如何实现西门子 S7-300 PLC 与 DCS 控制系统的通信

——上海泗博自动化 Modbus 转 PROFIBUS-DP 网关的应用

摘要：本文就西门子 S7-300 系列 PLC 与横河 CS3000 型 DCS 集散控制系统的之间的通信，介绍如何实现 Modbus 和 PROFIBUS-DP 协议设备的相互通信、上海泗博自动化的 Modbus 转 PROFIBUS-DP 网关 PM-160 在其中的应用，以及这两种不同通信协议的通信方式。

关键词：Modbus 协议　PROFIBUS-DP 协议　Modbus 转 PROFIBUS-DP　串口转 PROFIBUS-DP　分布式控制系统　通信网络

一. 引言

现代工业的迅速发展，不断促进着自动化控制技术及设备通信技术创新的发展。当前，PLC、DCS、智能仪表等已广泛应用到现场生产控制系统中，并发展到由上述设备相互协同、共同面向整个生产过程的分布式工业控制系统。在此系统中，现场总线通信技术至关重要。本文就某水利站分布式控制系统项目，介绍上海泗博自动化的 Modbus 转 PROFIBUS-DP 协议网关设备的应用。

二. 系统组成

1、系统结构

本系统构成如图 1，其中略去了西门子 S7-300PLC 之外的其它现场级控制设备。系统上位机采用横河 CS3000 型 DCS 集散控制系统，实现对整个水利项目进行集中监控。下位机之一采用的是西门子 S7-300 系列 PLC，实现对现场各种智能仪表，包括现场电机、智能开关、变频器、传感器等执行、检测设备的启停控制、信息采集等操作。

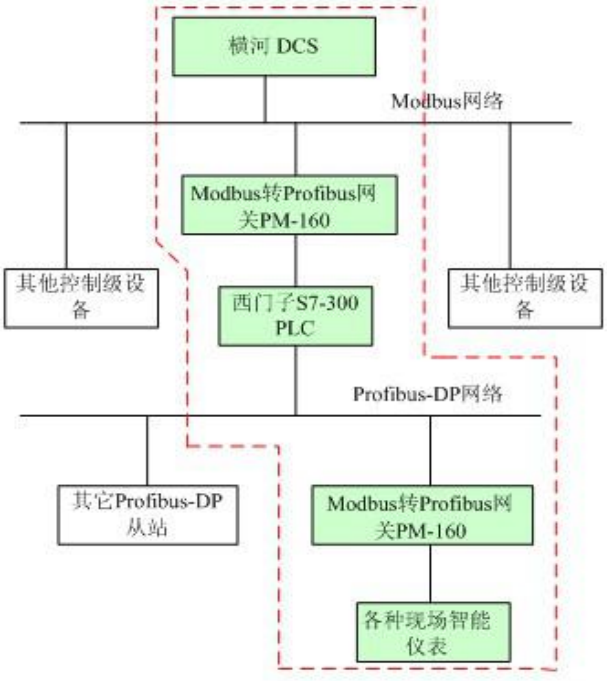

图 1 系统结构

在上图所示系统结构中，现场各种智能仪表（采用的是 Modbus 协议或者各种非标协议，接口为 RS485、RS422 或者 RS232）都能够通过上海泗博自动化的通用串口（Modbus/RS485/RS422/RS232）转 PROFIBUS-DP 网关 PM-160 连接到西门子 S7-300PLC。此时，网关 PM-160 在串口侧的协议类型为 Modbus 主站或者通用模式。横河 DCS 对西门子 S7-300PLC 的数据采集和监控同样需要使用上海泗博自动化的通用串口（Modbus/RS485/RS422/RS232）转 PROFIBUS-DP 网关 PM-160，此时，网关 PM-160 在串口侧的协议类型为 Modbus 从站。

2、通信网络组成

2.1 PROFIBUS 协议简介

PROFIBUS 是目前国际上通用的现场总线标准之一，以其独特的技术特点、严格的认证规范、开放的标准、众多厂商的支持和不断发展的应用行规，已成为很重要的和应用很广泛的现场总线标准。

PROFIBUS 现场总线通讯协议包括三个主要部分：

(1). PROFIBUS DP：主站和从站之间采用轮循的通讯方式，主要应用于自动化系统中单元级和现场级通信；

(2). PROFIBUS PA：电源和通信数据通过总线并行传输，主要用于面向过程自动化系统中单元级和现场级通讯；

(3). PROFIBUS FMS：定义了主站和主站之间的通讯模型，主要用于自动化系统中系统级和车间级的过程数据交换；

其中，PROFIBUS-DP 是高速网络，通讯速率达到 12M。PROFIBUS-DP 可以连接远程 I/O、执行机构、智能马达控制器、人机界面 HMI、阀门定位器、变频器等智能设备， 一条 PROFIBUS-DP 总线可以最多连接 123

