Modbus 使用说明详解

北京昆仑通态

2009-2-10

目录

前　言

Modbus 协议，是由 Modicon 公司开发设计的一种通讯协议，目前已经作为一种标准，在工业领域被广为应用。许多 PLC、DCS、智能仪表等工业设备都使用 Modbus 协议作为其通讯协议标准。

MCGS 软件及 TPC 触摸屏支持标准 ModbusRTU、ASCII、TCP 协议，并以此作为与其他软件及设备互通的标准的通讯协议。但目前由于很多使用 MCGS 的用户对 Modbus 协议并不十分了解，在使用 MCGS 的 Modbus 主从站驱动构件进行通讯时，常遇到很多问题而不知道如何有效解决。而且，由于对 Modbus 协议的理解及实现上的差别，很多国内厂家的设备所说的 Modbus 协议，在功能码支持、最大数据长度、校验及数据解码顺序等方面与标准 Modbus 协议实现均存在细节的差别，也导致了与此类设备通讯存在很多问题甚至无法正常通讯。

本文档的编写目的，是为了使用户对 Modbus 协议有进一步的了解，理解并掌握 MCGS 的 Modbus 主从站相关驱动构件的使用，并熟悉 Modbus 主从站通讯实现方案，掌握通讯常见问题的判断和解决方法。现对各章节内容简要概况说明如下：

第一、二章介绍了 Modbus 协议以及 ModbusRTU、ASCII、TCP 协议帧格式及其区别。

第三、四章讲解了 MCGS 嵌入版 Modbus 主从站驱动构件，驱动构件的基本使用、调试方法和相关注意事项。

第五章主要讲解数据转发（从站）与主站配合使用的实现，为用户提供 Modbus 主从站的常规通讯解决方案。

第六章主要讲解 MCGS 的 Modbus 主从站驱动常见问题的判断和处理方法，以提高用户解决相关问题的能力。

第七章主要讲述了 Modbus 协议的分析技巧，为用户提供实际问题的处理解决方案。

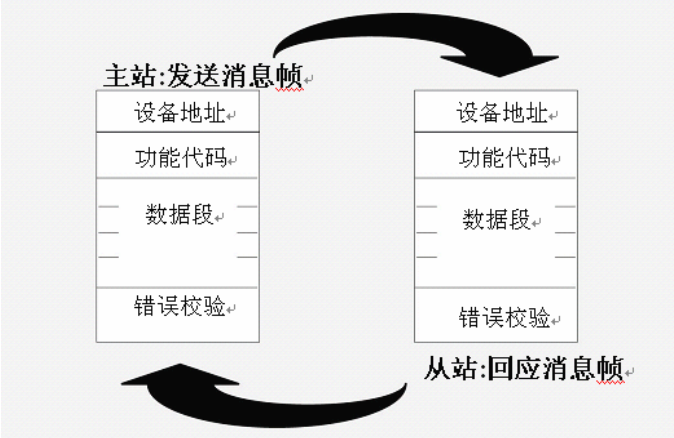
一、Modbus 协议简介

Modbus 协议是由 Modicon 公司开发设计的一种通信传输协议，在 1979 年该公司成为施耐德自动化(Schneider Automation)部门的一部分。现在 Modbus 已经是在工业领域被广为应用的最流行、最广泛的真正开放、标准的网络通讯协议。此协议支持传统的 RS-232、RS-422、RS-485 和以太网设备。许多工业设备，包括 PLC、DCS、智能仪表等都在使用 Modbus 协议作为其通讯标准。

1、 Modbus 协议主从响应过程

Modbus 协议规定了消息、数据的结构、命令和应答的方式，数据通讯采用 Maser/Slave 方式，即：通讯两方规定为“主站”（ Master）和“从站”（ Slave），主站发出数据请求消息，从站接收到正确消息后，响应请求并回应数据给主站；主站也可以发命令消息修改从站的数据。

主站可向多个从站发送通信请求，而每个从站都有唯一的设备地址，并按地址识别主站发来的消息。其命令及响应过程如下图所示:



Modbus 主从站命令响应过程

主从站命令响应过程说明：主站作为命令发起方，主动向指定的从设备发送命令消息帧，要求进行寄存器区的数据读取或写入，而从站被动接收主站命令，在收到主站消息帧后，首先判断设备地址，如果是发给从站本身，则根据功能代码做出相关的响应，并按功能代码不同组成数据帧或操作回应帧，回应给主站。如不是本站地址，则丢弃消息帧，继续等待主站命令帧。主站发送命令帧后，接收回应帧正确，表明通讯响应过程完成。如果主站超出约定时间未收到从站的回应帧，则说明与从站通讯失败。

如果主站所送命令帧从站无法识别，或从站无法满足主站的命令帧要求，例如：读取超出从站寄存地址范围的数据，则从站也将回应包含错误提示的消息帧，主站可根据错误提示，判断错误原因。

2、 Modbus 的寄存器区和常用功能码

Modbus 协议定义中，共包含 4 种寄存器区和多种功能码。不同功能码代表对不同寄存器区数据的不同操作。Modbus 的寄存器区和 MCGS 支持的常用功能码如下表所示：

寄存器	读取功能码	写入功能码	功能码说明	示例
[1 区]输入继电器	**02**	—	02: 读取输入状态	10001 输入继电器,地址 1
[0 区]输出继电器	**01**	**05** **15**	01: 读取线圈状态 05: 强制单个线圈 15: 强制多个线圈	00002 输出线圈,地址 2
[3 区]输入寄存器	**04**	—	04: 读输入寄存器	30005 输入寄存器,地址 5
[4 区]输出寄存器	**03**	**06** **16**	03: 读保持寄存器 06: 预置单个寄存器 16: 预置多个寄存器	40001 保持寄存器,地址 1

注：其中输出继电器也称作**线圈**，输出寄存器也称**保持寄存**器。

二、Modbus 协议帧格式

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）。在特定总线或网络上的 Modbus 协议映射能够在应用数据单元（ADU）上引入一些附加域。Modbus 通用帧格式如下:

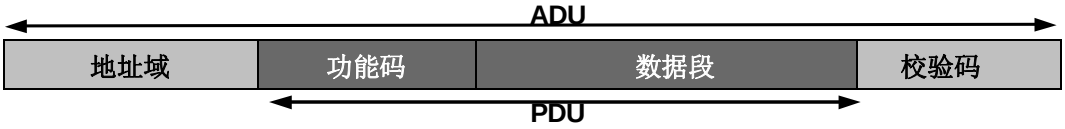


图 1. Modbus 通用帧格式

根据协议格式和总线方式不同，Modbus 协议可分为 RTU,TCP 和 ASCII 三种格式，具体格式如下：

1、 ModbusRTU：

RTU	设备地址	功能码	数据段	校验码 CRC
帧格式	1 字节	1 字节	N 字节	2 字节

示例: 设备地址 1, 用 03 功能码读取 40001 寄存器(即:4 区,寄存器地址为 1)为例，读取值为 123

主站	地址	功能码	起始地址 Hi	起始地址 Lo	数据个数 Hi	数据个数 Lo	CRC 校验 Lo	CRC 校验 Hi
发送帧	01	03	00	00	00	01	84	0A

从站	地址	功能码	字节数	寄存器值 Hi	寄存器值 Lo	[……]	CRC 校验 Lo	CRC 校验 Hi
回应帧	01	03	02	00	7B		F8	67

2、 ModbusASCII：

ASCII	帧头	设备地址	功能码	数据段	校验码 LRC	回车	换行
帧格式	:	2 字符	2 字符	N 字符	2 字符	2 字符	

示例: 设备地址 1, 用 03 功能码读取 40001 寄存器(即:4 区,寄存器地址为 1)为例，读取值为 123

主站	帧头	地址		功能码		起始地址 Hi		起始地址 Lo		数据个数 Hi		数据个数 Lo		校验码 LRC		回车	换行
发送帧	:	0	1	0	3	0	0	0	0	0	0	0	1	F	B	\r	\n
(Hex)	3A	30	31	30	33	30	30	30	30	30	30	30	31	46	42	0D	0A

从站	帧头	地址		功能码		字节数		寄存器值 Hi		寄存器值 Lo		[……]	校验码 LRC		回车	换行
回应帧	:	0	1	0	3	0	2	0	0	7	B		7	F	\r	\n
(Hex)	3A	30	31	30	33	30	32	30	30	37	42		37	46	0D	0A

注：\r 和\n 为回车(CR)和换行(LF)的转义字符表示方法，而非实际可见的字符。

3、 ModbusTCP：

TCP	报文头	设备地址	功能码	数据段
帧格式	6 字节	1 字节	1 字节	N 字节

示例: 设备地址 1, 用 03 功能码读取 40001 寄存器(即:4 区,寄存器地址为 1)为例，读取值为 123

主站	MBAP	地址	功能码	起始地址 Hi	起始地址 Lo	数据个数 Hi	数据个数 Lo
发送帧	000006	01	03	00	00	00	01

从站	MBAP	地址	功能码	字节数	寄存器值 Hi	寄存器值 Lo	[……]
回应帧	000006	01	03	02	00	7B	

说明: 1. Hi 代表高 8 位,Lo 代表低 8 位。

2. [……] 代表读取多个数据时相关的数据信息。

3. 以上示例只介绍了 4 区寄存器 03 功能码的协议格式，其他功能码协议格式请参见附录 1。

4、 RTU、TCP、ASCII 协议格式区别

ModbusRTU,TCP 和 ASCII 三者协议格式区别对比如下：

	ModbusRTU		ModbusASCII		ModbusTCP
编码格式	16 进制(HEX)		ASCII 可见字符		16 进制(HEX)
帧头格式	无帧头		以":"为帧头		6 字节 MBAP 报文头
最大帧(ADU)长度	256 字节		513 字符		256 字节
数据帧(PDU)长度	253 字节		252 字节（504 字符）		249 字节
有效数据长度	约 124 字(248 字节)		约 124 字(496 字符)		约 122 字(244 字节)
串口数据位数	8 位数据位		7 位数据位		——
校验方式	CRC(循环冗余)		LRC(纵向冗余)		无
通讯方式	RS232C	RS485	RS232C	RS485	TCP/IP 以太网
组网方式	1 主:1 从	1 主:N 从	1 主:1 从	1 主:N 从	M 主:N 从
通讯效率	较高		较低		较高

