能
Bit8	FREEZE_DISABLE	为 1 表示冻结禁止
Bit7:0	GROUP_NUM	同步冻结的分组组号

表 6-36

从站通信计数清除寄存器 保持寄存器 0x80C1 (32961)

表 6-37 从站通信计数清除寄存器

位编号	名称	功能
Bit1	COMCNTCLR_LEAVDEXC	为 1 表示清除从站退出数据交换次数统计
Bit0	COMCNTCLR_RETRY	为 1 表示清除针对从站的重发次数统计

第八章 基于 FDT/DTM 框架的 PA 通信实例

本章以主站网关 PBM-ETH-3.0 连接 PA 设备为具体实例，讲解了如何使用配置软件 PB-Confi 完成带有 PA 设备的网络配置，以及如何在 FDT 框架中使用主站网关的网关 DTM 和通信 DTM。

在本实例中，使用的第三方设备与软件如下所示：

- 使用的 DP/PA 耦合器：西门子 DP/PA Coupler（物理层耦合器）
- 使用的 PA 设备：ABB PA 仪表 2020TG
- 使用的 FDT 框架程序：P+F 开放 FDT 框架程序 PACTware（V4.1）

1、主站网关 PBM-ETH-3.0 的 PA 与 DTM 功能简介

1.1 关于 PA 连接

主站网关 PBM-ETH-3.0 支持 PROFIBUS PA 通信。

通过 DP/PA 耦合器的连接，主站网关 PBM-ETH-3.0 可以与 PA 设备进行正常的 DPV0/V1 通信。

PA 设备配置方式：通过鼎实软件 PB-Confi（V3.8）配置 PA 设备，配置方法见下文。

1.2 关于 DTM 通信

北京鼎实为主站网关 PBM-ETH-3.0 配备了以下两种 DTM，供客户在不同的场合下应用。

- 通信 DTM：PBMGETHCOMMDTMSetup.exe
- 网关 DTM：PBMGETHGWDTMSetup.exe

1.3 关于使用 DTM 触发主站网关 DPV1 通信

在本文档上文技术指标中已说明，主站网关支持 DPV1 中的 DPC1/C2 通信，用户通过访问 MODBUS 四区首地址 0x2000 区域发起 DPV1 请求操作。

在实际应用中，主站网关的 DPV1 通信通常由以下方式触发：

- 由 MODBUS TCP 客户端，如上位控制器，发起 MODBUS TCP 请求，主站网关接收到相关 MODBUS TCP 请求后，发起 DPV1 通信；
- 在设备管理系统中，如 FDT/DTM，EDD 上位软件，点击 PA 设备的设备描述/管理文件，发起设备数据读写请求。此数据读写请求在实际硬件通信网络系统中，转化为 MODBUS TCP 客户端的以太网读写请求发送给主站网关，继而由主站网关发起 DPV1 通信；

本实例中，使用了 FDT/DTM 框架系统，其通信数据流如下图所示：

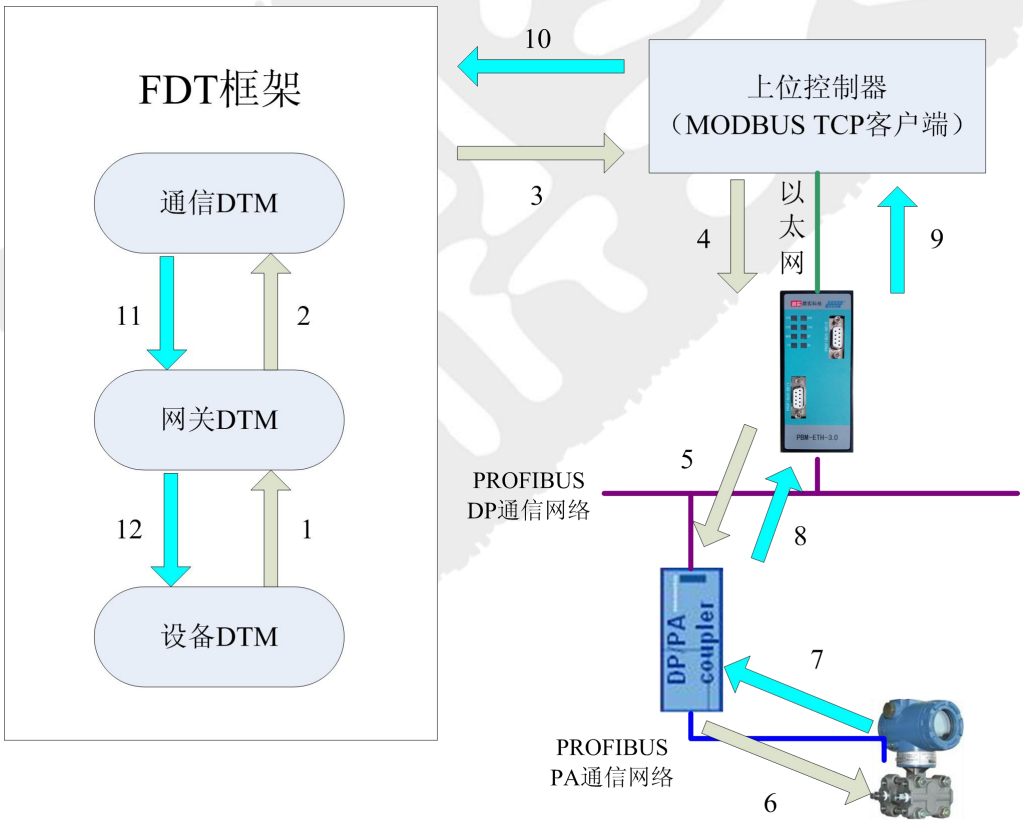


图 8-1 FDT/DTM 框架系统数据流图

2、实例系统与相关软件

本主站网关 PBM-ETH-3.0 连接 PA 设备的实例中，下文的表格中详细列出了使用的实验设备与上位软件。

实例中使用的设备如下表所示：

表 8-1 硬件设备表

实验设备	数量	制造商	说明
PBM-ETH-3.0	1	鼎实	以太网转 DP 主站网关
DP/PA Coupler	1	西门子	DP/PA 纯物理层耦合器
Transmitter 2020TG	1	ABB	ABB 传感器（PROFIBUS PA）
DP 电缆	1	西门子	
PA 电缆	1	西门子	
PC 机+软件			带有 FDT 框架程序，PB-Confi 配置软件，MODBUS TCP 客户端软件的 PC 机做上位控制使用

具体的使用软件和安装文件有：

表 8-2 PC 软件表

软件	制造商	说明
PBMGETHCOMMDTMSetup.exe	鼎实	主站网关通信 DTM
PBMGETHGWDTMSetup.exe		主站网关网关 DTM
PB-Confi		主站网关配置软件
3KXP000265S0005_DTM_2600T	ABB	PA 设备 2020TG 的设备 DTM
YP0004C2.GSD	ABB	PA 设备 2020TG 的 GSD
DSMODBUSTCPCommDTMSetup.exe	鼎实	通用 MODBUS TCP 通信 DTM
PACTware（V4.1）	P+F	开放式 FDT 框架上位软件

3、PA 配置

使用主站网关 PBM-ETH-3.0 连接 PA 设备，其配置依然使用 PB-Confi 配置软件完成。当使用西门子 DP/PA 耦合器时，其配置过程如下图所示。

配置 PBM-ETH-3.0 主站网关，在 DP_Master 列表中选中 PBMG-ETH-3 配置入 DP 网络。在 PA_SLAVE 列表中选中相应的 PA 设备，双击配置入 DP 网络。因选用的为纯物理层耦合，无需对 DP/PA 耦合器进行配置。

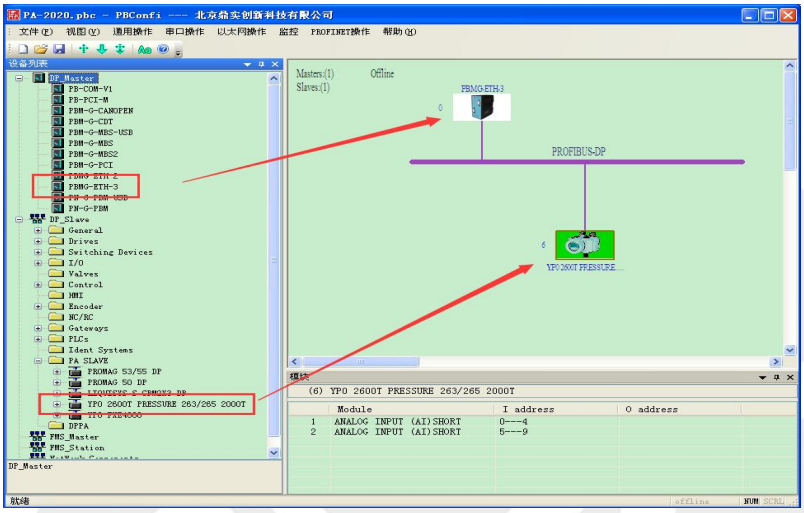


图 8-2 配置图

因使用 DP/PA 耦合器（纯物理层耦合），将主站网关的波特率属性改为 45.45K。

图 8-3 波特率设置

将此配置下载到主站网关，主站网关 PBM-ETH-3.0 即可以和已硬件连接好的 PA 设备进行通信。

4、PROFIBUS PA 通信中的 DTM 应用

本实例中以 FDT/DTM 系统作为设备管理上位，由 DTM 为源发起 PROFIBUS 通信网络中的 DPV1 通信，与 PA 设备进行通信，并将

FDT 框架程序选用开放软件 PACTware，由于北京鼎实提供两种主站网关 DTM：通信 DTM 与网关 DTM，故 DTM 应用有以下两种方式可选。

——方案一：主站网关通信 DTM + PA 设备 DTM；

——方案二：MODBUS TCP 通信 DTM + 主站网关网关 DTM + PA 设备 DTM；

4.1 方案一：主站网关通信 DTM + 设备 DTM

步骤 1：点击各 DTM 的 EXE 安装文件，把所有 DTM 文件安装到电脑中。

步骤 2：打开上位 FDT 框架程序，在本实例中为 PACTware 框架，在此 FDT 框架程序中按照实际通信网络，配置网络拓扑结构。

如下图中选中“主机 PC”，点击右键，在弹出的菜单中选取“添加设备”。在弹中的设备窗口中选中主站网关的通信 DTM“DS DPV1 CommDTM”，点击将其配置入 FDT 框架程序。