个从站设备。PROFIBUS-DP 的拓扑结构可以是总线型、星型和树型，通讯介质可以是屏蔽双绞线、光纤，也支持红外传输，采用双绞线时，不加中继器最远通讯距离可达 1.2 公里，最多可以采用 9 个中继器，最远通讯距离可达 9 公里。采用光纤时，最远通讯距离可达 100 公里以上，其中采用多膜光纤，两点间最远距离可达 3 公里，采用单膜光纤时，两点间最远距离可达 3 公里。

2.2 Modbus 协议简介

Modbus 协议是一种适用于工业控制领域的主从式串口通讯协议，它采用查询通讯方式进行主从设备的信息传输，可寻址 1-247 个设备地址范围。协议包括广播查询和单独设备查询两种方式，二者区别就是广播查询不需要从设备回应信息，主、从设备查询通讯过程见图 2：

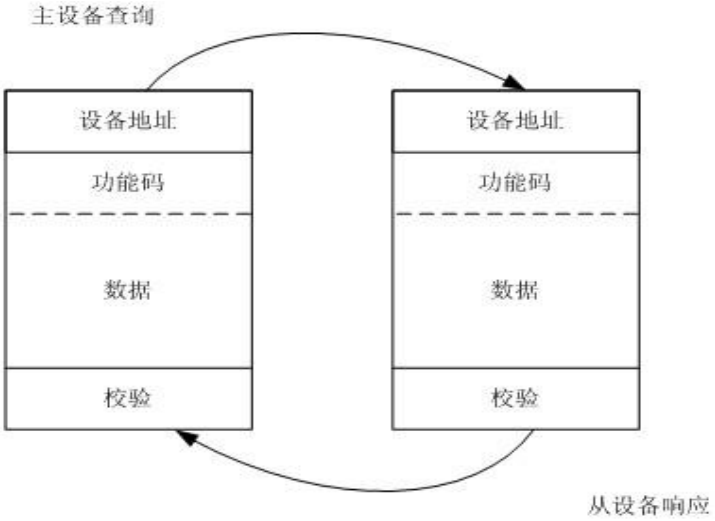

图 2 Modbus 主、从设备查询响应

Modbus 协议常用功能码如图 3 所示：

功能码	名称	作用
01	读线圈状态	读取一组逻辑线圈的当前状态：ON or OFF
02	读输入状态	读取一组输入线圈的当前状态：ON or OFF
03	读保持寄存器	读取一个或多个保持寄存器中的值
04	读输入寄存器	读取一个或多个输入寄存器中的值
05	写单个线圈	强制一个逻辑线圈的状态
06	写单个寄存器	把一个具体的值装入一个保持寄存器
15	写多个线圈	强制多个逻辑线圈的状态
16	写多个寄存器	将一组具体的值装入多个保持寄存器

图 3 Modbus 协议常用功能码

Modbus 协议有两种传输模式：ASCII 模式和 RTU 模式。同波特率下，RTU 模式较 ASCII 模式能传输更多的数据，所以工业网络大都采用 RTU 模式。RTU 模式下的信息传输报文格式如图 4：

起始符	设备地址	功能码	数据	校验	结束符
TI-T2-T3-T4	1 byte	1 byte	N byte	2 byte	TI-T2-T3-T4

图 4 Modbus RTU 信息报文格式

它没有起始位和停止位，而是由至少 3.5 个字符间隔时间作为信息的起始和结束标志。信息帧所有字符位由 16 进制字符 0-9、A-F 组成。

Modbus RTU 通讯协议帧结构：

类型	Bit数	备注
起始位	1	
数据位	8	最小的有效位先发送
奇偶校验位	1	无校验则无
停止位	有校验时停止位1Bit，无校验位时停止位1Bit或者2Bit	

图 5 RTU 通讯协议帧格式

Modbus RTU 方式主站读取从站寄存器数据示例：主设备查询。

地址	功能码	第一个寄存器的高字节地址	第一个寄存器的低字节地址	寄存器的数量的高字节	寄存器的数量的低字节	校验
01	03	00	10	00	01	XX（2Bytes）

图 6 主设备查询格式

Modbus RTU 方式主站读取从站寄存器数据示例：从设备响应。

地址	功能码	字节数	数据高字节	数据低字节	校验
01	03	02	25	20	XX（2Bytes）

图 7 从设备响应格式

2.3 网络构成及硬件介绍

如图1所示，在该系统设计中有两个网络使用了上海泗博自动化的Modbus转PROFIBUS-DP网关PM-160。网关在这两个网络中的作用不一样，其中：

在上层网络中（建立西门子 S7-300PLC 和横河 DCS 连接通信），Modbus 转 PROFIBUS-DP 网关 PM-160 在 Modbus 侧做 Modbus 从站，在 PROFIBUS-DP 侧做从站，建立 PROFIBUS-DP 主站（西门子 S7-300 PLC）和