说明：1、**组网方式**中：N 表示从站个数，不大于 247,从站地址范围为 1~247。M 表示主站个数，对于 ModbusTCP 从站，同时连接主站的个数 M 一般限制不超过 8 个。

2、**有效数据长度**：是指进行通讯时，通讯帧单元中所能包含的真正有效的数据的长度。例如：主站使用 03 功能码读取从站 4 区保持寄存器的数据，一次最多可以读取 124 个最小单位为字的数据，即：124 字(248 字节)。

由以上协议格式及对比可以看出：RTU 和 TCP 由于使用 16 进制进行传输，效率较高。而 ModbusASCII 格式通讯时，传送一个字节数据需要两个 ASCII 字符，通讯效率较前两个低。

目前 Modbus 协议已经成为业界的一个标准，很多 PLC、仪表控制器等设备均支持 Modbus 协议，一般来说 ModbusRTU 和 ModbusTCP 的比较多，而 ModbusASCII 由于通讯效率较低，使用也较少。

由于对 Modbus 协议的理解及实现上的细节差别，很多国内厂家的设备虽然支持 Modbus 协议，但在功能码支持、最大数据长度、校验及数据解码顺序等方面与标准 Modbus 协议实现均存在细节的差别。对于此类设备，我们称之为“非标准 Modbus 设备”，而 MCGS 的驱动构件，也充分考虑到并针对这种差别做了兼容性方面的处理，具体请参见第三章第 3 节说明以及驱动相关帮助。

三、MCGS 嵌入版 Modbus 相关驱动构件介绍

MCGS 软件提供了 Modbus 协议相关的驱动构件，通过 Modbus 驱动构件，MCGS 组态软件或嵌入式触摸屏可以作为主站与 Modbus 类设备通讯，实现数据的读写控制功能；也可以作为从站，与其他支持标准 Modbus 的软件或 HMI 进行通讯。本章将重点对各驱动构件及特点进行分类讲解。

1、 Modbus 驱动分类

现根据驱动及使用特点，对 MCGS 的 Modbus 驱动构件分类介绍如下：

通用设备驱动：适用于所有 Modbus 主从，以及 MCGS 软件与 TPC 触摸屏之间的数据转发通讯。

通用设备驱动	标准 ModbusRTU 设备	标准 ModbusTCP 子设备	Modbus 串口数据转发	ModbusTCPIP 数据转发
驱动目录	通用设备\ModBusRTU	通用设备\ModBusTCP	通用设备\ModBus 串口转发设备	通用设备\ModBusTcp 数据转发设备
基本协议	ModbusRTU 主站	ModbusTCP 主站	ModbusRTU 从站	ModbusTCP 从站
支持功能码	01,02,03,04,05,06,15(0x0F)，16(0x10)			
支持寄存器区	1 区(输入状态)，0 区(线圈)，3 区(输入寄存器)，4 区(保持寄存器)			
组态方式*	1 父:N 子	1 父:1 子	1 父:1 子	1 父:1 子
最大块长	96 字（可调整）	96 字（可调整）	120 字（固定）	120 字（固定）
解码顺序调整	可调 16/32 位整数,32 位浮点数解码顺序		可调 16/32 位整数,32 位浮点数解码顺序	
校验方式调整	可调整高低位顺序	—	—	
分块采集方式	可按最大块长或连续地址分块采集			
通讯日志功能	支持（在基本属性中设置）		不支持	
易用性接口支持	不支持		支持	
驱动特点	1.保持寄存器(4 区)，支持 MCGS 扩展的 128 字节字符读写功能 2.块长可以调整。		1.保持寄存器(4 区)，支持 MCGS 扩展的 128 字节字符读写功能 2.从站地址可在运行时通过设备命令修改。	
使用局限	1 不支持批量读写设备命令 2.4 区扩展的字符读写功能只限于与 MCGS 的 Modbus 从站设备配对实现。		4 区扩展的字符读写功能只限于与 MCGS 的 Modbus 主站设备配对实现。	

PLC 驱动：适用于莫迪康 PLC 等标准 Modbus 设备，针对 PLC 优化，支持动态分块。其中莫迪康 ModbusRTU 和莫迪康 ModbusTCP，也可作为主站与数据转发设备配对使用，用于 MCGS 软件与 TPC 触摸屏之间的数据转发通讯。

PLC 驱动	莫迪康 ModbusRTU	莫迪康 ModbusTCP	ModbusASCII
驱动目录	PLC\莫迪康\ModBus-RTU	PLC\莫迪康\ModBusTCP	PLC\莫迪康\ModbusASCII
基本协议	ModbusRTU 主站	ModbusASCII 主站	ModbusTCP 主站
支持功能码	01,02,03,04,05,06,15(0x0F)，16(0x10)		
支持寄存器区	1 区(输入状态)，0 区(线圈)，3 区(输入寄存器)，4 区(保持寄存器)		
组态方式*	1 父:N 子	1 父:N 子	1 父:N 子
最大块长	120 字（固定）	120 字（固定）	120 字（固定）
通讯日志功能	支持(设备命令)	支持(设备命令)	支持(设备命令)
解码顺序调整	可调 16/32 位整数,32 位浮点数解码顺序		—
校验方式调整	可调整高低位顺序	—	—
分块采集方式	可按最大块长或连续地址分块采集		—
易用性接口支持	支持		不支持
驱动特点	针对 PLC 优化，支持动态分块和批量读写设备命令		
使用局限	最大块长固定，无法用于对块长有特殊要求的非标准 Modbus 设备		

注：最大块长，即最大 1 次读写有效数据块的长度，与第二章第 4 节中有效数据长度描述相对应。

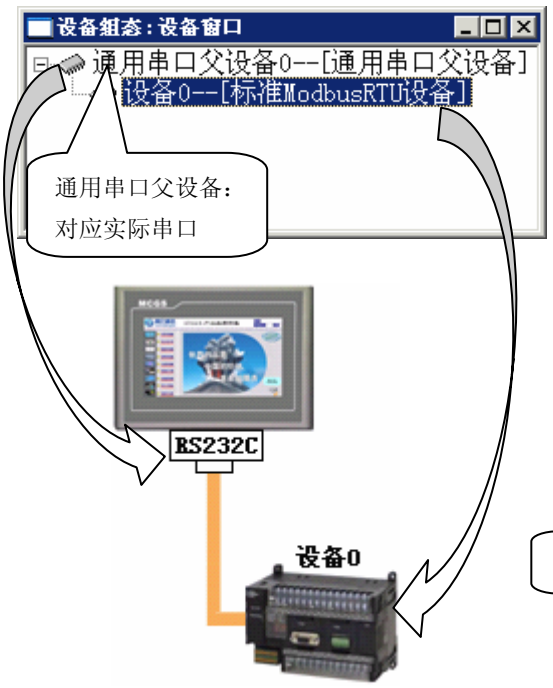
大多数情况下，建议使用通用设备目录下的驱动，如果是 PLC 等标准 Modbus 设备，对采集速度及读写控制有较高的要求，可以使用针对 PLC 优化的驱动，并可利用批量读写等功能，以提高效率。对于上分类对比表格中提及的部分功能及相关作用，我们在下面章节中做相应的讲解。

2、 组态及通讯组网方式

上面的对比表格中，提到了组态方式和组网方式，组态方式是指 MCGS 工程组态中父设备和子设备驱动构件组态方式，与实际通讯口及设备对应。包括：“1 父:1 子”和“1 父:N 子”两种方式，对应实际通讯组网方式的“1 主:1 从”和“1 主:N 从”。现分别说明如下：

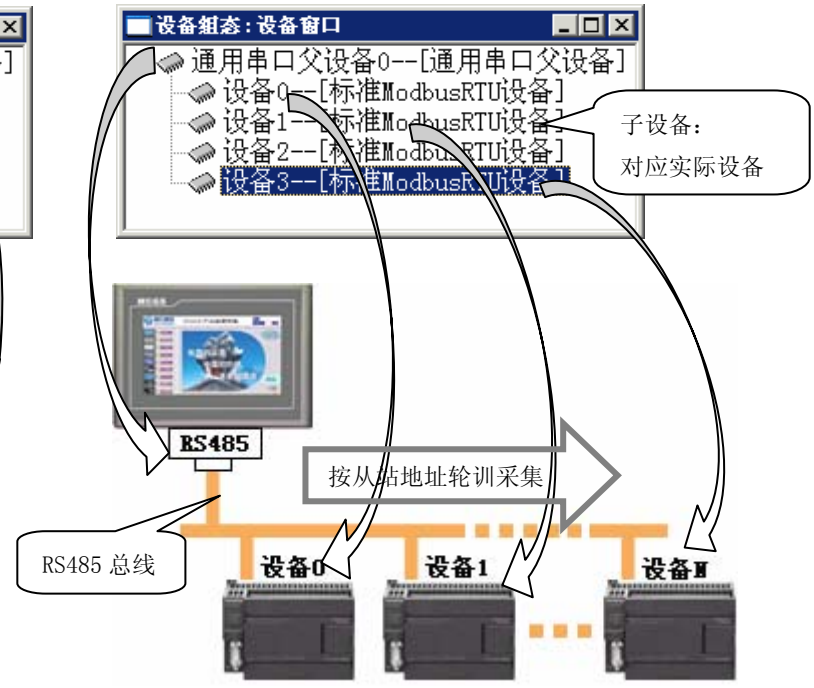
“通用串口父设备”对应触摸屏或上位模拟环境实际的物理通讯串口，挂接的子设备则对应实际与之通讯的设备。串口有 RS232、RS422 和 RS485 两种通讯方式，串口父设备与子设备的组态及通讯连接方式分别如下图所示：

1 父:1 子方式



RS232C(1 主:1 从通讯方式)

1 父:N 子方式



RS485(1 主:N 从通讯方式)

其中： RS232 方式只能使用 1 对 1 通讯方式，即：1 个 RS232 串口接 1 个 RS232 设备。而 RS485（或 RS422）方式则可支持 1 主对多从的通讯方式，但各子设备的串口通讯参数必须与父设备串口通讯参数设置相同，且各子设备要以不同地址区分。当 1 主 N 从方式进行数据采集时，一般按子设备(从站)地址轮训进行采集，此时，如果挂接子设备过多，会影响采集的速度和效率，在实际使用时要注意。

当使用“Modbus 串口数据转发设备”子设备作为从站使用时，从站要始终占用父设备对应通讯口，以随时接收主站的命令帧并进行响应。所以只可使用 1 父：1 子（数据转发设备）的组态方式，否则从站会因挂接的其他子设备干扰而导致无法正常接收主站命令帧。