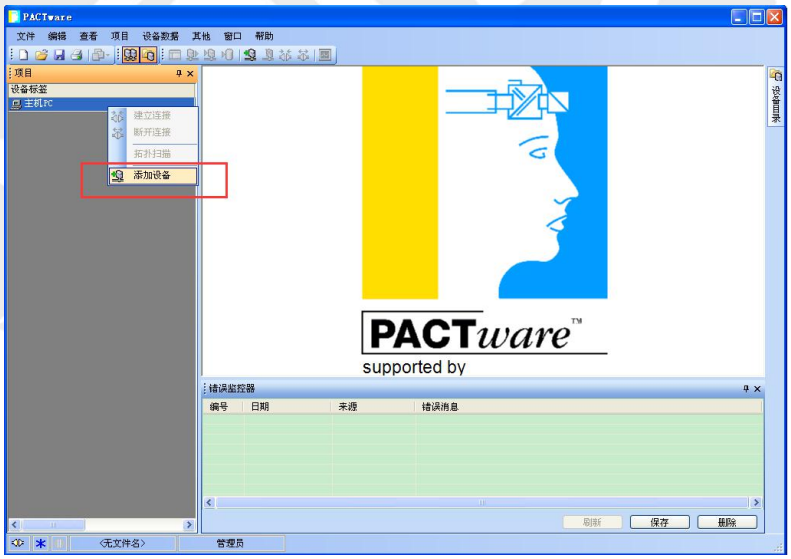


图 8-4 添加设备

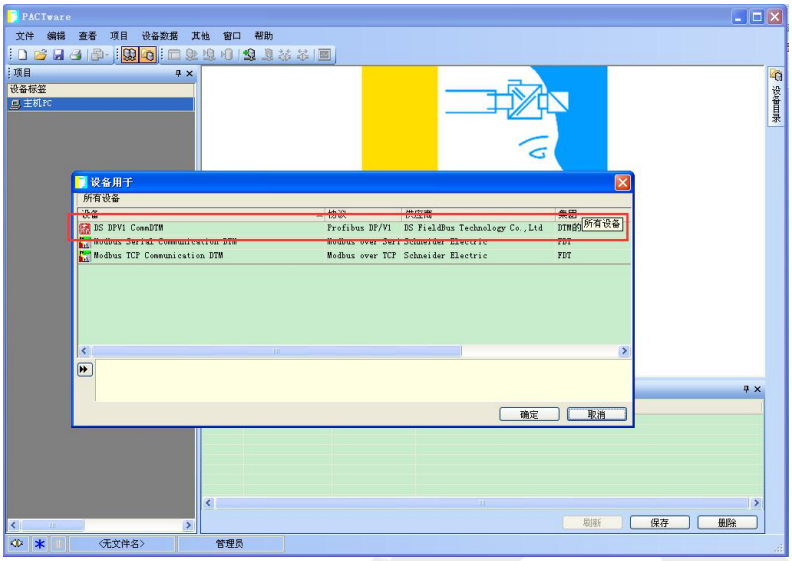


图 8-5 添加通信 DTM

步骤 3：配置设备 DTM。选中被配置的主站网关通信 DTM，点击右键，在弹出的菜单中选择“添加设备”，并在出现的设备窗口中选中 PA 设备的设备 DTM“DTM TG2600-PA”，点击将其配置入 FDT 框架程序，作为主站网关通信 DTM 下属的设备 DTM 存在。