Modbus 主站（横河 CS3000）的通信。DCS 通信部分采用横河型号为 ALR121 的通信模块，并配套横河提供的 Modbus 通信软件包，该通信模块最大通信数据容量为 4000 字。通过上海泗博自动化的网关配置软件对 PM-160 进行相关配置，将 DCS 的读、写指令及数据做相应转换、存储，并映射到西门子 PLC 的输入、输出映像区，以实现对上下位机控制信息的实时传输。

在下层网络中（建立西门子 S7-300PLC 和现场智能仪表的连接通信），Modbus 转 PROFIBUS-DP 网关 PM-160 在 Modbus 侧做 Modbus 主站，在 PROFIBUS-DP 侧做从站，建立 Modbus 从站（现场各种智能仪表（现场电机、智能开关、变频器、传感器等））与 PROFIBUS-DP 主站（西门子 S7-300PLC）的通信。串口网络（现场智能仪表)设备接口为 RS485 或者 RS232,它们都可以通过上海泗博自动化的 Modbus 转 PROFIBUS-DP 网关 PM-160 实现与西门子 S7-300PLC 的连接通信。其中，通过使用网关的配套配置软件对 PM-160 进行相关配置，将需要采集的从站设备信息通过网关读、写命令及数据转换、存储，映射到西门子 PLC 的输入、输出映射区，以实现 PLC 对现场智能仪表数据的采集和监控。

三. Modbus 转 PROFIBUS-DP 网关 PM-160 的配置

PM-160 是通用型 Modbus/RS485/RS422/RS232 到 PROFIBUS-DP 的协议转换网关，在网关 RAM 中建立了 Modbus/RS485/RS422/RS232 到 PROFIBUS-DP 的映射数据区，由软件实现 Modbus/RS485/RS422/RS232 到 PROFIBUS-DP 的协议转换和数据交换。凡具有 RS485/422/232 接口的设备（Modbus 协议或者非标协议）都可以通过 PM-160 与现场总线 PROFIBUS-DP 互联。其中，PM-160 在与 PROFIBUS-DP 通讯是作为 PROFIBUS-DP 从站，PM-160 在与串口设备通信时，可以作 Modbus 主站、Modbus 从站，也支持与非标串口设备实现数据透明传输。通过在西门子 STEP7 中注册网关 PM-160 的 GSD 文件，即可在该编程软件中对该网关进行相关硬件和软件配置，完成相应的通讯功能。请见如下详细的硬件和软件配置方法：

1、 Modbus 转 PROFIBUS-DP 网关 PM-160 的硬件配置

PM-160 的 PROFIBUS-DP 从站地址可以通过网关的硬件旋码开关或者配置按钮来设置。旋码开关有两位，左侧位设置地址高位（十位），右侧位设置地址低位（个位）。通过拨码开关可设置网关 PM-160 处于正常运行状态或者配置状态。当 PM-160 处于配置状态时，用户可通过配套配置软件设置相关读写命令和参数。

PM-160 自带标准 PROFIBUS-DP 接口，用户可使用标准 PROFIBUS-DP 连接头和标准的 PROFIBUS-DP 电缆将其连接至 PROFIBUS-DP 现场总线中。

PM-160 提供 RS485/422/232 三种串口，Modbus 从站、主站设备以及用户非标串口设备可以通过这三种接口实现与网关 PM-160 的连接通讯。PM-160 没有内置终端电阻，在进行 RS485 通信时，请注意在 RS485 总线终端各添加一个终端电阻（120 欧姆）。

2、Modbus 转 PROFIBUS-DP 网关 PM-160 的软件配置

1）使用配套软件设置 PM-160 的现场总新和子网相关参数和命令

通过拨码开关将 PM-160 设置为配置状态，打开安装的配置软件（产品光盘或者访问 http://www.sibotech.net/DownLoad01.asp）：

当实现 PLC 与 DCS 通信时，子网协议类型设置为 Modbus 从站，并设置串口通信波特率、数据位、奇偶校验位、停止位、PM-160 作为 Modbus 从站的地址、通信接口。其中，串口通信波特率、数据位、奇偶校验位、停止位的设置应该和所连接的 Modbus 主站设备（DCS）一致；