“通用 TCP/IP 父设备”对应实际计算机或 TPC 触摸屏的网络 IP 地址和端口，挂接的子设备则对应实际与之通讯的设备。MCGS 目前只支持 1 对 1 的以太网通讯连接方式，即：1 父:1 子方式，使用时要注意。如果在同一台 PC 机上要实现 1 主：N 从或 M 主对 1 从的方式。可以建立多对 TCP/IP 父设备与子设备来实现。此时，要保证每对父子设备使用不同的 IP 端口。

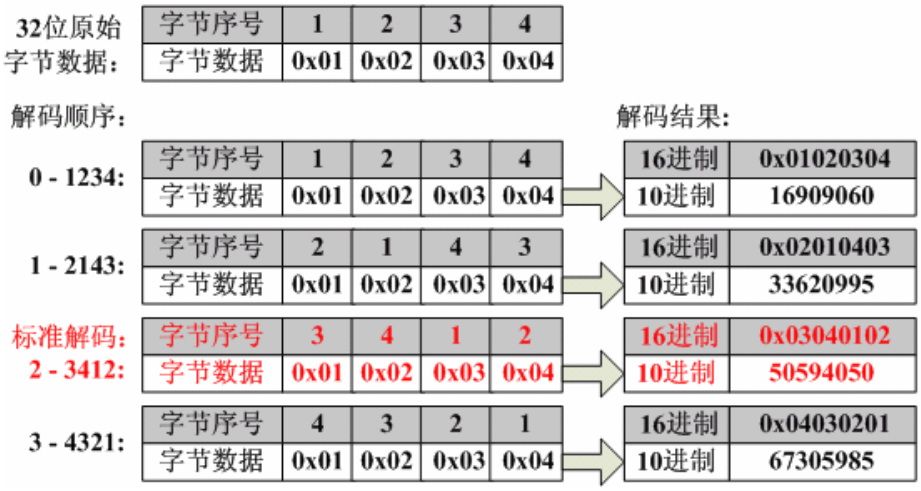
当使用“ModbusTCP 数据转发设备”子设备作为从站使用时，情况与“Modbus 串口数据转发设备”类似，只可使用 1 父：1 子（数据转发设备）的组态方式，否则也无法正常工作。

3、 非标准 Modbus 兼容处理

Modbus 协议已经成为业界通讯协议的标准，尤其是 ModbusRTU，应用十分广泛。但由于对 Modbus 协议的理解及实现上的细节差别，很多国内厂家的设备虽然支持 Modbus 协议，但在功能码支持、最大数据长度、校验及数据解码顺序等方面与标准 Modbus 协议实现均存在细节的差别。对于此类设备，我们称之为“**非标准 Modbus 设备**”，而 MCGS 的驱动构件，也充分考虑到并针对这种差别做了兼容性方面的处理，并在基本属性或内部属性中有相关设置。相关说明如下：

- **解码顺序调整：**

主要是针对非标准 ModbusRTU 和 TCP 协议设备的不同数据解码顺序导致的解析数据错误问题。由于 Modbus 协议传输 3 区和 4 区数据寄存器数据时，数据时最小单位为字，即两个字节组成的 16 位数据，字节有高低位顺序之分。由于不同厂家的开发人员对协议理解不同，会造成字节高低位解码顺序的处理方式不同，尤其是当双字（即：4 字节的 32 位）表示的整数或浮点数时，会因不同解码顺序，而解出不同的数据值。下图以 32 位无符号数据为例，说明对 4 个字节 4 种不同解码顺序的情况下，处理值结果的不同：



可见：不同的解码顺序会出现不同的数据结果，16 位数据解码与此相类似，在此不再详述。如果在测试过程中，出现解析数据值不对，可与厂家咨询后，对对应的解码顺序进行设置尝试。

MCGS 的 Modbus 驱动构件，默认 32 解码顺序为“0－1234”，主要是为了兼容以前旧有版本驱动，对于 Modicon PLC 及支持标准 ModbusRTU 的 PLC 及控制器等设备，要将“32 位整数解码顺序”和“32 位浮点数解码顺序”设置为“2－3412”的标准解码顺序。

- **校验方式调整：**

主要是针对非标准 ModbusRTU 协议设备的不同校验高低位组码顺序导致的通讯校验错误（通讯状态为 3）。对于 Modicon PLC 及支持标准 ModbusRTU 的 PLC 及控制器等设备，按默认值即可。如果出现通讯校验错误的提示(即：通讯状态为 3)，可与厂家咨询索取协议文档，与标准协议比较后，再对相关项进行设置再行尝试。

- **分块采集方式：**

主要是针对非标准 ModbusRTU 协议设备，不允许读取非连续寄存器地址的情况。对于 Modicon PLC 及支持标准 ModbusRTU 的 PLC 及控制器等设备，直接使用默认设置即可，这样可以提高采集效率。当与设备通讯时，如果按默认“0－按最大长度分块”时，出现读取连续地址正常，而不连续地址不正常时，可与厂家咨询，并设置为“1－按连续地址分块方式”尝试是否可正常通讯。

- **最大块长设置：**（只适用于通用设备中的标准 ModbusRTU 和 TCP）

最大块长，即最大有效数据长度（此定义在第二章第 4 节有相应说明），对于部分非标准 ModbusRTU 设备，其最大帧长度（或最大块长），小于标准 ModbusRTU 协议中规定的 256 字节（最大块长 120 字），从而出现添加少量通道时通讯正常，而添加多个通道时无法正常通讯的问题。此时，可以与厂家确定设备支持的最大通讯帧长度，并借助 MCGS 内部属性中提供的隐含的块长设置功能进行最大块长的设置。

隐含块长设置方法如下：

进入内部属性后，点击“增加通道”按钮，在弹出的“增加通道”窗口中，在右侧“通道数量”输入框中输入：“mcgsreadlen”，然后单击“取消”按钮，此时窗口下方会出现“最大块读字节数”的相关信息，如下图所示：

然后，选择相应寄存器类型，并根据设备支持的最大通讯帧长度，修改“最大块读字节数”即通讯帧块长的长度值，并进行寄存器通道的添加。

而对于 PLC 等标准设备，其每通讯数据帧（ADU）最大帧长度为 256 字节，而最大块长约为 120 字，对应的莫迪康 ModbusRTU 和莫迪康 ModbusTCP 主站块长则固定为 120 字而不需设置，这样可以保证最大块长情况下最优的采集效率。

- **PLC 地址与协议地址区别：**

MCGS 的 Modbus 驱动在内部属性中添加通道时，寄存器起始地址均为 1，这是遵从 Modbus 协议的，即所说的“协议地址”，而其实际寄存器地址(即所谓的“PLC 地址”)则为协议地址减 1，也就是说：以协议地址方式添加的地址为 1 时，实际寄存器地址为 0。

当应用时要注意，对于部分设备描述中，当寄存器地址表中寄存器起始地址为 0 时（PLC 地址方式），在使用 MCGS 进行内部属性通道添加或设备命令操作时，地址应转换为协议地址方式，即：寄存器地址应加 1 处理。

以上的相关设置的具体说明，也可直接参看各驱动的在线帮助。

4、 MCGS 驱动特殊处理

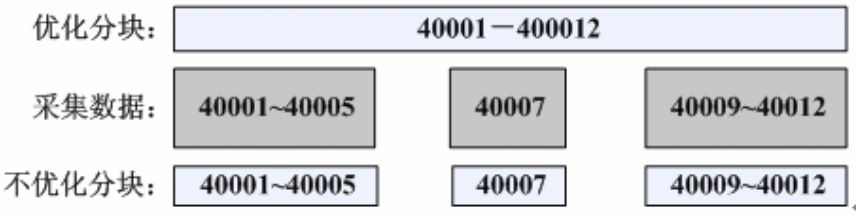
MCGS 的 Modbus 主站驱动，除遵循标准 Modbus 协议，以及对非标准 Modbus 协议设备的兼容性处理外，针对 Modbus 协议的特点，对通讯的性能和稳定性做了特殊优化处理。性能方面主要是利用了动态分块和分块采集方式时对非连续数据的特殊处理，并针对协议特点增加了批量读写设备命令功能；稳定性方面主要是增加了读写 3 次重试机制。另外，驱动还提供了 4 区扩展字符功能和通讯日志功能。

相关功能的说明如下：

- **动态分块机制：**

动态分块机制，是指数据采集时，动态的根据当前需采集通道的信息进行合理判断分块，以提高采集效率。对于 Modbus 协议，主要体现在对非连续数据的合理分块采集处理方面：当存在地址不连续但地址相近的多个分块时，采用分块优化机制时，可以将多个分块打包为一个分块，以优化采集效率。此时驱动基本属性中“分块采集方式”设置为默认的“0—按最大长度分块”。

例如：有 4 区寄存器地址分别为 1~5，7，9~12 的数据需采集，如果“分块采集方式”选择“0－按最大长度分块”，则可优化分块为地址 1~12 的 1 块数据打包 1 次完成采集；如果选择“1－按连续地址分块”，则需要分块采集 3 次。示意图如下：



分块采集方式分块示意图

一般情况下，通讯浪费时间最多的，主要是主从站的数据交互次数，通讯次数越多，则主从站判断响应时间越多，而数据帧中，地址帧、功能码帧、校验帧等与实际有效数据无关的数据收发所占用的时间也就越多。 在选择“1—按连续地址分块”时，不优化分块需要采集 3 次之多，而优化分块虽然多采集了 40006 和 40008 两个数据，但只采集了一次，从而达到了提高采集效率的目的。

另外有一点要注意：莫迪康 ModbusRTU 和莫迪康 ModbusTCP 等主站驱动，在第 1 次运行时，会固定发 1 帧读取 4 区寄存器地址为 1(即：40001)的数据帧，其目的是为了计算 PLC（或其他设备）的响应时间，以用于动态分块的分块计算判断的。此后不会再发此帧，在测试尤其是截获数据包时要注意排除掉此帧的干扰，以避免造成驱动发送数据帧错误的不正确判断。

- **批量读写设备命令：**

正常以通道写方式进行数据修改写入操作时，只能执行单个通道的写入操作。但在要写入配方等配置参数时，往往要写入多个数据，而 1 个 1 个的写入效率低下，速度也很慢。MCGS 的 Modbus 主站驱动则引入了批量读写机制，其原理是充分利用 Modbus 协议中的 15(0x0F)、16(0x10)功能码，将同寄存器中地址连续的数据连续写入，以提高批量数据写入的效率。但受协议的限制，要求读写的数据必须是同一寄存器的连续地址的数据。