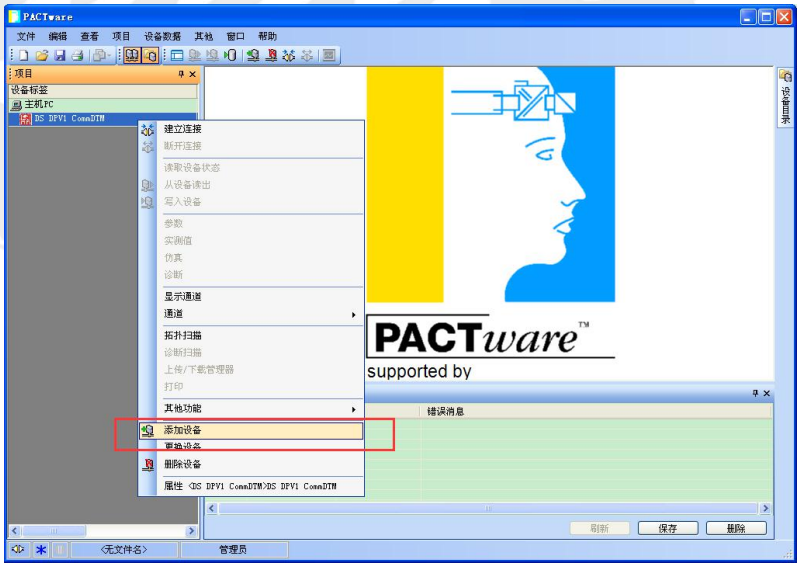


图 8-6 添加下属设备

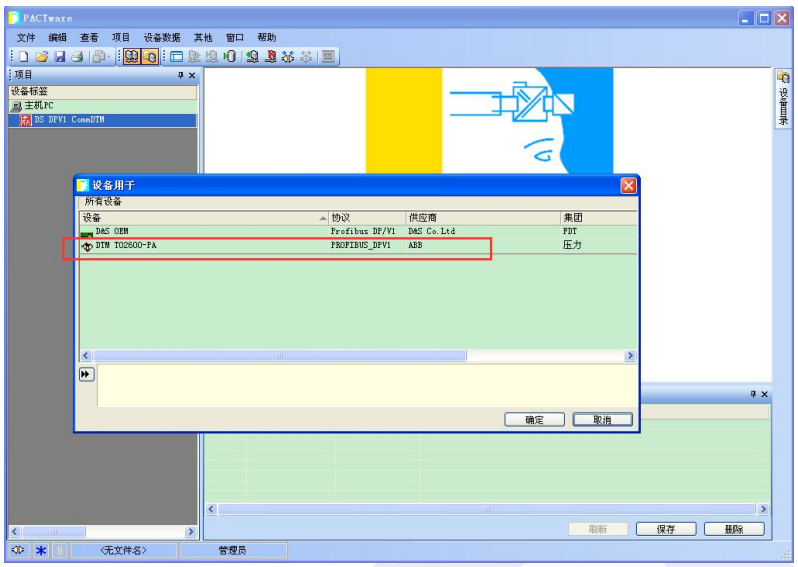


图 8-7 添加设备 DTM

步骤 4：配置各站点的通信地址信息。

配置 PA 设备 2020TG 的地址信息，如下图所示，在出现的 DP 地址设置窗口中，选中 PA 设备的通信地址为其实际通信地址。

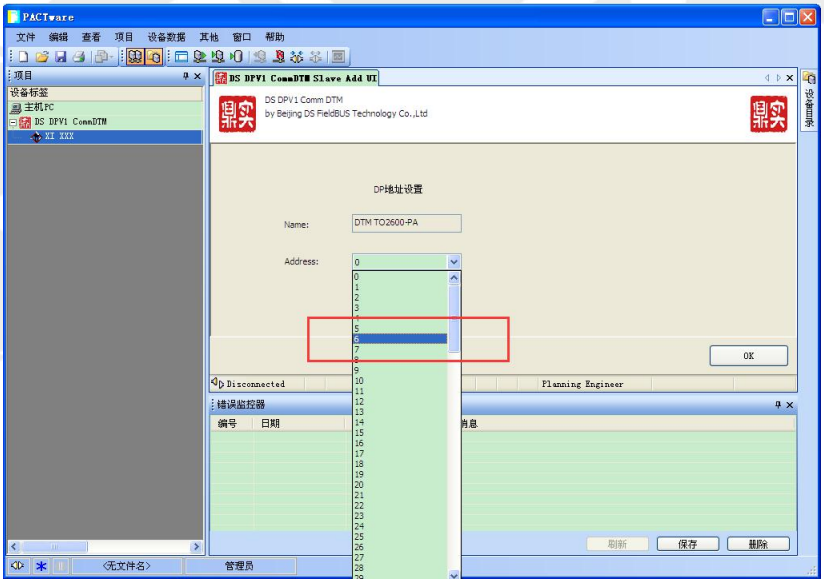


图 8-8 通讯地址设定

配置主站网关的以太网通信接口 IP 地址信息，点击主站网关的通信 DTM，在弹出的主站网关 IP 地址设置窗口中将其地址改为当前使用 IP。

在设置好 IP 地址后，点击“SAVE”按钮。

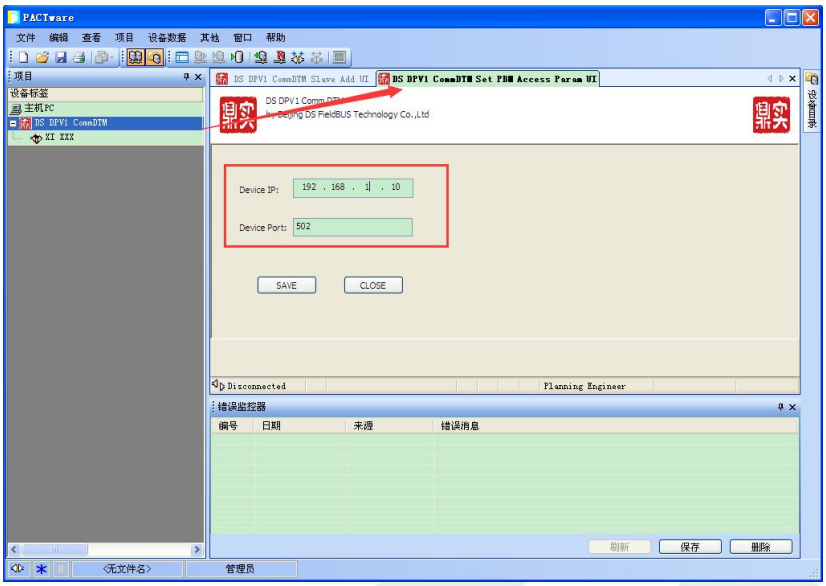


图 8-9 IP 设置

最终配置结果页面如下图所示，其中：

——DS DPV1 CommDTM：主站网关 3.0 通信 DTM

——XI XXX：PA 仪表（ABB 2020TG）设备 DTM

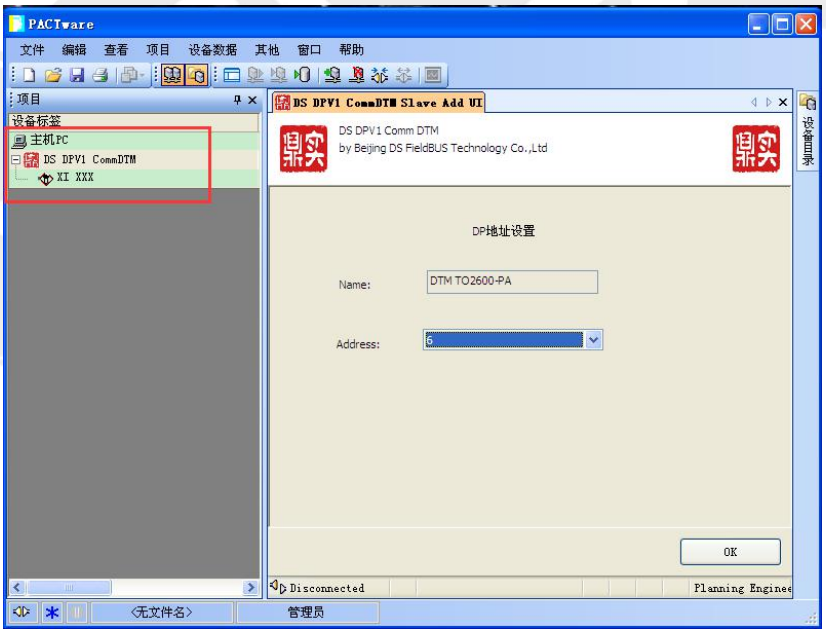


图 8-10 最终配置

步骤 5：双击 PA 设备 DTM 触发 PROFIBUS 网络 DPV1 通信，可获得的 PA 仪表（2020TG）通信数据如下面几张图所示：

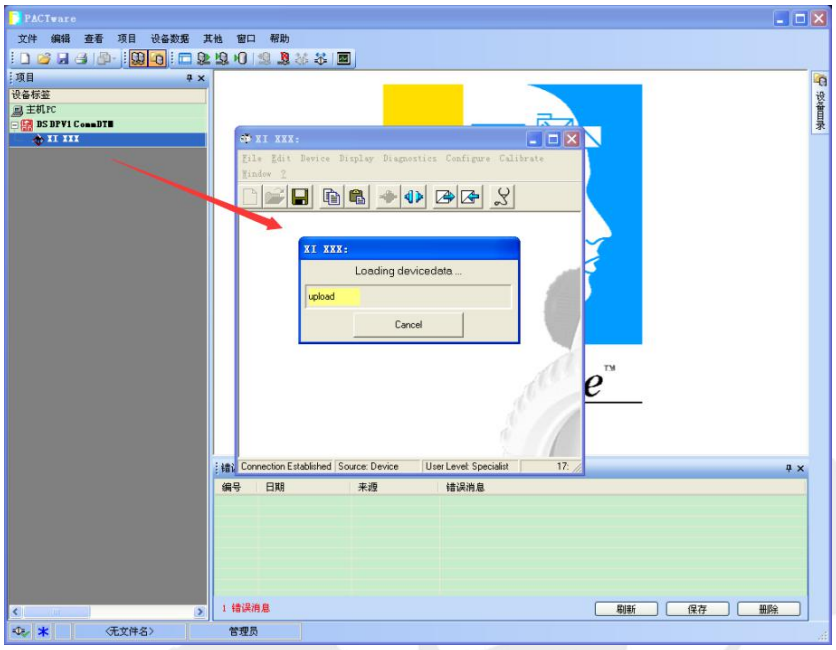


图 8-11 触发

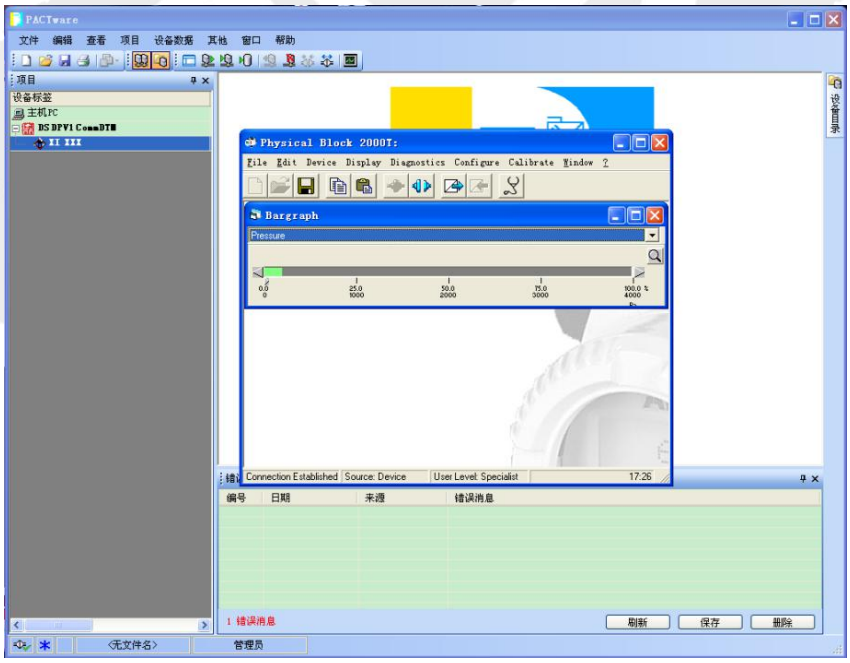


图 8-12 通讯数据一

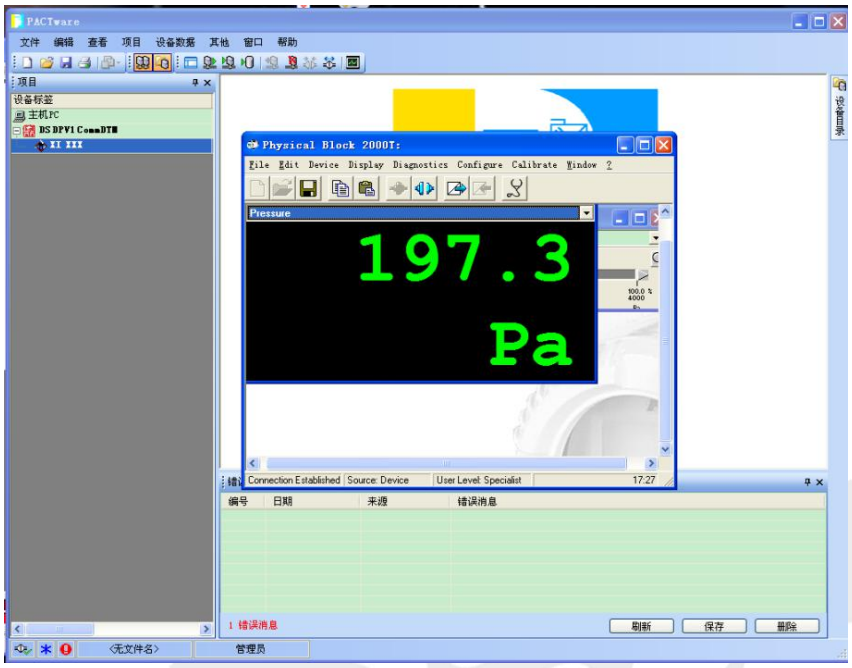


图 8-14 通讯数据二

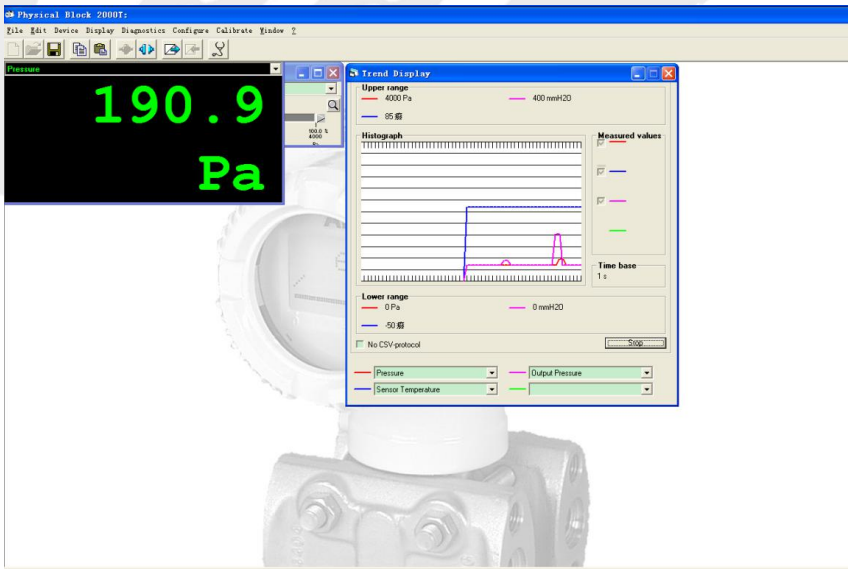


图 8-15 通讯数据三

4.2 方案二：MODBUS TCP 客户端通信 DTM + 主站网关网关 DTM +设备 DTM

步骤 1：点击各 DTM 的 EXE 安装文件，把所有 DTM 文件安装到电脑中。

步骤 2：打开上位 FDT 框架程序，在本实例中为 PACTware 框架，在此 FDT 框架程序中按照实际通信网络，配置网络拓扑结构。

如下图中选中“主机 PC”，点击右键，在弹出的菜单中选取“添加设备”。在弹中的设备窗口中选中 MODBUS TCP 客户端通信 DTM“DS MODBUSTCP CommDTM”，点击将其配置入 FDT 框架程序。

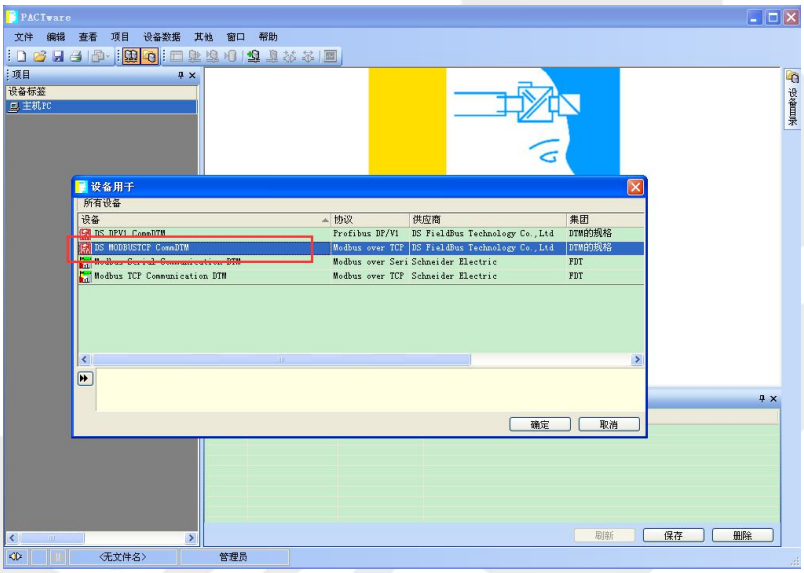


图 8-16 添加设备

步骤 3：选中 MODBUS TCP 客户端通信 DTM，右键弹出菜单，选择“添加设备”。在弹出的设备窗口中，选中主站网关 3.0 的网关 DTM，将其配置入 FDT 框架中。