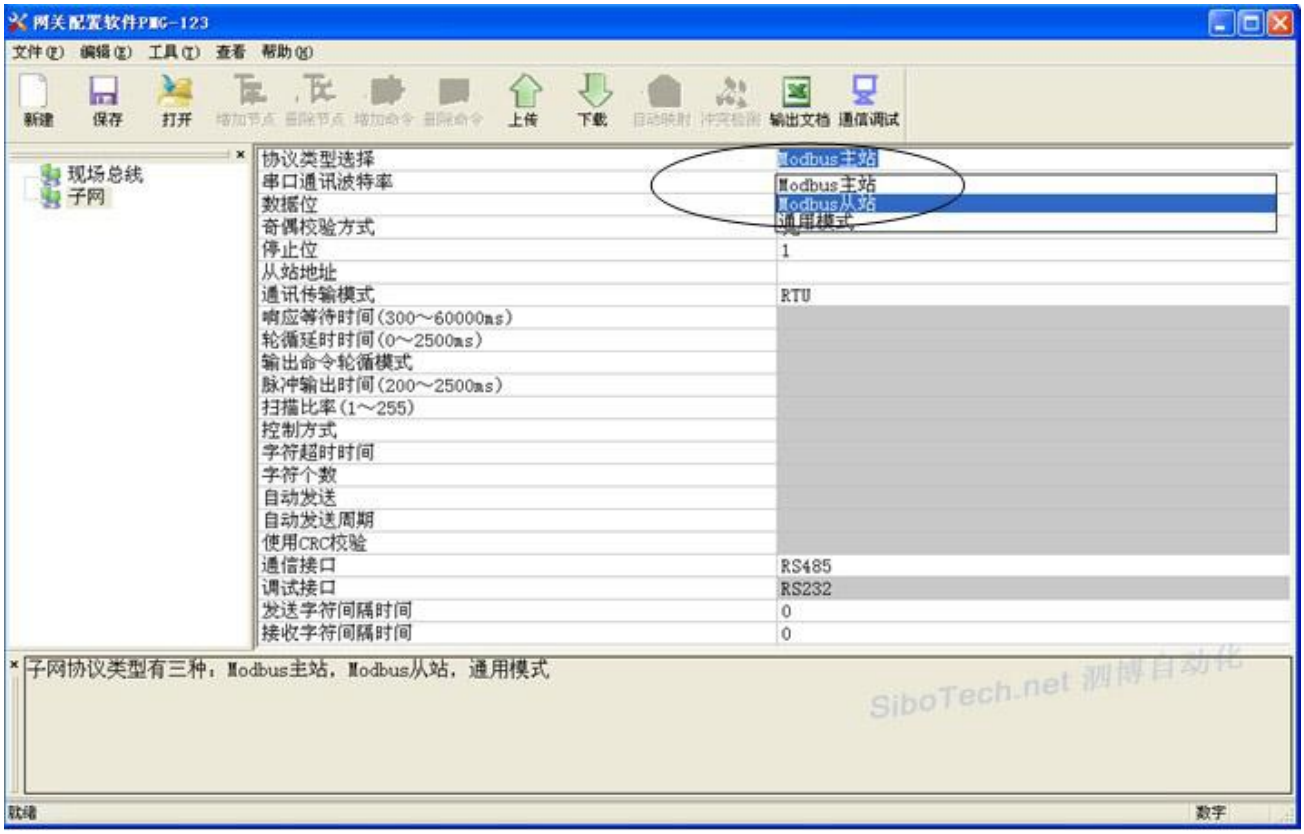

图 8 PM-160 在 Modbus 侧作 Modbus 从站（连接 PLC 和 DCS）

当实现 PLC 与 Modbus 设备通信时，子网协议类型设置为 Modbus 主站，并设置串口通信参数、通讯传输模式、通信接口等。其中，串口通信参数的设置应该和所连接的 Modbus 从站设备一致：