MCGS 的批量读写功能是通过设备命令来实现的。同时根据客户的不同要求，提供了 ReadP/WriteP、ReadPV/WritePV、ReadBlock/WriteBlock 三类命令格式，分别满足用户不连续变量名、连续变量名、CSV 格式字符方式的读写操作，其具体命令格式及示例可参见驱动的在线帮助。

其中 CSV 格式是以逗号间隔，回车换行结尾的 CSV 格式字符串。用户可以利用此设备命令实现类似配方方式的多组数据的读写功能。

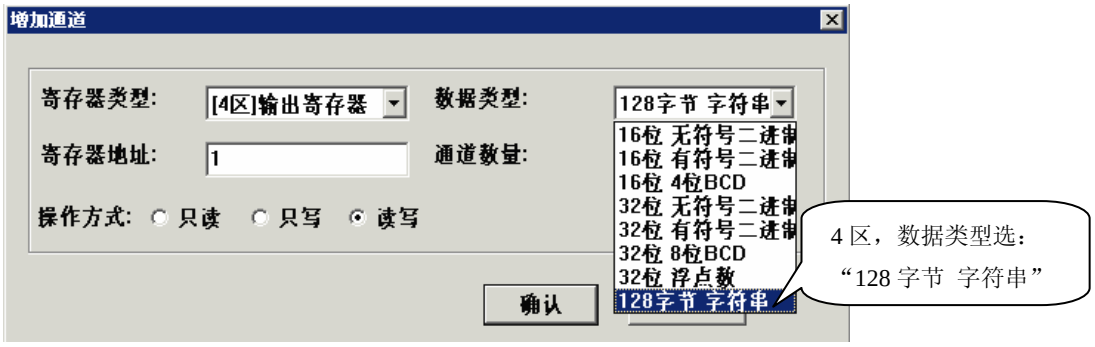
批量读写设备命令功能，不同于通道读写之处在于，命令执行受控制，可以在需要的时候进行操作。一般可以用于解决用户一次性设置多个参数，并对写入操作效率要求比较高的情况。也适用于工程采集速度优化，当用户实际采集数据量较大时，可以将部分不需要实时采集的数据，以设备命令批量读写的方式在需要的时候进行读写。例如：对于常规的参数数据设置，不需要进行实时的采集，则可以利用批量读写命令，在进入设置窗口进行参数设置时，将参数一次读入，并在修改参数后，退出设置窗口之前，一次性将参数数据写入。

- **读写重试机制：**

MCGS 的 Modbus 主站驱动遵循 Modbus 协议，具有读写重试机制，即：在读写功能码操作时，如果从站未及时响应，则重发数据帧进行尝试，如果连续 3 次从站都未及时响应或响应错误，则表明从站故障，此时不再重试，返回错误，“通讯状态”通道有相关错误值提示。

- **4 区扩展字符串功能：**

目前 MCGS 嵌入版新版本中,Modbus 转发设备已经代替网络数据同步使用，并在 Modbus 协议基础上进行扩展,增加了 4 区输出寄存器的字符数据的读写功能。可在内部属性中进行相应通道的添加。在添加通道时，如下图所示：



其功能及限制如下：

1)．提供短字符型数据类型,即 128 字节字符型数据类型,并只限于 4 寄存器区使用,可在内部属性中添加,每次添加数据长度为 128 字节(64 字)。

2)．字符型数据读写使用 4 区的 03 和 16(0x10)功能码,其他功能码无效。

3)．命令中数据区的数据格式实际为：“MCGSSTR:”+实际数据内容（128BYTE)。

4)．字符数据类型的通道，属于 MCGS 对 Modbus 协议的扩展功能,只适用于 MCGS 的 ModbusRTU 与 Modbus 串口数据转发,以及 ModbusTCP 与 ModbusTCP 数据转发构件之间的字符数据传输。

5)．对于主站驱动构件，扩展字符功能只支持通道读写方式，不支持设备命令方式读写。

由于此功能并非 Modbus 标准协议，MCGS 驱动构件中做了如下特殊判断和处理：

1).**Modbus 主站驱动构件：**

寄存器 4 区提供字符型数据类型，每个字符型数据占 64 字（128 字节）的连续地址区，且采集时每个字符型数据按 1 个分包处理。

主站发送数据帧时，与普通数据类型处理相同，均按正常协议发命令帧，只是数据长度为 64 字。而接收数据帧后，首先检查数据区前 8 个字节是否为：“MCGSSTR:”，如果不是就认为不是字

符型通道。

2).Modbus 数据转发从站驱动构件：

接收主站命令，并按标准协议进行常规解析，在回送数据时，根据添加的寄存器数据类型判断，如果是字符通道，则在填写回传实际数据区时，在实际数据前添加：“MCGSSTR:”。

3).实际通讯帧例子：

读取字符数据：主站用 03 功能码读取寄存器 4 区从地址 0(组态中地址加 1)开始的 128 字节的字符数据，从站回应字符数据内容为“你好 ABC”，其收发数据内容如下：

主站发送	01 03 00 00 00 40 44 3A
从站回应	01 03 0F 4D 43 47 53 53 54 52 3A C4 E3 BA C3 41 42 43 16 75

说明:从站回应数据帧中，从第 3 字节开始连接 8 个字节“4D 43 47 53 53 54 52 3A”，对应 ASCII 码字符内容为“MCGSSTR:”，而之后的“C4 E3 BA C3 41 42 43”，对应数据“你好 ABC”。.

写入字符数据：主站用 16(0x10)功能码向从站寄存器 4 区从地址 0(组态中地址加 1)开始的 128 字节的字符数据，写入字符内容为“你好 ABC”，其收发数据内容如下：

主站发送	01 10 00 00 00 07 0F 4D 43 47 53 53 54 52 3A C4 E3 BA C3 41 42 43 ED FA
从站回应	01 10 00 00 00 07 81 CB

说明:主站发送数据帧中，从第 3 字节开始连接 8 个字节“4D 43 47 53 53 54 52 3A”，对应 ASCII 码字符内容为“MCGSSTR:”，而之后的“C4 E3 BA C3 41 42 43”，对应数据“你好 ABC”。

说明：

1.地址添加注意事项：4 区扩展字符功能中，每个字符型数据通道固定占 64 字（128 字节）的连续地址区，在添加时，要注意地址连续关系。例如：添加了 4 区 1 地址为字符串通道，此字符串通道将占用 4 区地址 1－64 的连续地址，再添加字符串通道或其他数据通道时，只能从地址 65 开始，而 1－64 之间不能添加通道，否则会出现地址重叠。如果添加了重叠地址的通道，会导致无法正常通讯。

2.字符长度限制为 128：4 区扩展字符功能中，每个字符型数据通道固定占 64 字（128 字节）的连续地址区，使用时注意所操作的字符数据的字符长度不能超过 128 字节。

3.字符通道数量制约：4 区扩展字符功能中，采集时每个字符型数据按 1 个分包处理。所使用时，所添加的字符通道数量不宜过多，否则会增加通讯次数，影响通讯速度。

- **通讯日志功能：**

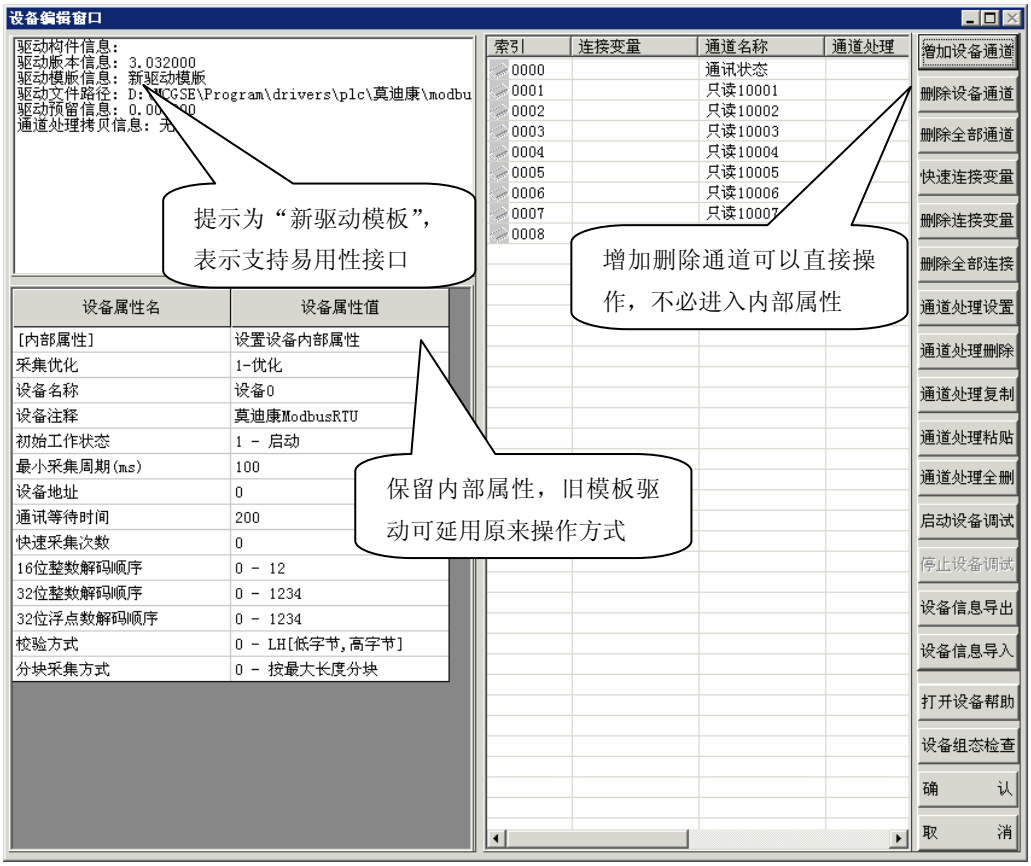
MCGS 的驱动设备命令中提供的通讯日志功能是为了方便用户现场调试，默认为不开启状态。正常时无需开启，否则影响速度。当现场有疑难无法正常通讯时，可开启通讯日志功能，记录日志信息，将通讯过程记录以供技术人员分析。其具体使用方法，请参见相关驱动的在线帮助。