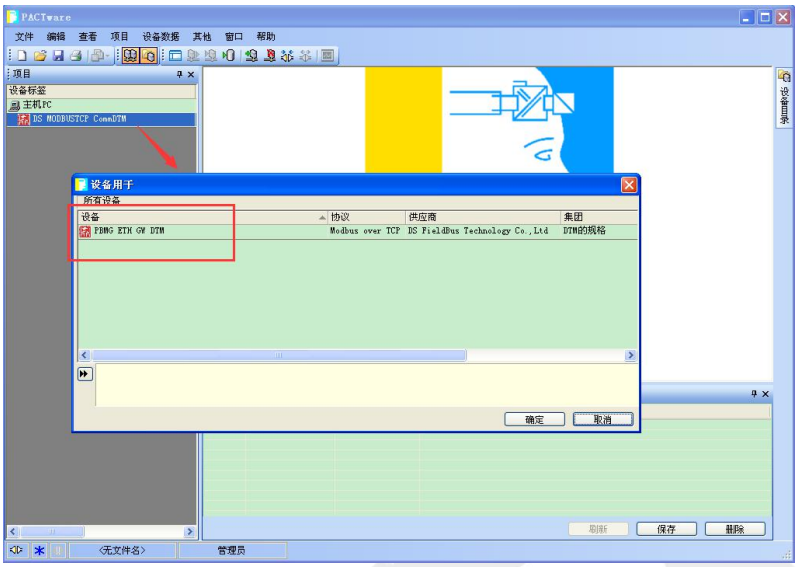


图 8-17 添加网关 DTM

步骤 4：选中主站网关的网关 DTM，点击右键，在弹出的菜单中选中“添加设备”。将 PA 设备 DTM 配置进 FDT 框架，作为网关 DTM 的下属设备存在。

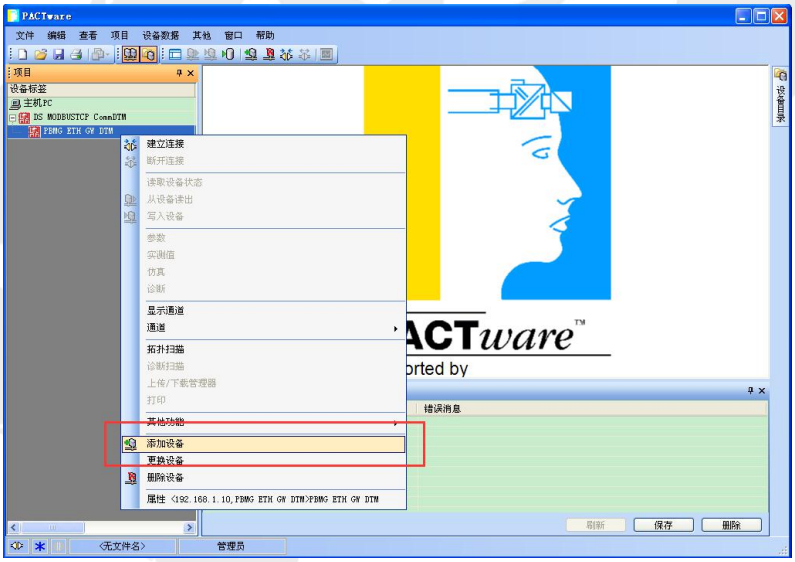


图 8-18 添加下属设备

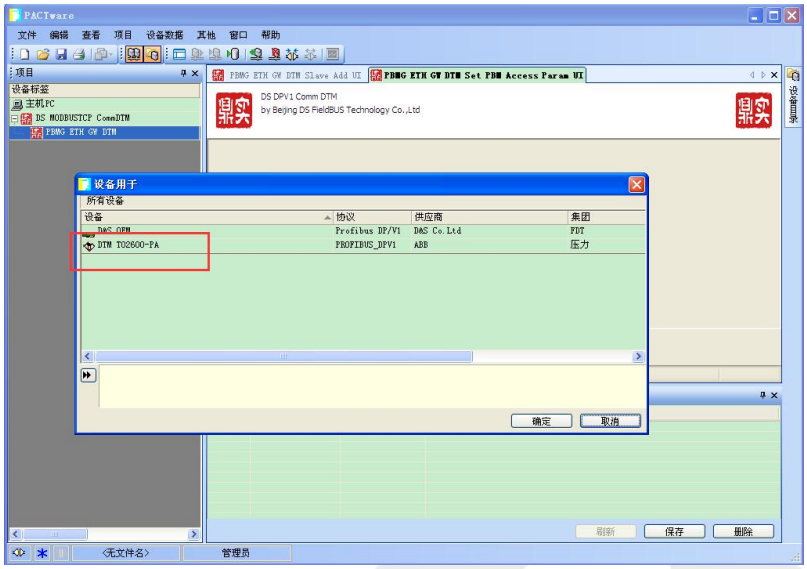


图 8-19 添加设备 DTM

步骤 5：配置各站点的通信地址信息。

配置 PA 设备 2020TG 的地址信息，如下图所示，在出现的 DP 地址设置窗口中，选中 PA 设备的通信地址为其实际通信地址。

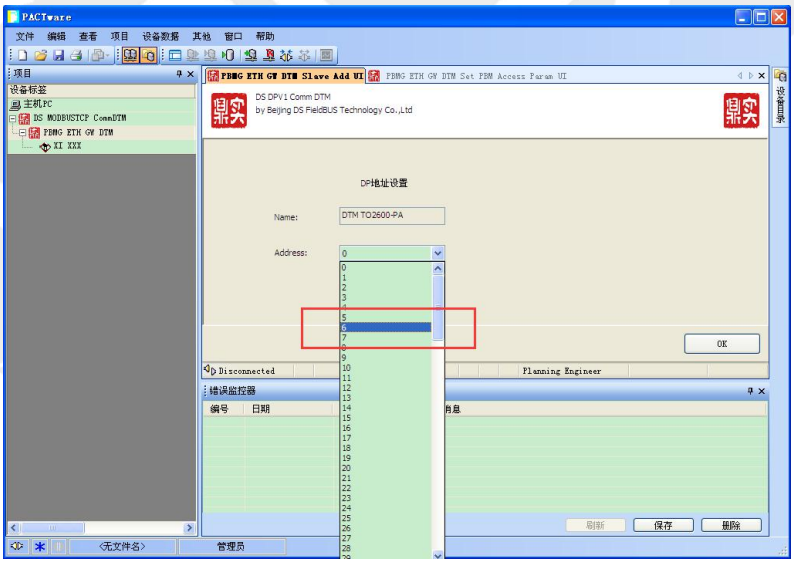


图 8-20 DP 地址设置

配置主站网关的以太网通信接口 IP 地址信息，点击主站网关的网关 DTM，在弹出的主站网关 IP 地址设置窗口中将其地址改为当前使用 IP。

在设置好 IP 地址后，点击“SAVE”按钮。

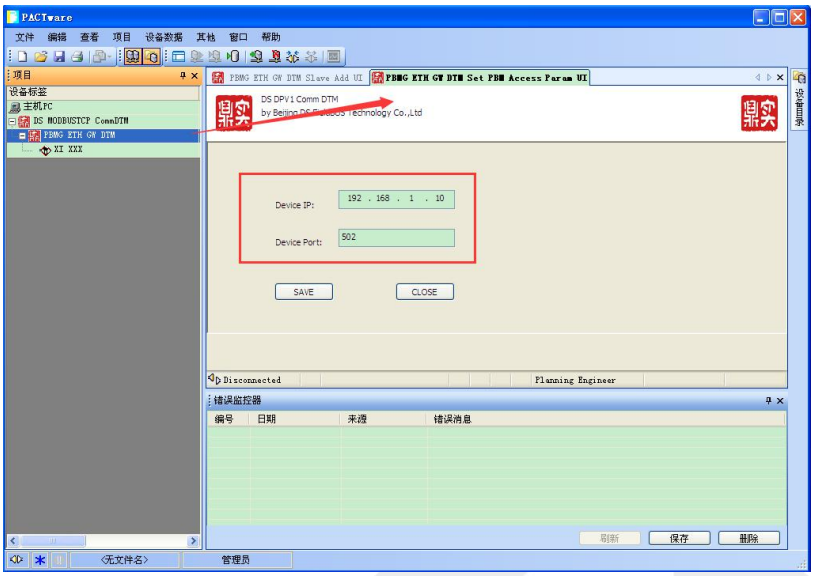


图 8-21 网关 IP 地址选择

最终配置结果页面如下图所示，其中：

——DS MODBUSTCP CommDTM：MODBUS TCP 客户端通信 DTM

——PBMG ETH GW DTM：主站网关 3.0 网关 DTM

——XI XXX：PA 仪表（ABB 2020TG）设备 DTM

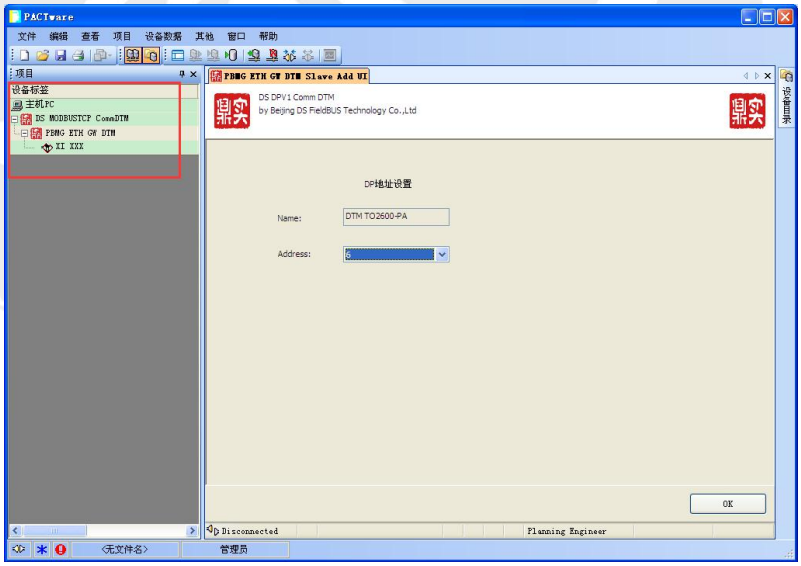


图 8-22 最终配置

步骤 6：双击 PA 设备 DTM 触发 PROFIBUS 网络 DPV1 通信，可获得的 PA 仪表（2020TG）通信数据。其通信数据在线显示图如方案一部分文档所示，不再重复说明。