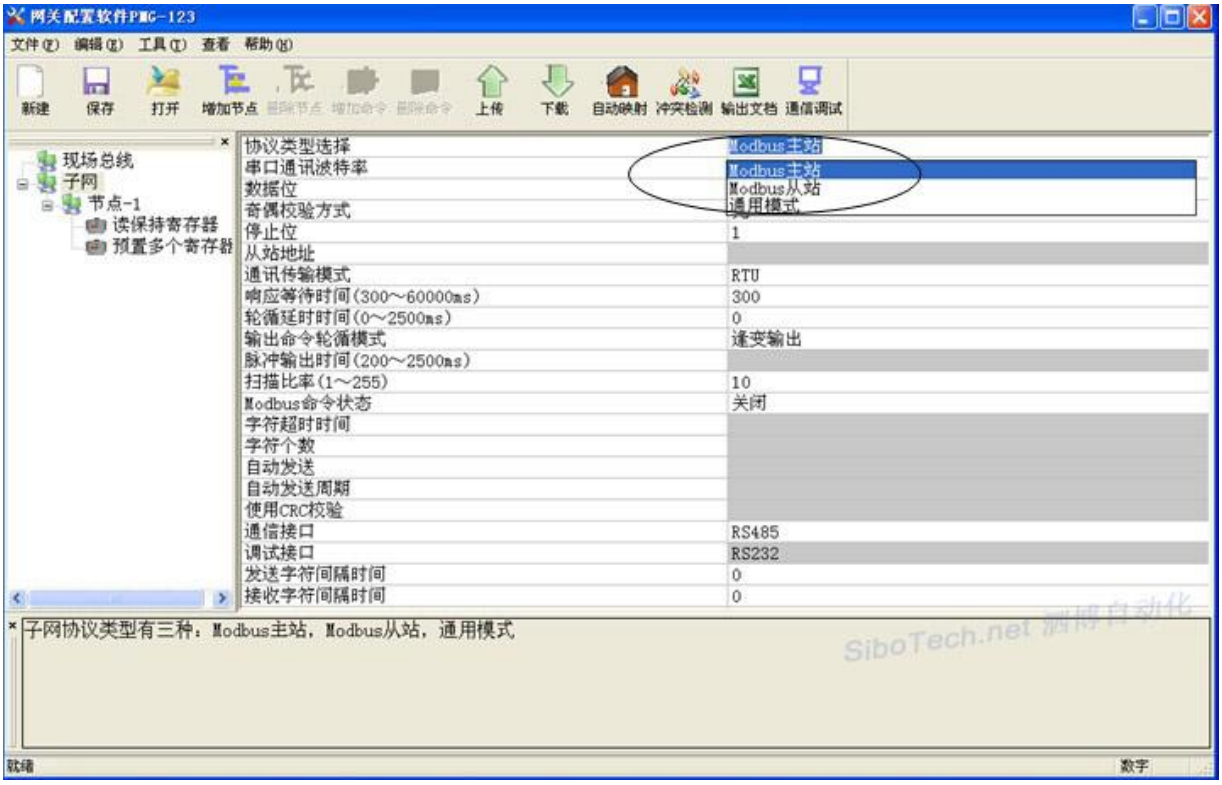

图 9 PM-160 在 Modbus 侧作 Modbus 主站（连接 PLC 和 Modbus 从站）

其中，图 9 中的“节点-1”表示连接的从站设备地址为 1，配置了“读保持寄存器”和“预置多个寄存器”两条命令，表示网关读取了从站对应地址的数据，并且能够输出数据到 Modbus 从站设备，命令配置方法如下：