说明：

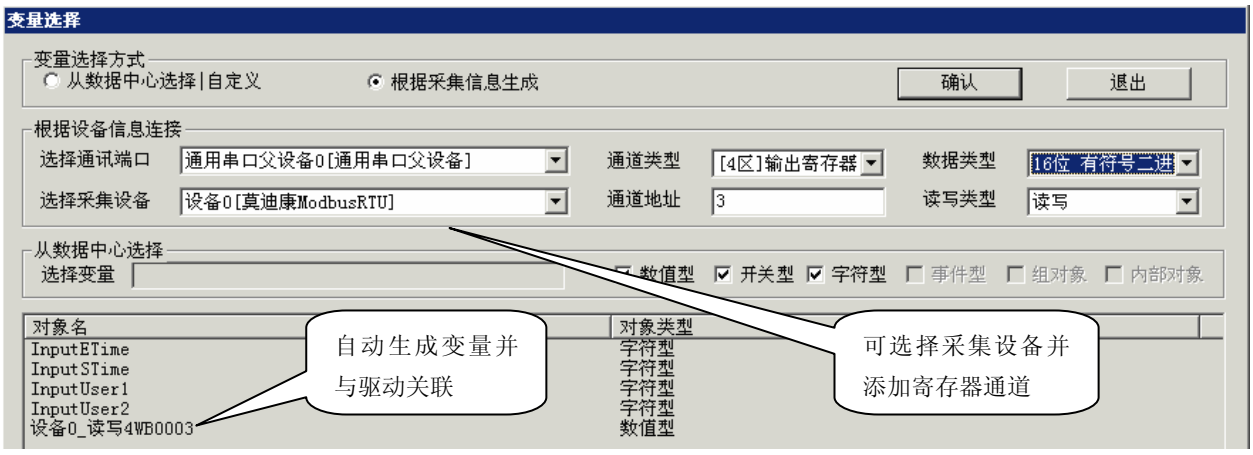
此处所说的通讯日志功能，是指驱动本身设备命令中所提供了通讯日志功能，并不同于嵌入版组态环境下载界面中的“驱动日志”的相关功能。“驱动日志”的功能主要是用于记录运行环境驱动状态及采集设备命令调用过程以供分析的。其具体的使用过程请参考嵌入版组态软件在线帮助或相关文档，在此不累述。

5、 易用性接口支持

最新推出的 MCGS 嵌入版 6.8(01.0001)及后续版本，增加了驱动易用性接口的支持，其通道添加和变量关联方式都有了功能性的改变，更便于用户组态和操作。组态相关画面如下图所示：



变量关联选择时，选择“根据采集信息生成”时，可以选择相应的设备驱动构件，直接添加对应驱动的通道并自动关联生成实时数据库变量。



目前支持易用性接口的驱动有“莫迪康 ModbusRTU”、“莫迪康 ModbusTCP”、“Modbus 串口数据转发设备”、“ModbusTCPIP 数据转发设备”，而“标准 ModbusRTU 设备”、“标准 ModbusTCP 子设备”由于要考虑到对使用以前旧版本用户改变块长等特殊功能的兼容支持，未增加易用性接口的支持。

四、Modbus 驱动构件的基本使用

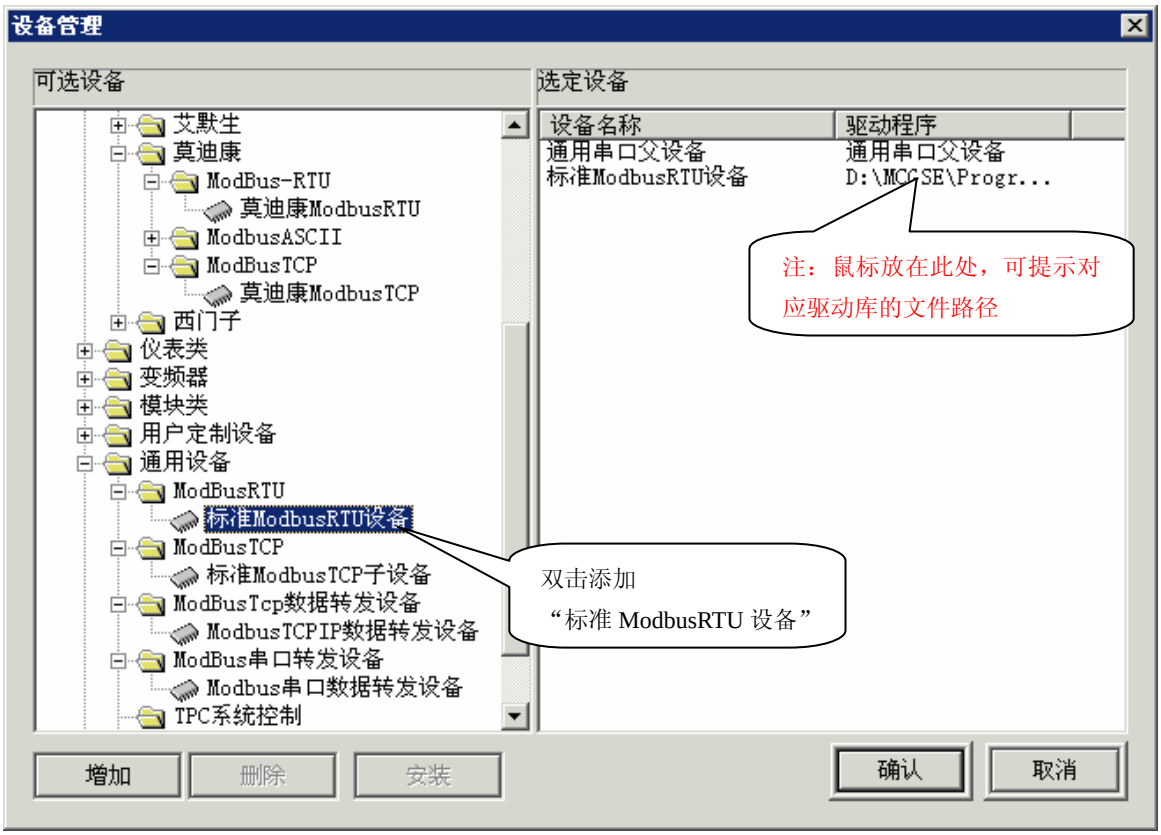
上一章中对 Modbus 相关驱动做了分类比较和介绍，本章将对驱动使用方法进行详细讲解。由于 Modbus 相关驱动的基本添加和使用方法基本相同，在此只做简单讲解，对于初学 MCGS 的用户可以先参考 MCGS 在线帮助中驱动使用的相关帮助说明。

1、驱动选择和添加

Modbus 驱动已经在第三章的驱动分类比较列表中已有相关说明，在此仅以通用设备中的“标准 ModbusRTU 设备”驱动为例，介绍如何进行选择添加和使用：

⑴、在工作台中激活“设备窗口”页面，并双击 

进入设备窗口的“设备组态”画面，然后点击工具条中的  ，打开“设备工具箱”，之后点击“设备工具箱”中的“设备管理”按钮，打开“设备管理”窗口，在左侧的“可选设备”栏中，分别找到“通用串口父设备”和“标准 ModbusRTU 设备”构件，双击增加到“选定设备”栏中，然后点击“确认”按钮，即可完成设备构件的添加。

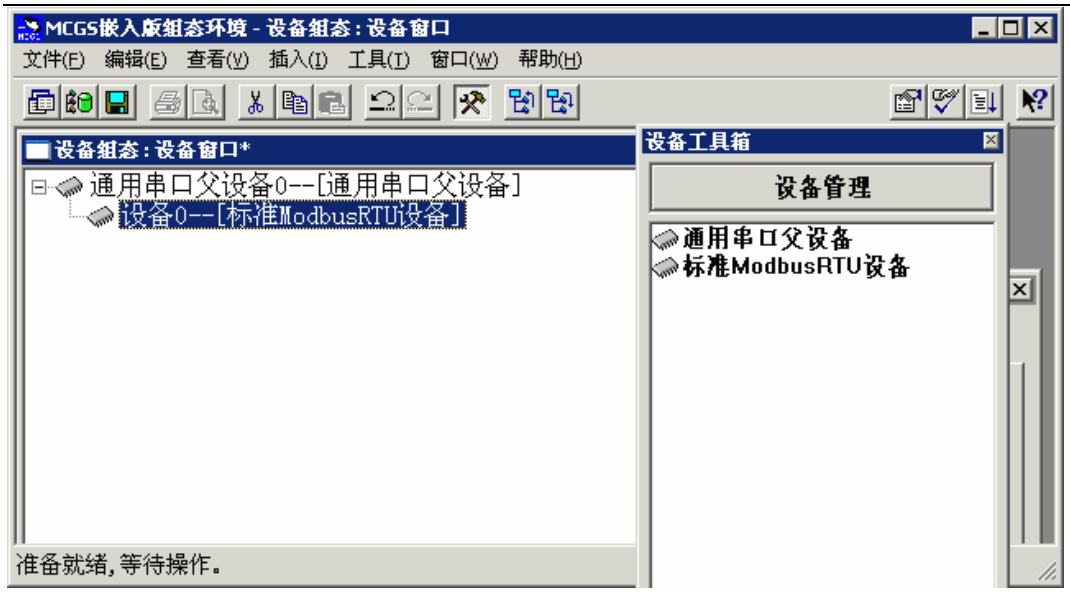


说明：1、左侧“可选设备”栏中的驱动目录树与 MCGS 嵌入版本驱动安装目录结构相对应，默认为“D:\MCGSE\Program\Drivers”，用户可根据不同需要添加相应的 PLC、变频器或用户定制设备的驱动构件。用户可双击目录或点击左侧的“+”号打开子目录，找到设备驱动构件后，双击完成添加。

2、对于右侧“选定设备”栏中已选的设备驱动构件，如果想知道其具体驱动库的文件路径，可以将鼠标放在驱动对应的“驱动程序”一列，组态即会提示出对应驱动的文件路径。如标准 ModbusRTU 设备的驱动，提示为：

D:\MCGSE\Program\Drivers\通用设备\ModBusRTU\ModbusRTUEX.dll

⑵、依次添加父设备和子设备：完成驱动构件的选定后，“设备工具箱”中则会出现已经添加的设备驱动构件，此时可以依次双击“通用串口父设备”和“标准 ModbusRTU 设备”，将其添加到“设备组态：设备窗口”中供工程实际使用。