附录一：术语

交换双网口模式：

通过主站网关内置的交换芯片提供主站网关自身及对外两个网口所连设备间的数据转发功能的工作模式，交换双网口模式可组建菊花链型网络而不必使用外部交换机。

独立双网口模式：

主站网关两个网络接口各自有自己的 IP 地址，位于不同的网段，两个网口间不转发报文的工作模式。交换双网口模式可用来组建冗余以太网网络。通过两个网口的 IP 地址都可同时与主站网关进行 MODBUS/TCP 通信。

主站网关正常工作模式：

与固件升级模式对应，为主站网关正常工作时的运行模式。该模式下不能进行固件升级。

主站网关固件升级模式：

进行固件升级时主站网关的运行模式。该模式仅能进行固件升级，不能进行 MODBUS/TCP-PROFIBUS 的协议转换通信功能。

PROFIBUS 安全输出数据：

主站网关向 DP 从站发送 0 长度数据或全零数据。

主站 RUN（运行）状态：

主站的正常工作状态，将 Modbus 输出数据区更新到 DP 从站输出数据，将 DP 从站输入数据更新到 Modbus 输入数据区的状态。

主站 STOP（停止）状态：

主站的安全输出状态，使用 PROFIBUS 安全输出数据而非 Modbus 输出数据区中的数据发送到 DP 从站，将 DP 从站输入数据更新到 Modbus 输入数据区的状态。

主站 OFFLINE（离线）状态：

主站的离线工作状态，主站既不向 DP 总线发送报文也不接收来自 DP 总线的任何报文。在主站网关内部没有正确配置或拨码设置“离线模式”位时主站工作在该状态。

主站网关自动工作模式：

使能主站配置中的 AUTO RUN 选项时（默认 PB-Confi 配置软件使能该选项），主站网关工作在自动工作模式，上电后主站自动运行到 RUN 状态。若 AUTO STOP 使能且其动作条件有效，主站网关会运行到 STOP 状态，当 AUTO STOP 条件无效后，主站网关会自动回到 RUN 状态。

主站网关手动工作模式：

禁止主站配置中的 AUTO RUN 选项时，主站网关工作在手动工作模式，上电后主站运行并停止在 STOP 状态，需要用户手动切换到 RUN 状态。若使能 AUTO STOP 且其动作条件有效，主站切换到 STOP 状态，此时即便 AUTO STOP 条件无效后，主站依然保持在 STOP 状态，必须由用户手动切换回 RUN 状态。该模式常用于安全等级要求较高的系统。

PROFIBUS DPV0 数据通信：

DP 主站与 DP 从站设备之间的周期性数据通信。

DPV0 输入数据：

由 DP 从站设备周期性上传给主站网关的数据。

DPV0 输出数据：

由主站网关周期性发送给 DP 从站设备的数据。

PROFIBUS DPV1 数据通信：

DP 主站与 DP 从站设备之间的非周期性数据通信。

DPV1 读数据：

由主站网关读取的从站设备非循环数据。

DPV1 写数据：

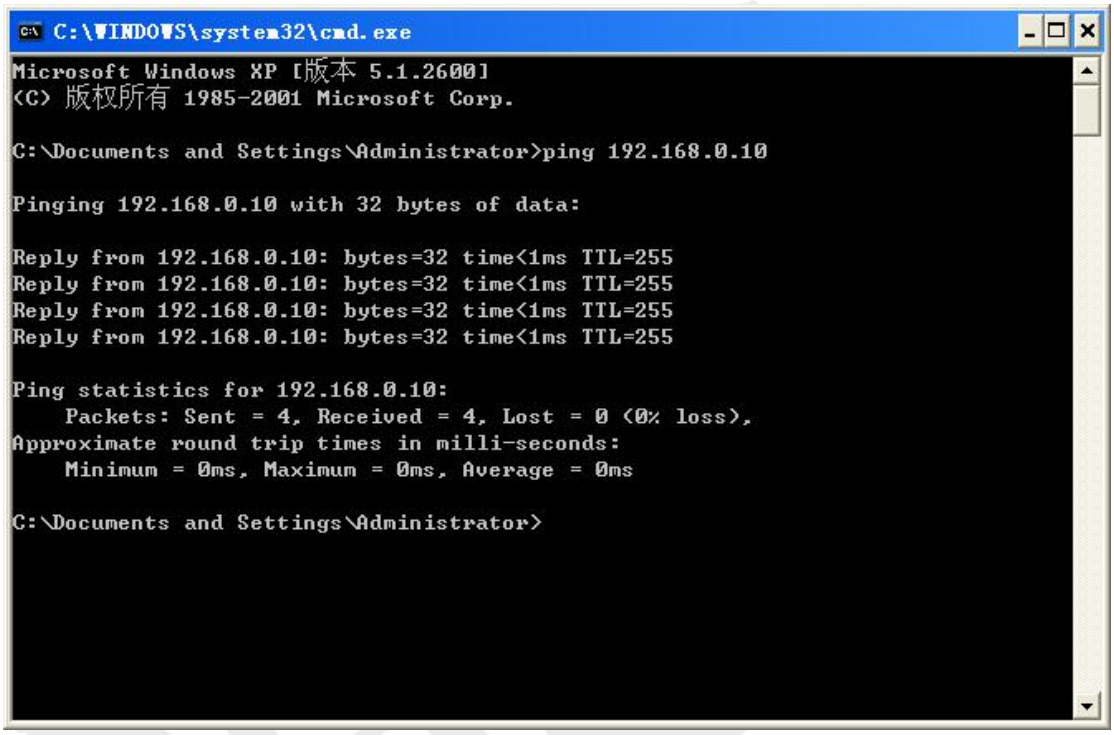
由主站网关发送给从站设备的非循环数据

附录二：常见故障排查（补充中）

网络操作

利用 ICMP ping 进行设备通信诊断

PBM-ETH-3.0 支持 ICMP 协议，通过 ping 命令可以诊断与主站网关间的网络通信。例如在 Windows XP 系统下 cmd 窗口进行 ping 操作。判断主站网关网络是否连通。不通，检查网络是否故障。



注意：为了抵御网络攻击，在利用默写 ping 工具以较短的时间间隔密集对主站网关进行 ping 通信时，主站网关会拒绝 ping 请求，ping 工具看到的是有 ping 响应超时，此时并不是网络通信异常。在使用 ping 工具进行网络通信诊断时，建议以 1s 为间隔进行 ping 测试。

主站网关 IP 冲突检测

主站网关支持 IP 冲突检测机制。主站网关上电时会首先查询当前网络内是否已经存在自身欲设置的 IP 地址。若存在则认为出现 IP 冲突，此时设备前面板上相应网口的 ETH 指示灯会呈现红色闪烁状态，此时设备正常启动。之前检测到 IP 冲突事件的主站网关会每隔 10 秒再次检测 IP 冲突，若检测到不再存在 IP 冲突则将 ETH 指示灯置为绿色状态，否则维持 IP 冲突状态。

附录三：MODBUS/TCP 通信规范简介

声明：使用以太网主站网关产品不必了解 MODBUS 的技术细节，如果读者仅从使用产品角度出发，可以只阅读本章正体部分（*忽略斜体部分*）。

1. 概述

MODBUS/TCP 是简单的、中立厂商的用于管理和控制自动化设备的MODBUS 系列通讯协议的派生产品。显而易见，它覆盖了使用TCP/IP 协议的"Intranet"和"Internet"环境中MODBUS 报文的用途。协议的最通用用途是为诸如PLC，I/O模块，，以及连接其它简单域总线或I/O 模块的网关服务的。

MODBUS/TCP 协议是作为一种（实际的）自动化标准发行的。既然MODBUS 已经广为人知，该规范只将别处没有收录的少量信息列入其中。然而，本规范力图阐明MODBUS 中哪种功能对于普通自动化设备的互用性有价值，哪些部分是MODBUS 作为可编程的协议交替用于PLC's 的"多余部分"。

1.1 面向连接

在MODBUS 中，数据处理传统上是无国界的，使它们对由噪音引起的中断有高的抵抗力，而且在任一端只需要最小的维护信息。

编程操作，另一方面，期望一种面向连接的方法。这种方法对于简单变量通过唯一的"登录"符号完成，对于Modbus Plus 变量，通过明确的"程序路径"容量来完成，而"程序路径"容量维持了一种双向连接直到被彻底击穿。

MODBUS/TCP 处理两种情况。连接在网络协议层很容易被辨认，单一的连接可以支持多个独立的事务。此外，TCP 允许很大数量的并发连接，因而很多情况下，在请求时重新连接或复用一条长的连接是发起者的选择。

熟悉MODBUS 的开发者会感到惊讶：为什么面向连接TCP 协议比面向数据报的UDP要应用广泛。主要原因是通过封装独立的"事务"在一个连接中，此连接可被识别，管理和取消而无须请求客户和服务器采用特别的动作。这就使进程具有对网络性能变化的适应能力，而且容许安全特色如防火墙和代理可以方便的添加。

类似的推理被最初的万维网的开发者所采用，他们选用TCP 及端口80 去实现一个作为单一事务的最小的环球网询问。

1.2 数据编码

MODBUS 采用"big-endian"来表示地址和数据对象。 这就意味着当一个数字表示的数量大于所传输的单一字节，最大有效字节将首先被发送。例如：

16 - bits 0x1234 将为 0x12 0x34

32 - bits 0x12345678L 将为 0x12 0x34 0x56 0x78

1.3 参考编号的解释

MODBUS 将其数据模型建立在一系列具有不同特征的表的基础之上。这四个基本表如下:

- *离散输入 单比特，由I/O 系统提供，只读*
- *离散输出 单比特，由应用程序更改，读写*
- *输入寄存器 16 比特，数值，由I/O 系统提供 ，只读*
- *输出寄存器 16 比特，数值，由应用程序更改，读写*

输入和输出之间以及可寻址位和可寻址代码的数据对象之间的差别并不意味着任何应用性能的不同。如果这是我们所讨论的目标机械的最自然的解释，那么认为所有的四个基本表是相互覆盖的看法也是非常普通而完全可以接受的。

对于每一个基本表，协议允许单独选择65536 个数据对象中的任何一个，而且对那些对象的读写操作可以跨越多个连续的数据对象，直到达到基于处理事务功能代码的数据大小限制。

这儿没有假定数据对象代表一种真正邻接的数据阵列，而这是大多数简单PLC's 的解释。

"读写常用参考"功能代码被定义为携带32 位的参考值并且能允许在"非常"大的空间里可以直接访问数据对象。现在没有可以利用这一特点的PLC 设备。

一个易造成混乱的潜在来源是用于MODBUS 功能的参考值和用于Modicon PLC's 的"寄存器值"之间的关系。由于历史原因，用户参考值使用从1 开始的十进制数表示。而MODBUS 采用更普通的从0 开始的无符号整数进行软件数据整理分析。