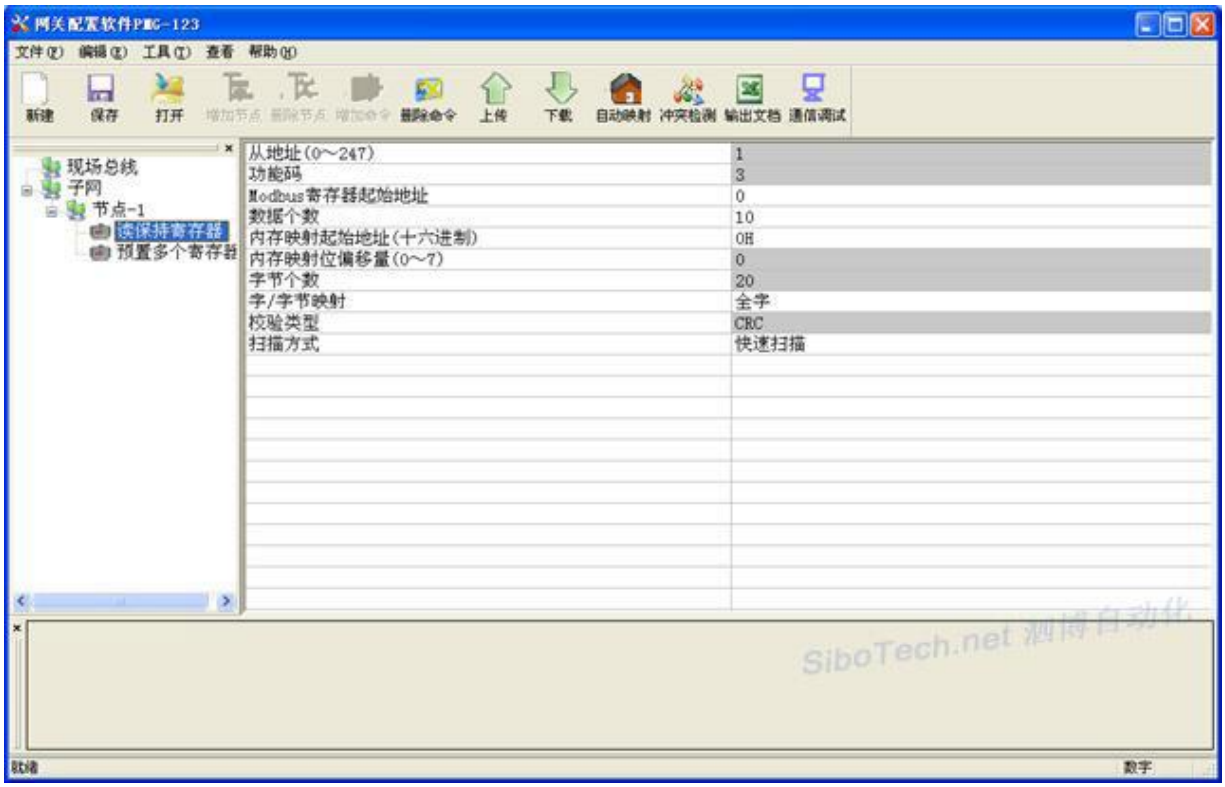

图 10 PM-160 在 Modbus 侧作 Modbus 主站（命令配置）

在 STEP7 中对网关 M-160 进行组态设置；

Modbus 寄存器起始地址：用户输入目标采集数据的 Modbus 寄存器起始地址；

数据个数：目标数据的寄存器个数或者线圈条数；

内存映射起始地址：Modbus 从站设备数据的对应内存缓冲区地址；

当实现 PLC 与非标协议设备通信时，子网协议类型设置为通用模式，并设置串口通信参数、控制方式、通信接口等。其中，串口通信参数的设置应该和所连接的非标串口设备（现场智能仪表）一致：PM-160 支持的通用模式即透明传输模式，用户可通过数据中的数据长度和事务序列号以判断数据完整性和是否是一帧新的数据。

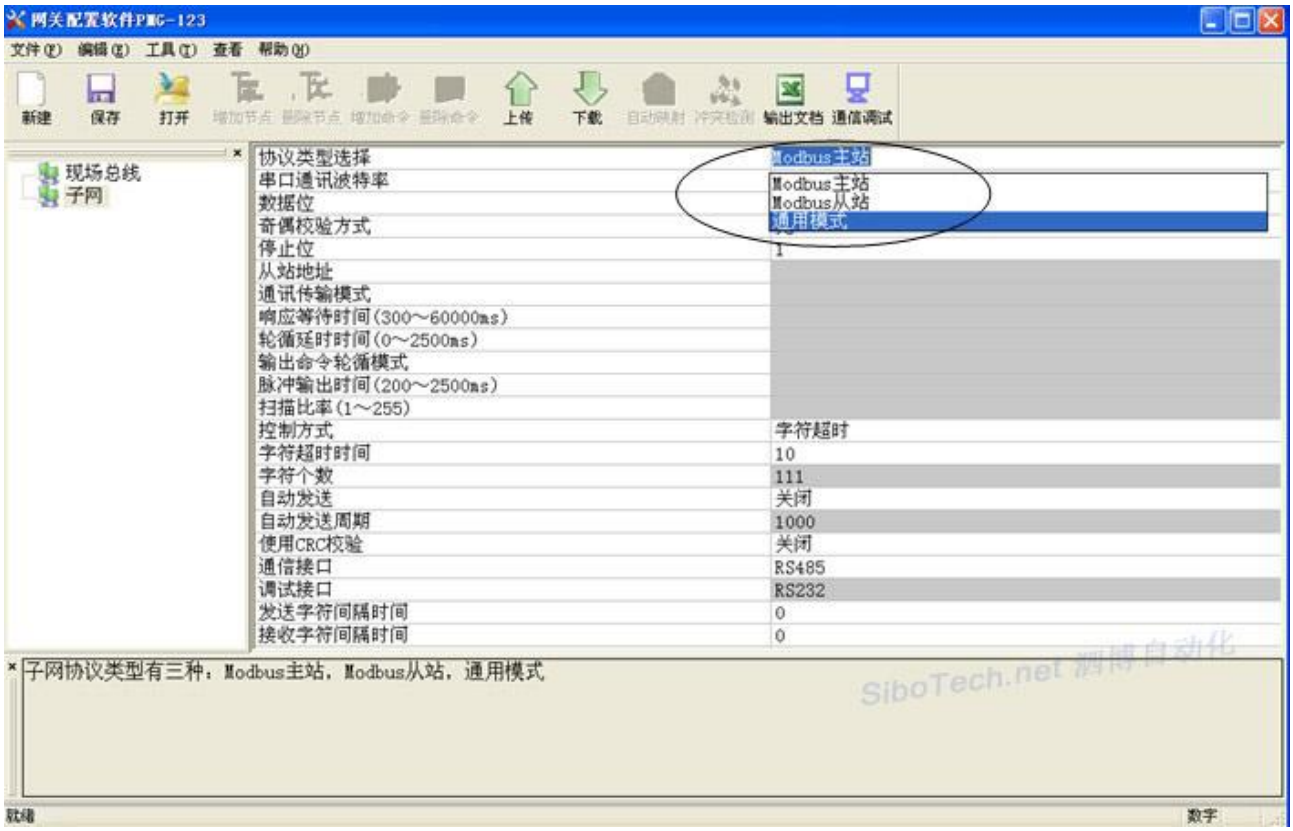

图 11 通用模式

在 STEP7 中对网关 M-160 进行组态设置

在 STEP7 的硬件组态界面，导入 PM-160 对应的 GSD 文件，把 PM-160 的配置文件添加到 STEP7 的设备配置库中。用户可在硬件组态界面找到注册的设备：Catalog->PROFIBUS DP->Additional Field Devices->General->CONVERTER->PM-160。