2、驱动设置和使用

完成驱动构件添加后，需要根据实际情况进行父设备和子设备参数的设置。现分别说明如下：

⑴、设置父设备参数：双击“设备组态：设备窗口”中添加好的“通用串口父设备 0”，根据实际所连接设备所约定的串口通讯波特率、数据位、奇偶校验位等参数，对父设备进行设置。

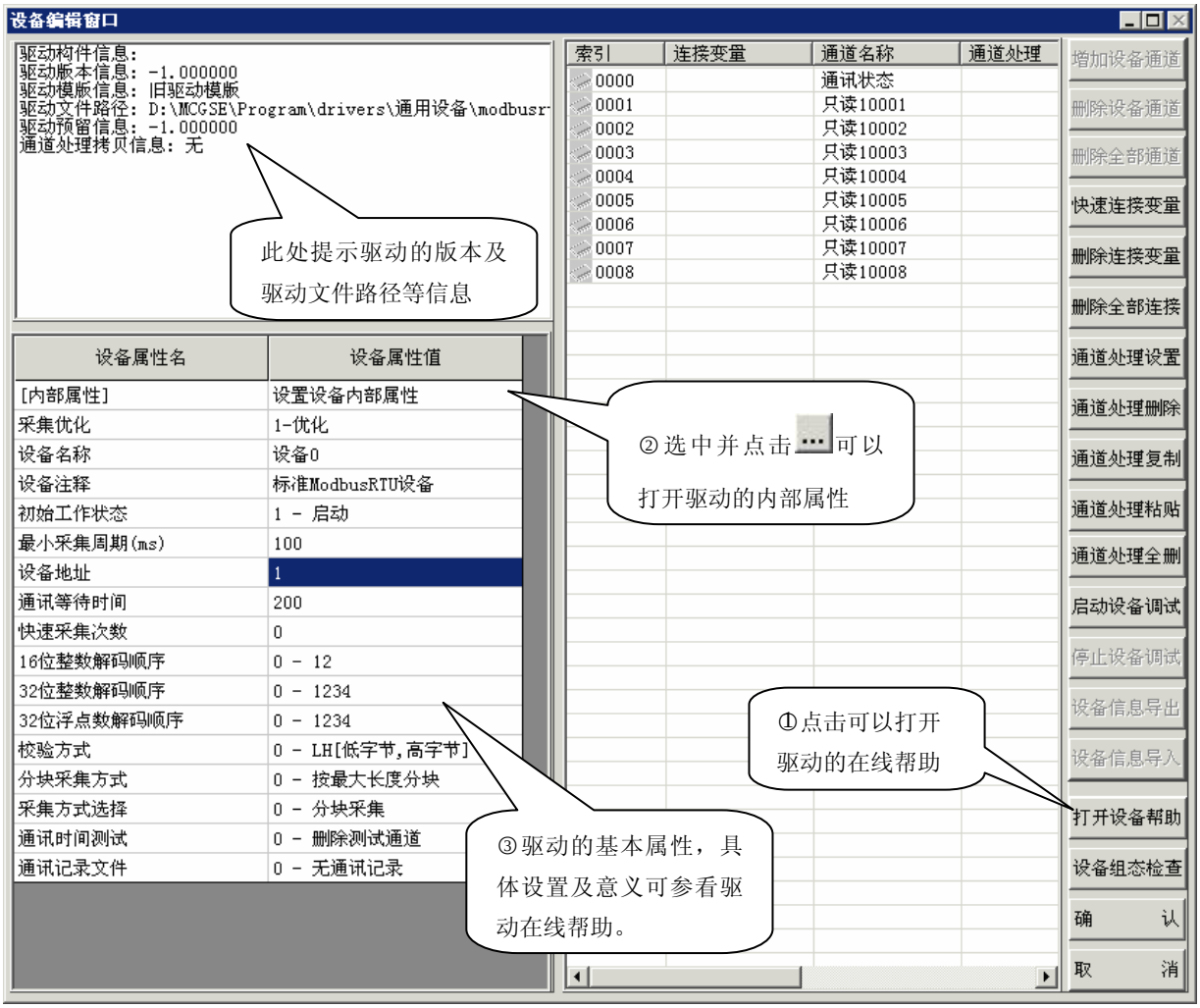
在“通用串口父设备”的基本属性页中，设置了串口通讯参数，包括串口端口号、通讯波特率、数据位位数、停止位位数、数据校验方式等，具体设置参数项如下：

设置项	参数项	默认值
串口端口号	1~254	COM2 串口
通讯波特率	9600, 19200, 38400 等	9600 波特率
数据位位数	7、8	8 位
停止位位数	1、1.5、2	1 位
奇偶校验位	无校验、奇校验、偶校验、 标志位、空格位	无校验

以上参数设置中，“串口端口号”要对应实际所使用的串口，其他通讯参数要按照与所通讯实际设备的通讯参数要求来设置，如设置不正确，无法正常通讯。

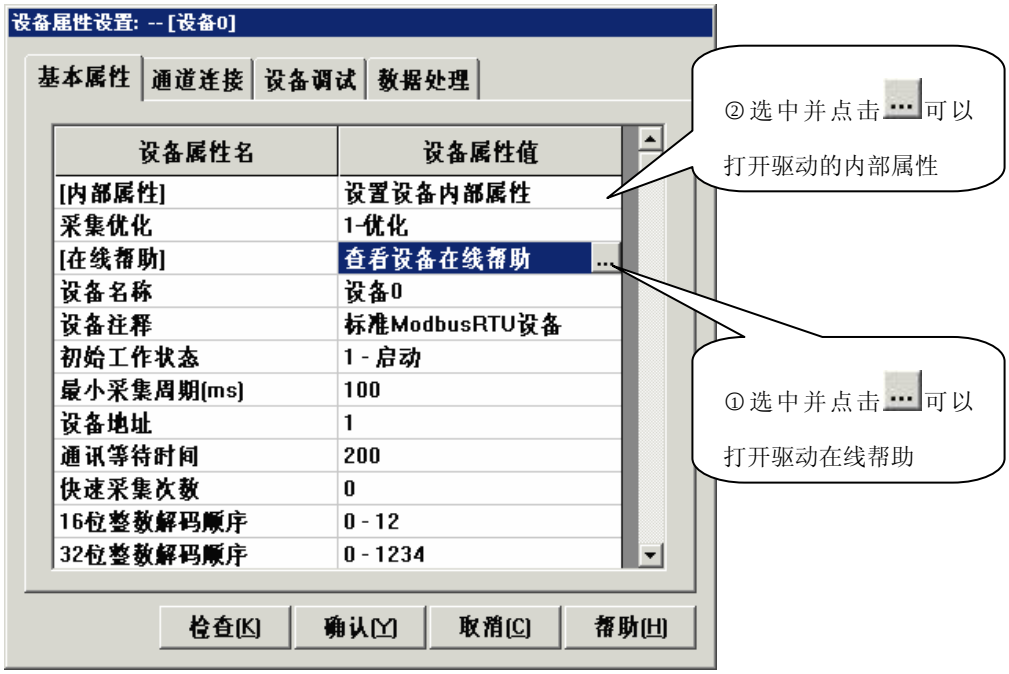
说明：“串口端口号”设置应与实际通讯所用端口对应。在使用 TPC 触摸屏通讯时，所设置的“串口端口号”要对应触摸屏的串口；而在使用上位机模拟运行环境或设备调试时，则所设置的“串口端口号”要与上位机实际串口对应。例如：当使用 TPC 触摸屏的 COM3 口与 ModbusRTU 设备通讯时，上位机模拟运行环境调试时，设置的“串口端口号”要设置为上位计算机的 COM1 串口，而实际下载时，则要改为触摸屏实际使用的 COM3 口，下载之后才能正常通讯。

⑵、子设备参数设置：双击“设备组态：设备窗口”中添加好的“设备 0－标准 ModbusRTU 设备”，进入“设备编辑窗口”，可根据实际所连接设备设置“设备地址”、“通讯等待时间”等参数。对于解码顺序、校验方式等基本属性的设置，请点击右下侧“打开设备帮助”按钮，打开设备的在线帮助，并参照帮助说明进行设置。



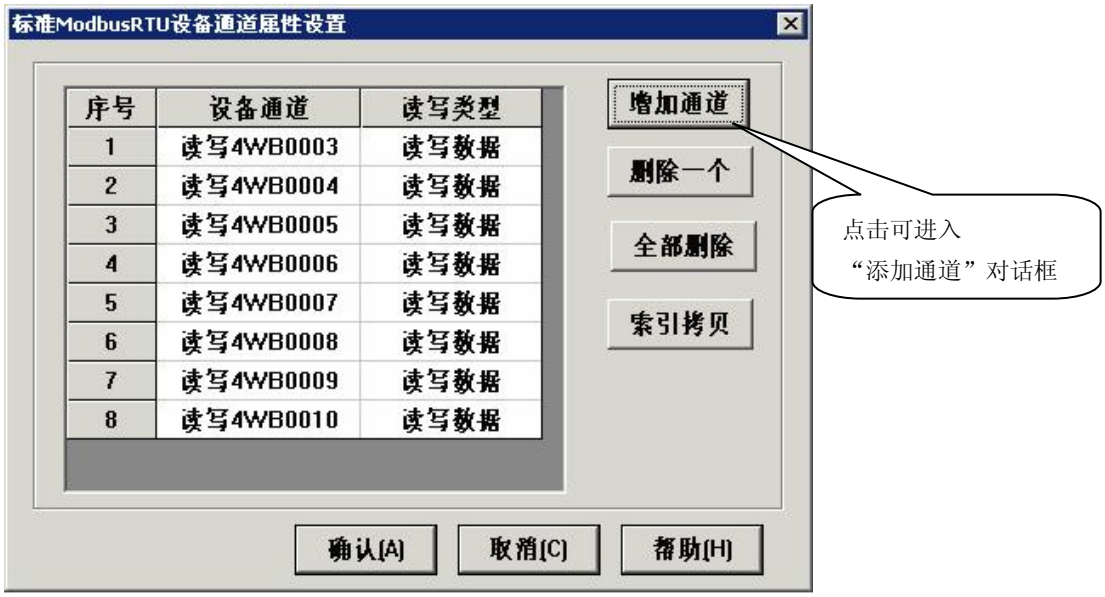
说明：标准 ModbusRTU 设备出于对旧有用户工程的兼容，沿用原有旧驱动模板，不支持易用性接口。所以左上栏驱动模板提示为旧驱动模板，版本信息为-1。 而对于莫迪康 ModbusRTU,莫迪康 ModbusTCP 等支持易用性接口的新模板驱动，左上栏驱动模板会提示为新模板，并有明确的驱动版本信息。此时可以使用左上角易用性接口提供的添加、删除设备通道等功能，而不必打开内部属性后再进行驱动通道的添加。易用性接口的说明，具体请参见第三章第 5 小节内容。