于是，请求从0 读取寄存器的Modbus 消息将已知值返回建立在寄存器4：00001（存储类型4=输出寄存器，参考值00001）中的应用程序。

1.4 隐含长度基本原则

所有的MODBUS 请求和响应都被设计成在此种方法下工作，即接收者可确认消息的完整性。 对于请求和响应为固定长度的功能代码，仅发送功能代码就足够了。对于在请求和响应中携带不定长数据的功能代码，数据部分前将加上一个字节的数据统计。

当 Modbus 通过TCP 运送，前缀中携带附加的长度信息以便接收者识别消息的边界，甚至消息被分成若干组进行传输。 外在的和隐含的长度准则的存在，以及CRC-32 检错代码（以太网）的使用使请求和响应消息中发生未被识别的错误的机率减至无限小。

2. 一致性等级概述

当从草稿开始定义一种新的协议，有可能加强编码方式和阐述的一致性。MODBUS 由于其先进的特性，已经在很多地方得到了实施，必须避免破坏它已经存在的实施。

因此，已经存在的成套的处理类型被划分出一致性等级：等级0 代表普遍使用且总体上一致的功能；等级2 代表有用的功能，但带有某些特性。现存装置的不适应于互用性的功能也已确认。

必须注意到，将来对该标准的扩充将定义附加的功能代码来处理现存事实标准不适用的情形。然而，被提议扩充的详细资料出现在本手册中将会另人误解。通过将代码"随机的"发送或者即便是通过检查异常响应的类型来确定特别的目标装置是否支持特别的功能代码总是可能的，而且该方法将保证引入这些扩充的现使用的MODBUS 设备的连续的互用性。事实上，这就是当前功能代码的分级原则。

2.1 等级0

这是最小的有用功能，对主站和从站来说。

- *读乘法寄存器 (fc 3)*
- *写乘法寄存器 (fc 16)*

2.2 等级 1

这是附加的被普遍实现的和能共同使用的成套功能，正如前面介绍过的，许多从站把输入，输出，离散值和寄存器值作为同等的进行处理。

- *读线圈 (fc 1)*

- *读离散输入 (fc 2)*
- *读寄存器输入 (fc 4)*
- *写线圈 (fc 5)*
- *写单一寄存器 (fc 6)*
- *读异常状态字 (fc 7)*

此功能对于每一个从站系列显然具有不同的含义。

2.3 等级 2

这些是需要HMI 和管理等例行操作的数据传送功能。

- *强制型多路线圈 (fc 15)*
- *读一般参考值 (fc 20)*

该功能可以处理并发的多个请求，而且能接收32 位的参考数值，最适于扩充以处理大的寄存器空间和缺少诸如"未定位"变量的参考值的数据对象。

- *写一般参考值 (fc 21)*

此功能可以处理并发的多个请求 ，也可接收32 位的参考数值，最适于扩充以处理大的寄存器空间和缺少诸如"未定位"变量的参考值的数据对象。

- *掩膜写寄存器 (fc 22)*
- *读/写寄存器 (fc 23)*

此功能把一定范围的寄存器输入和输出当作单一的处理事务。使用MODBUS 是执行规则的带有I/O 模块的状态影象交换的最好办法。

如此，高性能的通用的数据采集装置可以执行功能3，16和23，从而把快捷的数据规则交换（23）和执行特殊数据对象的需求询问或更新的能力结合起来（3和16）。

- *读FIFO 队列 (fc 24)*

一个有点专用的功能，打算将表结构的数据像FIFO一样传送到主机。对于某种事件录入软件很有用。

2.4 机器/厂家/网络的特殊功能

以下所有的功能，虽然在MODBUS 协议手册中提到，但由于它们有很强的机器依赖性，因而不适于互用性的目的。

- *诊断 (fc 8)*

- *编程 (484) (fc 9)*
- *轮询 (484) (fc 10)*
- *获取通讯事件计数器值(Modbus) (fc 11)*
- *获取通讯事件记录(Modbus) (fc 12)*
- *编程 (584/984) (fc 13)*
- *轮询(584/984) (fc 14)*
- *通告从站 ID (fc 17)*
- *编程 (884/u84) (fc 18)*
- *恢复通讯连接 (884/u84) (fc 19)*
- *编程 (原理) (fc 40)*
- *固件置换 (fc 125)*
- *编程 (584/984) (fc 126)*
- *通告本地地址 (Modbus) (fc 127)*

3. 协议结构

本部分阐述了通过MODBUS/TCP 网络携带的MODBUS 请求和或响应封装的一般格式。必须注意到请求和响应本体（从功能代码到数据部分的末尾）的结构和其它MODBUS 变量具有完全相同的版面格式和含义，如：

MODBUS 串行端口 - ASCII 编码

MODBUS 串行端口 - RTU (二进制) 编码

MODBUS PLUS 网络 – 数据通道

这些其它案例仅在组帧次序，检错模式和地址描述等格式有所不同。

所有的请求通过TCP 从寄存器端口502 发出。

请求通常是在给定的连接以半双工的方式发送。也就是说，当单一连接被响应所占用，就不能发送其它的请求。有些装置采用多条TCP 连接来维持高的传输速率。

MODBUS "从站地址"字段被单字节的"单元标识符"替换，从而用于通过网桥和网关等设备的通讯，这些设备用单一IP 地址来支持多个独立的终接单元。

请求和响应带有六个字节的前缀，如下：

byte 0: 事务处理标识符 –由服务器复制 –通常为 0

byte 1: 事务处理标识符 –由服务器复制 –通常为 0

byte 2: 协议标识符= 0

byte 3: 协议标识符= 0

byte 4: 长度字段 （上半部分字节） = 0 (所有的消息长度小于256)

byte 5: 长度字段 (下半部分字节) = 后面字节的数量

byte 6: 单元标识符 (原"从站地址")

byte 7: MODBUS 功能代码

byte 8 on: 所需的数据

因而处理示例"以4 的偏移从UI 9 读1 寄存器"返回5 的值将是

请求：00 00 00 00 00 06 09 03 00 04 00 01

响应：00 00 00 00 00 05 09 03 02 00 05

熟悉MODBUS 的设计师将注意到MODBUS/TCP 中不需要"CRC-16"或"LRC"检查字段。而是采用TCP/IP 和链路层（以太网）校验和机制来校验分组交换的准确性。

4. 一致性等级的协议参考值

注意到在例子中，请求和响应列在功能代码字节的前面。如前所述，在MODBUS/TCP 案例中有一个依赖传输的包含7 个字节的前缀。

ref ref 00 00 00 len unit

前面两个字节的"ref ref"在服务器中没有具体的值，只是为方便客户端而从请求和响应中逐字的复制过来。单客户机通常将该值置为0。

在这个例子中，请求和响应的格式如下（例子是"读寄存器"请求，详述见后面部分）。

03 00 00 00 01 => 03 02 12 34

这表示给前缀加上一个十六进制的串联的字节，这样，TCP 连接上的整个消息将是（假设单元标识符还是09）

请求： 00 00 00 00 00 06 09 03 00 00 00 01

响应： 00 00 00 00 00 05 09 03 02 12 34

4.1 等级0 指令详述

4.1.1 读乘法寄存器(FC 3)

请求

Byte 0: FC = 03

Byte 1-2: 参考数值

Byte 3-4: 指令数(1-125)

响应

Byte 0: FC = 03

Byte 1: 响应的字节数 (B=2 x 指令数)

Byte 2-(B+1): Register values

异常

Byte 0: FC = 83 (hex)

Byte 1: 异常代码 = 01 or 02

示例

读参考值为0 (Modicon 984 中为40001)时的1 寄存器得到十六进制的值1234

03 00 00 00 01 => 03 02 12 34

4.1.2 写乘法寄存器(FC 16)

请求

Byte 0: FC = 10 (hex)

Byte 1-2: 参考数值

Byte 3-4: 指令数 (1-100)

Byte 5: 字节数 (B=2 x word count)

Byte 6-(B+5): 寄存器值

响应

Byte 0: FC = 10 (hex)

Byte 1-2: 参考数值

Byte 3-4: 指令数

异常

Byte 0: FC = 90 (hex)

Byte 1: 异常代码 = 01 or 02

示例

读参考值为0(Modicon 984 中为40001)时的1 寄存器得到十六进制的值1234

10 00 00 00 01 02 12 34 => 10 00 00 00 01

4.2 等级1 指令详述

4.2.1 读线圈 (FC 1)

请求

Byte 0: FC = 01

Byte 1-2: 参考数值

Byte 3-4: 比特数(1-2000)

响应

Byte 0: FC = 01

Byte 1: 响应的字节数 (B=(比特数+7)/8)

Byte 2-(B+1): 比特值(最小意义位首先绕线圈!)

异常

Byte 0: FC = 81 (hex)

Byte 1: exception code = 01 or 02

示例

读参考值为0 (Modicon 984 中为00001)时的1 线圈得到的值1

01 00 00 00 01 => 01 01 01

注意到返回的数据的格式和big-endian 体系结构不同。而且此请求如果调用乘法指令字且这些指令不以16 位为界排列，那么该请求将在从站得到计算强化。

4.2.2 读离散输入 (FC 2)

请求

Byte 0: FC = 02

Byte 1-2: 参考数值

Byte 3-4: 比特数 (1-2000)

响应

Byte 0: FC = 02

Byte 1: 响应的字节数 (B=(比特数+7)/8)

Byte 2-(B+1): 比特值 (最小意义位首先绕线圈!)