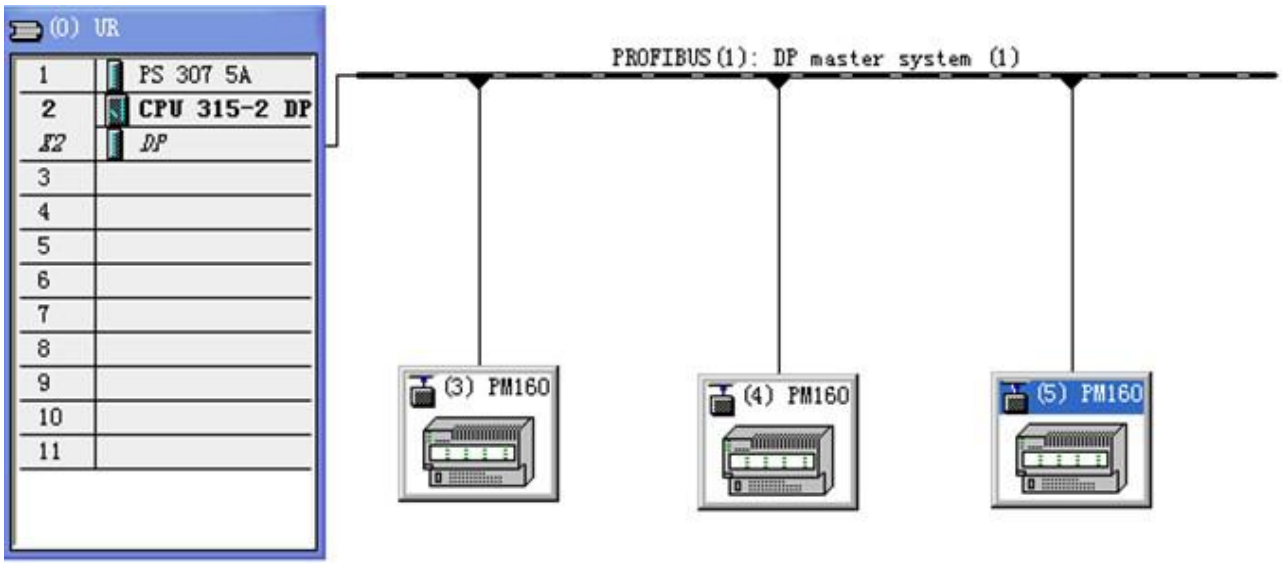

图 12 组态界面

将 PM-160 添加到 STEP7 的组态页面后，可以插入相应的数据块进行映像区地址映射。PM-160 提供的数据块如下：

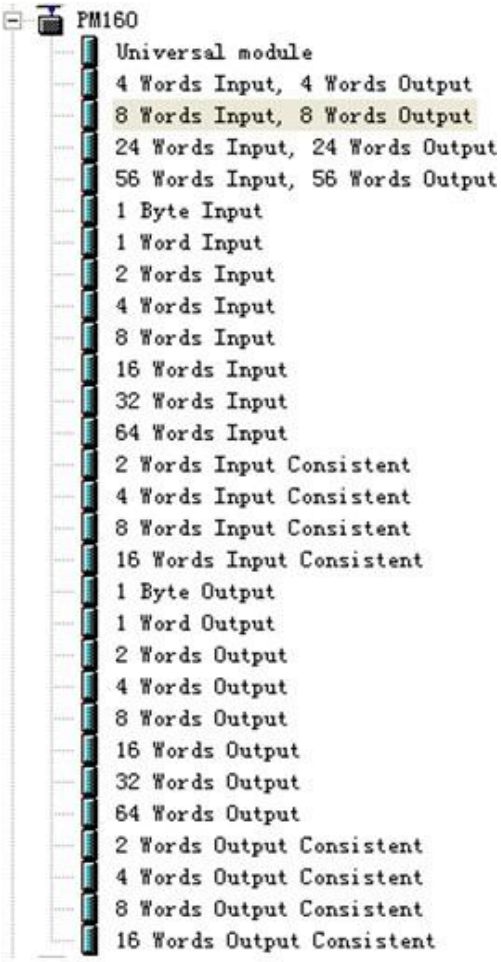

图 13 PM-160 提供的数据块

推动需要的输入输出数据块到网关对应的槽位。如下图所示，将数据块“24Words Input，24Words Output”拖动到 PROFIBUS-DP 从站地址为 3 的 PM-160 的槽位中，此时，对应的映射区地址分别为 256，PLC 程序需通过 PIW256（PIB256）或者 PQW256（PQB256）对相应的数据进行寻址访问。