如果所用版本为 6.8 以前的旧版本，则设备属性窗口如下图：

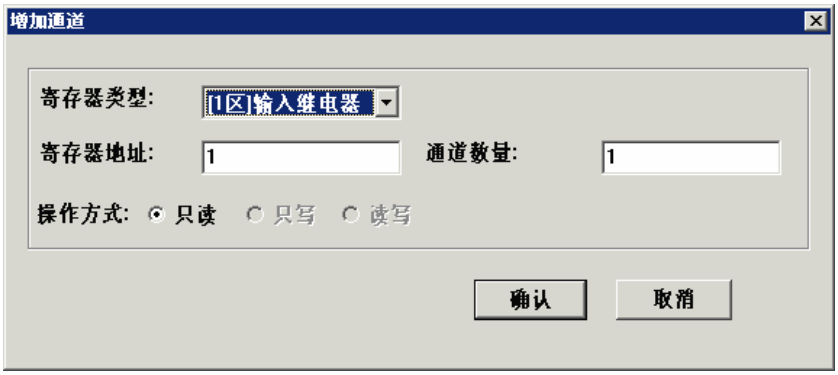


其基本属性设置与 6.8 基本相同，但驱动在线帮助开发方式有所不同。

⑶、内部属性通道添加：6.8 版本一般不需要进入内部属性，即可进行通道添加。对 6.8 以前的版本，则要按上图提示，选中设备属性值一列的“设置设备内部属性”，并点击... 打开设备驱动的内部属性页“标准 ModbusRTU 设备通道属性设置”对话框。



驱动默认添加了 10001－10008 共 8 个只读通道，此时，可利用右侧按钮进行通道的添加和删除操作。当点击“增加通道”按钮，同弹出“增加通道”对话框：



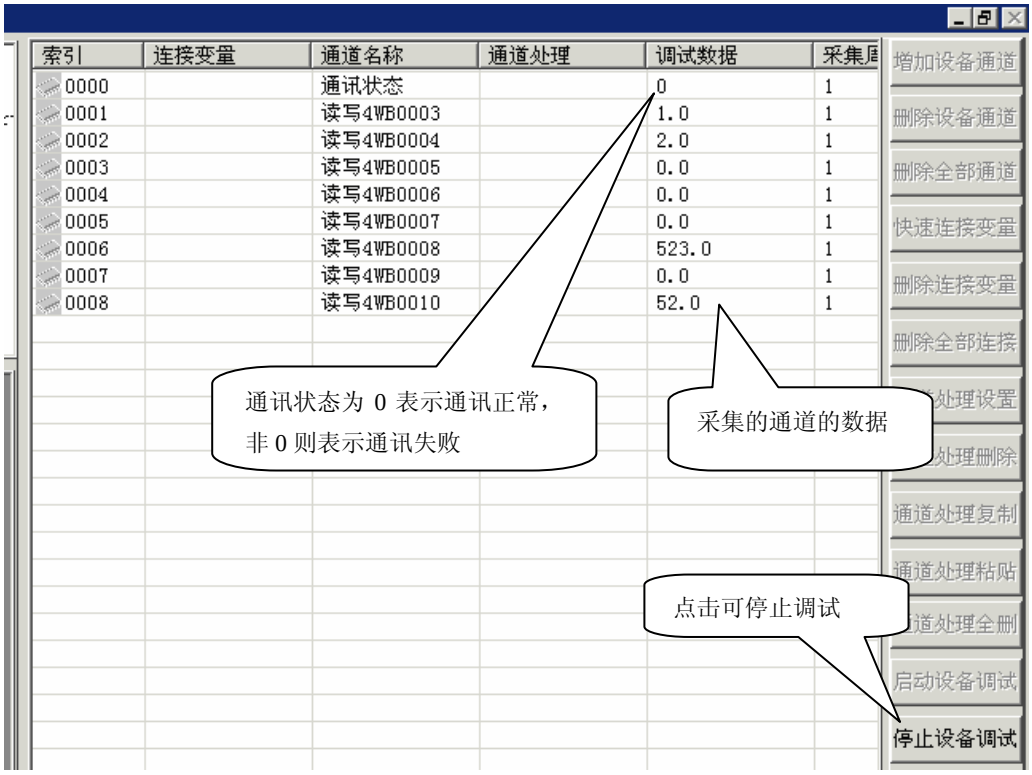
此时可根据需要进行相应寄存器地址通道的添加。例如：要添加 4 区保持寄存器的 40003－40010 共连续 8 个 16 进制有符号(INT 型)，要求可读可写，则寄存器类型选择“[4 区]输出寄存器”，数据类型选择“16 位有符号二进制”，寄存器地址为 3,通道数量为 8,操作方式选择“读写”，然后点击“确认”按钮，即完成通道的添加，添加及添加完成后的内部属性通道如下图示：

说明：1、MCGS 的 Modbus 驱动在内部属性中添加通道时，寄存器起始地址均为 1，这是遵从 Modbus 协议的，即所谓的“协议地址”，而其实际寄存器地址(即所谓的“PLC 地址”)则为协议地址减 1,也就是说：以协议地址方式添加的地址为 1 时，实际寄存器地址为 0。 而对于部分设备描述中，当寄存器地址表中寄存器起始地址为 0 时（PLC 地址方式），在使用 MCGS 进行内部属性通道添加或设备命令操作时，地址应转换为协议地址方式，即寄存器地址应加 1 处理。

2. 对于莫迪康 ModbusRTU 和莫迪康 ModbusTCP 以及相关转发等支持易用性接口功能的驱动，其通道添加可以通过易用性接口实现，具体见第三章第 5 小节易用性接口说明。

3、驱动设备调试

在完成参数设置及寄存器通道的添加后，可以通过设备调试来验证与设备是否通讯正常。具体操作为，双击“设备 0－标准 ModbusRTU 设备”，进入“设备编辑窗口”，点击右下侧“启动设备调试”按钮，进入设备调试状态，此时可查看窗口右侧的调试数据栏“通讯状态”通道的状态，如果“通讯状态”为 0，则表示通讯正常，非 0 则表示通讯不正常，通讯状态值表示的意义及处理方法可参见驱动在线帮助。



说明：1、在设备调试时，是使用上位计算机的物理串口进行通讯，所以要保证设备与上位计算机串口连接，组态中通用串口父设备的“串口端口号”要设置为上位计算机与设备连接对应的实际串口号。

2、设备调试时，一定要在添加了实际寄存器通道后进行，如果不添加任何通道，即：通道列表中只有通讯状态 1 个通道。此时由于没有添加实际寄存器通道，驱动构件并没有进行实际的采集操作，而通讯状态也会为 0，但并不代表通讯正常。

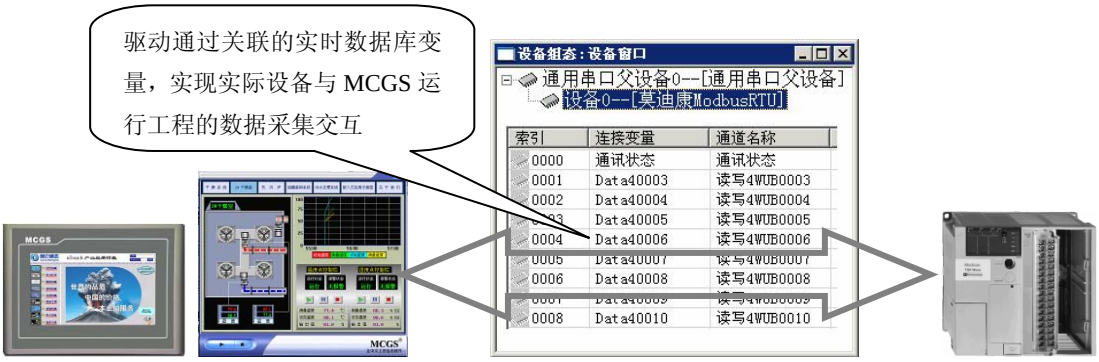
3、对于部分非标准 Modbus 设备，会出现添加少量通道通讯正常，但添加多个通道通讯失败的现象。此时，建议先添加 1 个通道进行设备调试，确认通讯正常后，再逐步添加通道进行测试，并进一步分析原因所在。

4、设备命令和通道写功能操作，无法在设备调试中执行，只能在模拟运行环境或 TPC 实际运行工程中操作。

5、对于使用 6.8 以前版本的用户，除界面有所不同外，其过程与上基本相同，在此不做描述。

4、模拟运行测试

在驱动测试后，可以使用 MCGS 提供的“模拟运行”功能，利用模拟运行环境对整个工程进行较为系统的测试，此时注意，驱动构件连接变量中，必须要关联实时数据库的变量，驱动在实际工程运行才能通过连接的实时数据库变量，实现与 MCGS 运行主程序的数据采集读写交互。否则无法正常进行数据采集交互。



TPC 或上位模拟运行环境(主站)　　驱动构件　　实际设备(从站)

另外，设备命令及通道写功能的测试，无法在设备调试中测试，可以在模拟运行环境中测试。设备命令的格式及相关操作，请参见相关驱动的在线帮助中设备命令的说明及示例。

5、设备调试与模拟运行、实际运行区别

使用“设备编辑窗口”中设备调试功能和利用模拟运行环境都可以进行驱动通讯的调试，但两者还是有区别的，现将其与实际 TPC 触摸屏运行环境的区别列举如下：

	设备调试	模拟运行	TPC 实际运行
运行系统环境	上位计算机(Windows 98、2000、XP)		TPC 触摸屏(Windows CE)
运行软件环境	MCGS 嵌入版组态环境	MCGS 嵌入版模拟运行环境	TPC 运行环境
工程运行效果	无，只在组态环境下使用	实际工程运行效果	实际工程运行效果
物理通讯端口	上位计算机物理通讯端口(串口或以太网)		TPC 触摸屏物理通讯端口
变量关联必要性	可不关联变量	必须关联变量	
初始工作状态	无效，固定为启动状态	与设置状态相同(可通过!SetDevice 在运行时修改)	
最小采集周期	固定为 1000ms	以用户设定值为准	
采集机制	采集添加的所有只读或读写通道的值	采集优化模式下，只采集当前界面关联变量对应的只读或读写通道的值； 不优化模式下，采集所有只读或读写通道的值。	
写入机制	不支持写入功能	工程运行时，通过设备命令或只写、读写通道数变发机制执行写操作。	
显示数据区别	固定只显示 1 位小数	最多可以显示 5 位小数(与数据值及显示设置有关)	