异常

Byte 0: FC = 82 (16 进制)

Byte 1: 异常代码 = 01 or 02

示例

读参考值为0 (Modicon 984 中为10001)时的1 离散输入得到的值1

02 00 00 00 01 => 02 01 01

注意到返回的数据的格式和big-endian 体系结构不同。而且此请求如果调用乘法指令字且这些指令不以16 位为界排列，那么该请求将在从站得到计算强化。

4.2.3 读输入寄存器 (FC 4)

请求

Byte 0: FC = 04

Byte 1-2: 参考数值

Byte 3-4: 指令数 (1-125)

响应

Byte 0: FC = 04

Byte 1: 响应的比特数 (B=2 x 指令数)

Byte 2-(B+1): 寄存器值

异常

Byte 0: FC = 84 (hex)

Byte 1: 异常代码 = 01 or 02

示例

读参考值为0 (Modicon 984 中为30001)时的1 输入寄存器得到十六进制的值1234

04 00 00 00 01 => 04 02 12 34

4.2.4 写线圈 (FC 5)

请求

Byte 0: FC = 05

Byte 1-2: 参考数值

Byte 3: = FF 打开线圈, =00 关闭线圈

Byte 4: = 00

响应

Byte 0: FC = 05

Byte 1-2: 参考数值

Byte 3: = FF 打开线圈, =00 关闭线圈(回波)

Byte 4: = 00

异常

Byte 0: FC = 85 (16 进制)

Byte 1: 异常代码 = 01 or 02

示例

将值1 在参考值为0（Modicon 984 中为00001）时写入1 线圈

05 00 00 FF 00 => 05 00 00 FF 00

4.2.5 写单一寄存器(FC 6)

请求

Byte 0: FC = 06

Byte 1-2: 参考数值

Byte 3-4: 寄存器值

响应

Byte 0: FC = 06

Byte 1-2: 参考数值

Byte 3-4: 寄存器值

异常

Byte 0: FC = 86 (16 进制)

Byte 1: 异常代码= 01 or 02

示例

将十六进制值1234 在参考值为0（Modicon 984 中为40001）时写入1 线圈

06 00 00 12 34 => 06 00 00 12 34

4.2.6 读异常状态字 (FC 7)

注意“异常状态字”和“异常响应”没有关系。“读异常状态字”消息欲在采用小波特率轮询多点网络的早期MODBUS 中允许最大的响应速度。PLC’s 将特别规划一个8 线圈（离散输出）的范围用此消息进行询问。

请求

Byte 0: FC = 07

响应

Byte 0: FC = 07

Byte 1: 异常状态字 (通常预先确定8 线圈的范围)

异常

Byte 0: FC = 87 (16 进制)

Byte 1: 异常代码 = 01 or 02

示例

读异常状态字得到16 进制值34

07 => 07 34

4.3 等级2 指令详述

4.3.1 强制多点线圈 (FC 15)

请求

Byte 0: FC = 0F (16 进制)

Byte 1-2: 参考数值

Byte 3-4: 比特数 (1-800)

Byte 5: 字节数 (B = (比特数 + 7)/8)

Byte 6-(B+5): 写入的数据 (最小意义位 = 第一个线圈)

响应

Byte 0: FC = 0F (16 进制)

Byte 1-2: 参考数值

Byte 3-4: 比特数

异常

Byte 0: FC = 8F (16 进制)

Byte 1: 异常代码 = 01 or 02

示例

当参考值为0（在Modicon 984 中为00001）时给3 线圈写入值0，0，1

0F 00 00 00 03 01 04 => 0F 00 00 00 03

注意到返回的数据的格式和big-endian 体系结构不同。而且此请求如果调用乘法指令字且这些指令不以16 位为界排列，那么该请求将在从站得到计算强化。

4.3.2 读一般参考值 (FC 20)

请求

Byte 0: FC = 14 （16 进制）

Byte 1: 请求余项的字节数 (=7 x 组数)

Byte 2: 第一组的参考值类型 = 适合于 6xxxx 扩展寄存外存储器的06

Byte 3-6: 第一组的参考数值

= 适于 6xxxx 外存储器的存储器偏移量

= 适于 4xxxx 寄存器的32 位参考数值

Byte 7-8: 第一组的指令

Bytes 9-15: (至于2-8 字节，适于第二组)

. . .

响应

Byte 0: FC = 14 (16 进制)

Byte 1: 响应的全部字节数

(=组数+ 组的总的字节数)

Byte 2: 第一组的字节数 (B1=1 + (2 x 指令数))

Byte 3: 第一组的参考类型

Byte 4-(B1+2): 第一组的寄存器值

Byte (B1+3): 第二组的字节数 (B2=1 + (2 x 指令数))

Byte (B1+4): 第二组的参考类型

Byte (B1+5)-(B1+B2+2): 第二组的寄存器值

. . .

异常

Byte 0: FC = 94 (16 进制)

Byte 1: 异常代码 = 01 或 02 或03 或04

示例

参考值为1 时读1 扩展寄存器： 2 （在 Modicon 984 中外存储器1 偏移量2）得到 16 进制值1234

14 07 06 00 01 00 02 00 01 => 14 04 03 06 12 34

(将来)

参考值0 时读1 寄存器返回16 进制值1234，参考值5 时读2 寄存器返回16 进制值5678 和 9abc。

14 0E 04 00 00 00 00 00 01 04 00 00 00 05 00 02 => 14 0A 03 04 12 34 05 04 56 78 9A BC

注意传输尺寸限制很难用数学公式精确定义。概括说来，由于缓冲的大小的限制以及考虑到每个请求和响应数据帧的总长度请求和响应的消息尺寸均限于256 个字节。如果从站由于响应太大而拒绝发送此消息将产生异常类型04。

4.3.3 写一般参考值(FC 21)

请求

Byte 0: FC = 15 (16 进制)

Byte 1: 请求余额的字节数

Byte 2: 第一组的参考值类型= 6xxxx 扩展寄存器存储器的06

Byte 3-6: 第一组的参考数值

= 适于 6xxxx 外存储器的存储器偏移量

= 用于 4xxxx 寄存器的32 位的参考数值

Byte 7-8: 第一组的指令数 (W1)

Byte 9-(8 + 2 x W1): 第一组的寄存器数据

(从字节2 开始为其它组复制组的数据帧)

. . .

响应

响应是对询问的直接回应

Byte 0: FC = 15 (16 进制)

Byte 1: 请求余额的字节数

Byte 2: 第一组的参考值类型 = 6xxxx 扩展寄存器存储器的06

Byte 3-6: 第一组的参考数值

= 6xxxx 外存储器的存储器偏移量

=用于 4xxxx 寄存器的32 位的参考数值

Byte 7-8: 第一组的指令数 (W1)

Byte 9-(8 + 2 x W1): 第一组的寄存器数据

(从字节2 开始为其它组复制组的数据帧)

. . .

异常

Byte 0: FC = 95 (16 进制)

Byte 1: 异常代码= 01 或 02 或03 或04

示例

参考值为1时写1扩展寄存器： 2 （在 Modicon 984 中外存储器1 偏移量2）得到 16 进制值1234

15 09 06 00 01 00 02 00 01 12 34 => 15 09 06 00 01 00 02 00 01 12 34

(将来)

参考值0 时写1 寄存器返回16 进制值1234，参考值5 时写2 寄存器返回16 进制值5678 和 9abc。

15 14 04 00 00 00 00 00 01 12 34 04 00 00 00 05 00 02 56 78 9A BC

?15 14 04 00 00 00 00 00 01 12 34 04 00 00 00 05 00 02 56 78 9A BC

注意传输尺寸限制很难用数学公式精确定义。概括说来，由于缓冲的大小的限制以及考虑到每个请求和响应数据帧的总长度请求和响应的消息尺寸均限于256 个字节。如果从站由于响应太大而拒绝发送此消息将产生异常类型04。

4.3.4 掩膜写寄存器 (FC 22)

请求

Byte 0: FC = 16 (16 进制)

Byte 1-2: 参考数值

Byte 3-4: AND 掩膜用于寄存器

Byte 5-6: OR 掩膜用于寄存器

响应

Byte 0: FC = 16 (16 进制)

Byte 1-2: 参考数值

Byte 3-4: AND 掩膜用于寄存器

Byte 5-6: OR 掩膜用于寄存器

异常

Byte 0: FC = 96 (16 进制)

Byte 1: 异常代码 = 01 或 02

示例

在参考值为0（Modicon 984 中为40001）时将寄存器的0-3 位字段改为16 进制值4

(AND 用 000F, OR 用 0004)

16 00 00 00 0F 00 04 => 16 00 00 00 0F 00 04

4.3.5 读/写寄存器 (FC 23)

请求

Byte 0: FC = 17 (16 进制)

Byte 1-2: 用于读的参考数值

Byte 3-4: 用于读的指令数 (1-125)

Byte 5-6: 用_____于写的参考数值

Byte 7-8: 用于写的指令数 (1-100)

Byte 9: 字节数 (B = 2 x 用于写的指令数)

Byte 10-(B+9): 寄存器值

响应

Byte 0: FC = 17 (16 进制)

Byte 1: 字节数Byte count(B = 2 x 用于读的指令数)

Byte 2-(B+1) 寄存器值

异常

Byte 0: FC = 97 (16 进制)

Byte 1: 异常代码 = 01 或 02

示例

参考值为3（在Modicon 984 中为40004）时写入1 寄存器16 进制值0123，参考值为0 时

读2 寄存器返回值0004 和5678（16 进制）

17 00 00 00 02 00 03 00 01 02 01 23 => 17 04 00 04 56 78

注意如果寄存器交替的进行读写操作，结果是不明确的。一部分设备先写后读，另部分则先读后写。

4.3.6 读FIFO 队列 (FC 24)

请求

Byte 0: FC = 18 (16 进制)

Byte 1-2: 参考数值

响应

Byte 0: FC = 18 (16 进制)

Byte 1-2: 字节数 (B = 2 + 指令数) (最大64)

Byte 3-4: 指令数 (FIFO 中累积的指令数) (最大 31)

Byte 5-(B+2): 从 FIFO 前开始的寄存器数据

异常

Byte 0: FC = 98 (16 进制)

Byte 1: 异常代码 = 01 或02 或 03

示例

读从参考值0005 （Modicon 984 中为40006）开始的FIFO 区段内容，其中包括2 指令的值1234 和5678（16 进制）

18 00 05 => 18 00 06 00 02 12 34 56 78

注意到执行在984 上的该功能在通用性方面非常有限-假定寄存器的该区段包括含有从0 到31 值的计数器，后面还跟着最大到31 指令字的数据。当该功能完成，该计数器指令字不会象经过FIFO 操作所期望的回复为0。

一般说来，这可被看作函数16-读乘法寄存器的有限子集，既然后者可用来完成所必须的功能性。

5. 异常代码

在出问题的时候，有一系列定义过的异常代码被从站送回。注意到主站会“投机地”发送指令，利用接收到的成功或异常代码来确定支配设备的哪一个MODBUS 愿意响应以及从

站不同可用数据区的大小。

所有的异常通过添加0x80 到请求的功能代码来标记，跟随此字节的是一个单一的原因字节，如下例所示：

03 12 34 00 01 => 83 02

当索引0x1234 响应异常类型2-“非法的数据地址”时请求读1寄存器

异常情况列举如下：

01 非法的功能

对从站来说，在询问过程中收到的功能代码是不允许的行为。这可能是由于功能代码只适用于新近的控制器，而不能在所选的单元使用。也可推断出从站处于错误的状态而发出这样的一种请求，例如未经配置而被要求返回寄存器值。