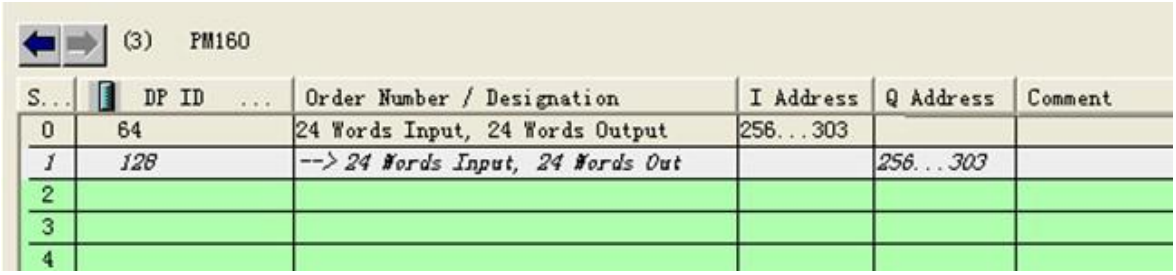

图 14 PLC 映像区起始地址（命令配置）

四. 数据读写

1、DCS 读写 PLC 数据

DCS 作为 Modus 主站通过 PM-160 读写 PLC 数据，使用 04H 功能码读数据，对应的寄存器起始地址为 0H（30001H），使用 10H（03H）功能码写数据，对应的寄存器起始地址为 0H（40001H）。

2、PLC 读写现场智能仪表数据

1）PLC 读写 Modbus 从站设备数据

PLC 通过 PM-160 发送 Modbus 主站指令读写现场串口设备数据。映像区起始地址和网关内存映射起始地址对应关系如下：以图 14 中的配置为例。

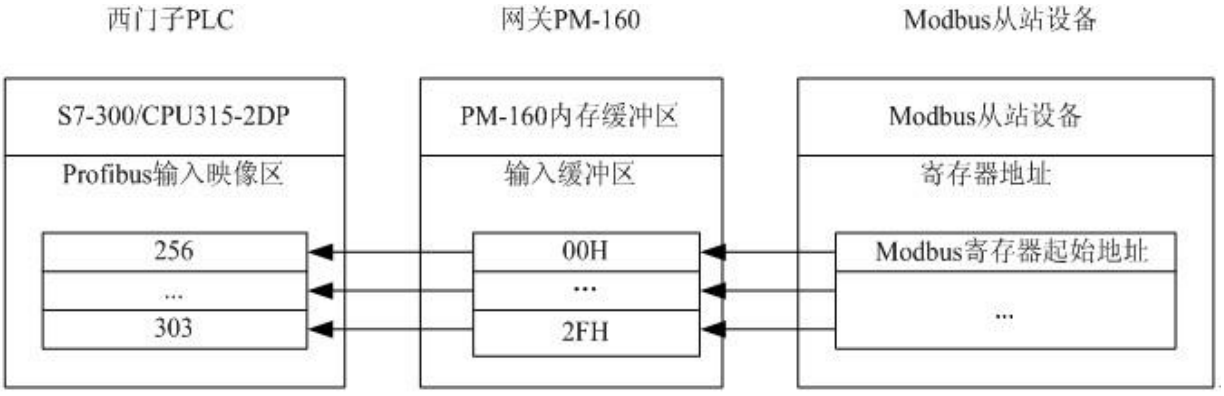

图 15 PLC 通过 PM-160 读写 Modbus 从站设备数据地址对应关系

2）PLC 读写非标串口设备数据

PLC 的输入映射区前两个字节分别表示接收的串口数据长度和事务序列号，其它为接收到的数据。事务序列号变化，表示接收到了一帧新的串口数据。其中，可通过配置软件设置是否开启串口数据长度功能。PLC 的输出映射区前两个字节分别表示发送的串口数据长度和事务序列号，其它为要发送的串口数据。事务序列号变化，PLC 发送相应长度的串口数据。

五. 结束语

在该系统中，Modbus 转 PROFIBUS-DP 网关 PM-160 扮演了三种角色：建立 Modbus 主站和 PROFIBUS-DP 主站之间的连接通信（Modbus 主站模式）；建立 Modbus 从站和 PROFIBUS-DP 主站之间的连接通信（Modbus 从站模式）；建议非标串口设备和 PROFIBUS-DP 主站之间的连接通信（通用模式）。自本通信系统运行以来，整个系统通讯正常，有效保证了整个水利工程控制系统的正常运行。使用上海泗博自动化的 Modbus 转 PROFIBUS-DP 网关可以更大地方便自动化工业现场的控制和操作。