02 非法的数据地址

对从站来说，在询问过程中收到的数据地址不是允许的地址。更明确一点，参考数值和传输长度的结合是无效的。对于一个有100 个寄存器的控制器来说，具有偏移96 和长度4 的请求将能成功，而具有偏移96 和长度5 的请求将产生异常02。

03 非法的数据值

对从站来说，在询问数据区段所包含的值是不允许的。这推断出在复杂请求余额的结构中的一个错误，例如隐含长度是不正确的。既然MODBUS 协议不了解一些特殊寄存器的特殊值的意义，因此这并不意味着寄存器中被提交用于存储的数据对象有一个应用程序期望值之外的值。

04 非法的响应长度

指出加外框的请求将产生一个尺寸超出可用MODBUS 数据尺寸的响应。仅用于由功能所产生的多部分响应，如功能20 和21。

05 确认

专用于关联程序设计指令。

06 从站设备忙

专用于关联程序设计指令。

07 否认

专用于关联程序设计指令。

08 存储器奇偶校验错误

专用于关联功能代码20 和21，指出扩展文件区没通过一致性检验。

0A 网关通路不可用

专用于关联Modbus Plus 网关，指出网关未能分配Modbus Plus 路径以处理请求。通常意味着网关配置错误。

0B 网关目标设备响应失败

专用于关联Modbus Plus 网关，指出从目标设备未能获得响应。通常意味着设备没有连接到网络上。

6. MODBUS 存储区

MODBUS 涉及到的控制器（或 MODBUS 设备）存储区以 3XXXX、4XXXX 标识；

存储区标识	名称	类型	读/写	存储单元地址
3XXXX	输入寄存器	字	只读	3001~3XXXX， XXXX：与设备有关
4XXXX	保持/输出寄存器	字	读/写	4001~4XXXX， XXXX：与设备有关

7. MODBUS 功能

即 MODBUS 应用层，规定了 MODBUS 报文格式和服务功能。

MODBUS 协议定义了一个与基础通信层无关的简单协议数据单元（PDU） 。特定总线或网络上 MODBUS 协议映射能够在应用数据单元（ADU）上引入一些附加域。

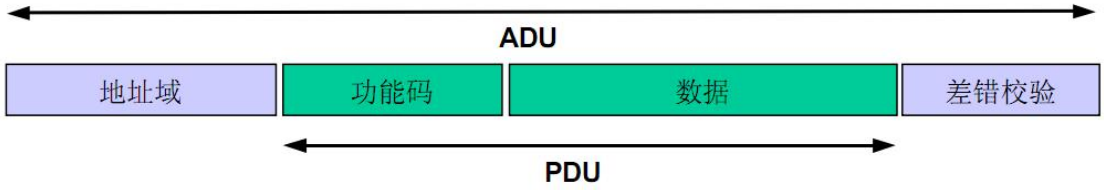


图 3-1 通用 MODBUS 帧

通用 MODBUS 帧如上图所示，而 MODBUS/TCP IP 网络中进行的 MODBUS 请求或响应的封装如下图所示：

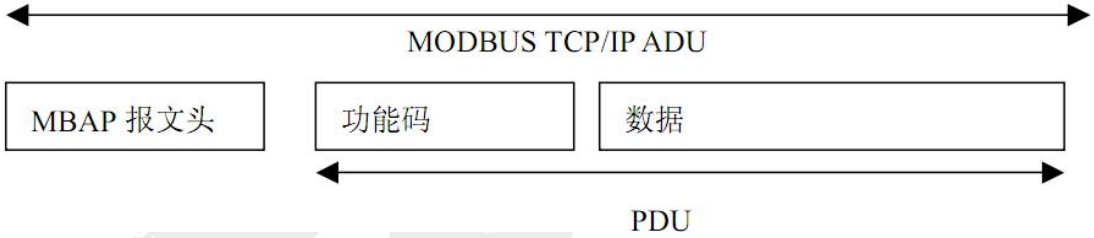


图 3-2 TCP/IP 上的 MODBUS 的请求/响应

如上图所示，在 TCP/IP 上使用一种专用报文头识别 MODBUS 应用数据单元。 将这种报文头称为 MBAP 报文（MODBUS 协议报文头）。

MBAP 报文头包括下列域：

域	长度	描述	客户机	服务器
事物元标识符	2 个字节	MODBUS 请求响应事物处理的识别码	客户机启动	服务器从接收的请求中重新复制
协议标识符	2 个字节	0=MODBUS 协议	客户机启动	服务器从接收的请求中重新复制
长度	2 个字节	一下字节的数量	客户及启动（请求）	服务器（响应）启动
单元标识符	1 个字节	串行链路或其他总线上连接的远程从站的识别码	客户机启动	服务器从接收的请求中重新复制

报文头为 7 个字节长

事务处理标识符： 用于事务处理配对。在响应中， MODBUS 服务器复制请求的事务处理标识符。

协议标识符：用于系统内的多路复用。通过值 0 识别 MODBUS 协议。

长度：长度域是下一个域的字节数，包括单元标识符和数据域。

单元标识符：为了系统内路由，使用这个域。专门用于通过以太网 TCP-IP 网络和 MODBUS 串行链路之间的网关对 MODBUS 或 MODBUS+串行链路从站的通信。MODBUS 客户机在请求中设置这个域，在响应中服务器必须利用相同的值返回这个域。

下面介绍 MODBUS TCP/IP 报文 支持的几种功能码 PDU 部分的格式：

7.1 读取保存寄存器

功能码：03H

主站询问报文格式：（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	06	01

PDU 部分：

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
03	00	6B(107)	00	03

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： 起始地=006BH=107，对应地址 40108；寄存器数=0003；末地址=40108+3-1=40110；

因此，本询问报文功能是：读单元标识符为 01 的从站 3 个保持寄存器 40108—40110 的值；

从站应答格式：（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	09	01

PDU 部分：

功能码	字节计数	寄存器 40108 低位	寄存器 40108 高位	寄存器 40109 低位	寄存器 40109 高位	寄存器 40110 低位	寄存器 40110 高位
03	6	02	2B	01	06	2A	64

功能：从站返回保持寄存器 40108—10110 的值；(40108)=022BH，(40109)=0106H，(40110)=2A64H

7.2 读取输入寄存器

功能码：04H

主站询问报文格式（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	06	01

PDU 部分：

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
04	00	08	00	01

功能：读从站输入寄存器 3XXXX 值。

注意：报文中寄存器起始地址 00000 对应设备中 30001 地址；其他顺延。

本例：读 11H 号从站输入寄存器值，起始地=0008H=8，对应地址 30009；寄存器数=0001；末地址=30009；

因此，本询问报文功能是：读 01 号从站 1 个保持寄存器 30009 的值；

从站应答格式：（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	05	01

PDU 部分：

功能码	字节计数	输入寄存器低位 30009	输入寄存器高位 30009
04	2	01	01

功能：从站返回输入寄存器 30009 的值；（30009）=0101H

7.3 预置单寄存器

功能码：06H

主站询问报文格式（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	06	01

PDU 部分：

功能码	寄存器地址高位	寄存器地址低位	数据高位	数据低位
06	00	08	00	17

功能：读从站输入寄存器 3XXXX 值。

功能：预置从站单个保持寄存器值, 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 01 号从站单个保持寄存器值，寄存器地址为 0008H=8，对应地址 40009；

因此，本询问报文功能是：预置 01 号从站 1 个保持寄存器值；0017H→40009;

应答格式（MBAP 报文头+PDU）：

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	06	01

PDU 部分：

功能码	寄存器地址高位	寄存器地址低位	数据高位	数据低位
06	00	08	00	17

7.4 预置多寄存器

功能码：10H

主站询问报文格式：（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	0B	01

PDU 部分：

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
10	00	87	00	02	04	01	05	0A	10

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 01 号从站多个保持寄存器值，寄存器起始地=0087H=135，对应地址 40135；线圈数=0002H=2；末地址=40135+2-1=40136；

因此，本询问报文功能是：预置 01 号从站 2 个保持寄存器值；0105H→40135; 0A10H→40136.

应答格式：（MBAP 报文头+PDU）

MBAP 报文头部分：

事务元标识符		协议标识符		长度		单元标识符
E3	76	00	00	00	06	01

PDU 部分：

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
10	00	87	00	02

附录四 主站网关 2.0 与 3.0 的技术指标对比

技术指标名称\设备型号	PBMG-ETH-2.0	PBM-ETH-3.0
PROFIBUS 协议标准	DPV0	DPV0，**DPV1(C1,C2)**
所带从站个数	两个 DB 口共 31 个	两个 DB 口共 62 个
波特率	9.6K、19.2K、93.75K、187.5K、500K、1.5M	9.6K、19.2K、**45.45k**、93.75K、187.5K、500K、1.5M、**3M、6M**
最大 DPV0 IO 数据量	4k 输入，4k 输出	8k 输入，8k 输出
最大从站配置数据量	4k	8k
主站安全模式	不支持	支持 支持故障安全从站，支持向从站的安全输出
同步冻结功能	不支持	支持
设置从站地址	不支持	支持
网关 DTM/通信 DTM	不提供	提供
以太网接口数量	2 个，但不可以同时使用	2 个，可以同时使用
以太网接口通信距离	60m	100m
以太网接口工作模式	单网口工作模式	支持交换机模式，用于组建菊花链网络 支持独立双网口模式，用于组建双以太网冗余系统
是否支持 IP 冲突检测	不支持	支持
支持的 Modbus TCP 连接数	1 个	4 个（交换机模式下共 4 个，双网口模式下每个网口上支持 4 个）
Modbus TCP 存储区	DPV0 的 IO 数据区	DPV0 的 IO 数据区 寄存器区 DPV1 数据区 诊断数据区 系统日志数据区
Modbus TCP 应答扩展错误码	不支持	支持
DP 线缆故障指示灯	不支持	支持 可以检测 AB 线短路，AB 线连接不好时通时断的问题
Modbus TCP 活动指示灯	不支持	支持
设备识别功能	不支持	支持
设备名称,设备描述信息写入	不支持	支持
网关/主站/从站在线监控功能	部分支持从站的在线监控	对主站网关设备自身，DP 主站部分，DP 从站进行全面的在线运行监控
通过设备 DTM 操作 DP 或 PA 从站	不支持	支持
系统日志	不支持	支持
固件升级	不支持	支持
生成系统报告	不支持	支持

附录五 有毒有害物质表

根据中国《电子信息产品污染控制管理办法》的要求出台

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

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

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

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

现场总线 PROFIBUS（中国）技术资格中心
北京鼎实创新科技股份有限公司
电话：010-82078264、010-62054940　　传真：010-82078264
地址：北京德胜门外教场口 1 号，五号楼 A-1　　邮编：100120
Web:www.c-profibus.com.cn　　Email: tangjy@c-profibus.com.cn