由上可见，设备调试与模拟运行、实际运行区别较大，尤其是采集机制部分。而设备调试功能设计的目的也主要是为了更方便用户进行驱动构件的调试。设备调试正常，即意味着与之通讯设备的硬件链路以及通讯参数设置正常，而驱动也可以正常工作。

而模拟运行则与 TPC 触摸屏实际运行很相近，主要区别是运行的系统和软件环境的区别，以及物理通讯端口的区别。模拟运行环境主要目的是为了方便用户进行实际工程的调试测试。一般情况下，在模拟运行环境下测试正常的工程，只要物理通讯端口(串口或以太网)正确设置为对应 TPC 的通讯端口，通讯链路及接线也正确，工程下载后基本上就不会有问题。

6、Modbus 驱动使用注意事项

以上介绍了“标准 ModbusRTU 设备”驱动构件的使用，对其他驱动，驱动添加、内部属性通道添加，以及调试方法基本相同，在此不一一说明。各个驱动的区别可参考第三章第 1 节 Modbus 驱动分类中的对比描述。下面将各驱动的设置和使用注意事项说明如下：

- **标准 ModbusRTU 设备与莫迪康 ModbusRTU：**

两者基本兼容，但有一定针对性，“标准 ModbusRTU 设备”基于原有开发模板，可支持最大块长的设置修改；而“莫迪康 ModbusRTU”则专门针对 PLC 优化，支持动态分块和批量读写设备命令，但不支持最大块长的修改。与 Modicon PLC 或标准 Modbus 设备通讯时，建议使用后者。

- **标准 ModbusTCP 子设备与莫迪康 ModbusTCP：**

ModbusTCP 协议，两驱动基本兼容，区别同前。设置时，请按帮助说明，注意 IP 地址和端口设置，“服务器/客户设置”设置为“0-客户”即可。用户实际使用时，部分设备在设备调试情况下可能无法正常通讯，此时，可以先 Ping 通 IP，确认硬件链路无问题后，在模拟环境下进行测试。 另外 MCGS 组态 TCP/IP 通讯目前只支持 1 父：1 子方式，1 个父设备不能挂多个子设备。

- **Modbus 串口数据转发设备与 ModbusTCPIP 数据转发设备：**

数据转发设备在与主站配合使用时要注意以下几点：

组态方式：作为从站，只能以 1 父：1 子方式实现，同时相应的父设备下不能再挂接任何其他子设备，否则会干扰从站正常的监视和响应。如果想要实现多个从站连接方式，可以使用多对 1 父：1 子设备构件的方式实现，此时要保证每对设备构件占用不同的物理端口。

基本属性对应：作为 Modbus 从站，与 Modbus 主站通讯数据交互时，相对于主站，可被视为设备。此时，主站和从站设备地址、通讯参数等设置也要保持一致：串口数据转发要保证串口波特率、数据位、校验位等通讯参数相同；TCPIP 数据转发则要保证主站的远程 IP 地址、端口号和从站的本地 IP 地址、端口号相同，否则无法正常通讯。

通道寄存器地址对应：主站要采集的相关寄存器地址，从站中必须保证包含这些地址，例如，主站想采集 4 区的地址 1 和地址 2，那么数据转发设备中应该至少有这两个通道地址，否则无法正常通讯。

通道数据类型对应：添加通道时，主从站寄存器通道的数据类型要相同。数据转发设备(从站)添加通道的只读、只写、读写属性是相对于主站而言的，即：被主站进行只读、只写和读写操作。

4 区扩展字符串功能：目前 MCGS 嵌入版在 Modbus 协议基础上进行扩展增加了 4 区输出寄存器的字符数据的读写功能。此扩展功能可以代替旧有的网络数据同步功能使用，但每个字符型数据固定占 64 字（128 字节）的连续地址区，且采集时每个字符型数据按 1 个分包处理。所使用时有几点要注意：一是操作的字符数据长度不能超过 128 字节，且所占连续地址为 64 字，不能地址重叠添加通道；二是由于每字符型通道会按 1 个分包处理，所添加的字符通道数量不宜过多，否则会增加通讯次数，影响通讯速度。4 区扩展的字符功能具体可参考第三章第 4 节中相关描述。

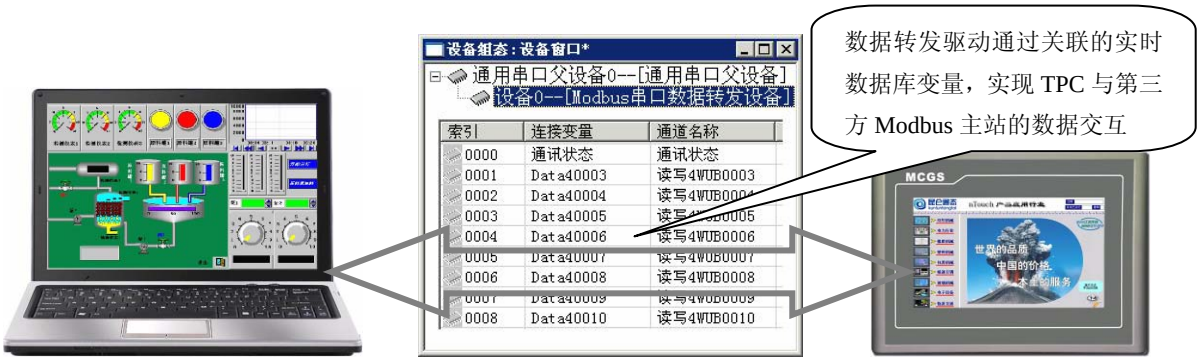
另外，串口转发设备作为从站，其通讯状态已经不起作用，不代表通讯状态，此点与主站有所不同。

五、数据转发设备(从站)与主站的配合使用

本章将重点对“Modbus 串口数据转发设备”、“ModbusTCPIP 数据转发设备”数据转发从站驱动与 Modbus 主站的配合使用进行讲解。驱动的使用与“标准 ModbusRTU 设备”驱动构件的添加设置使用基本相同，具体请参考第四章内容及驱动在线帮助，使用的注意事项请参考第四章第 6 节。

1、与第三方 Modbus 主站数据交互

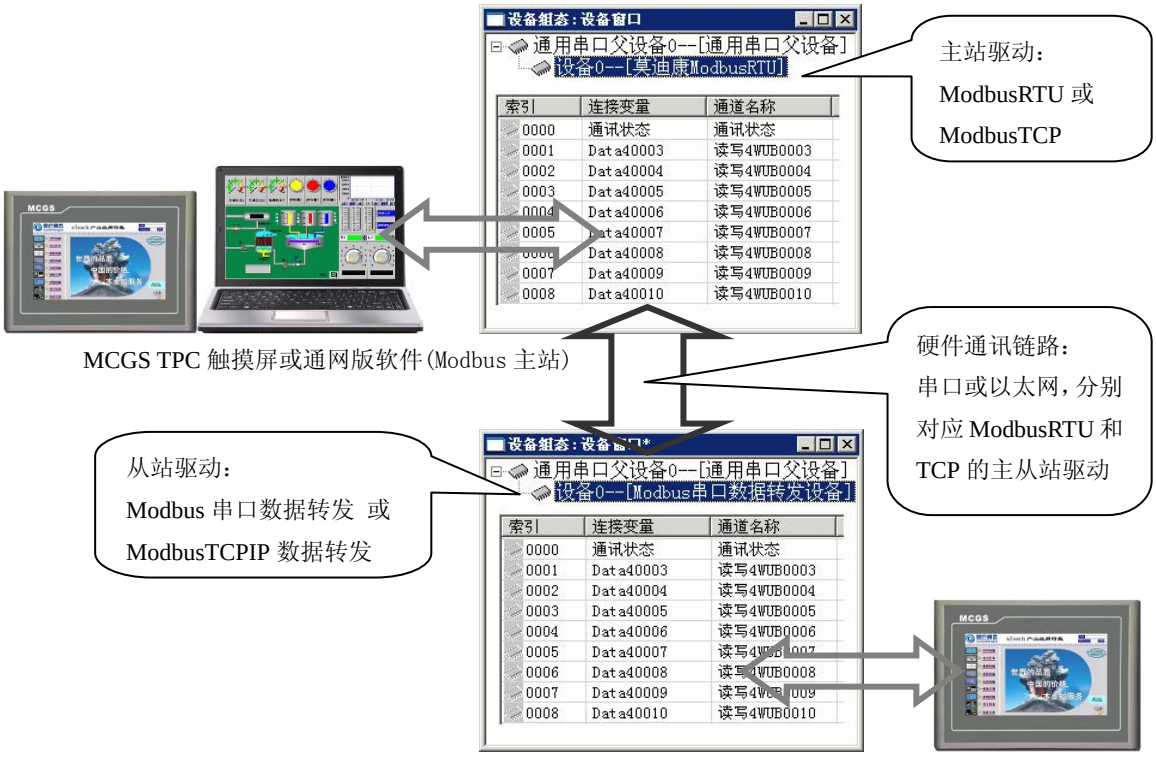
数据转发设备(从站)驱动，可用于将 MCGS 的 TPC 触摸屏作为 Modbus 从站，与其他第三方软件或 HMI 等 Modbus 主站通讯并提供数据交互，此时 TPC 相当于从站终端设备，驱动通过关联的实时数据库变量，实现 TPC 触摸屏与第三方 Modbus 主站的数据交互：



第三方 Modbus 主站　　数据转发驱动构件　　TPC 触摸屏(Modbus 从站)

2、与 MCGS 通网版软件或 TPC 触摸屏数据交互

数据转发设备(从站)驱动，也可用于将 MCGS 的 TPC 触摸屏作为 Modbus 从站，与 MCGS 的 TPC 触摸屏或通网版软件的 Modbus 主站通讯实现数据交互。



MCGS TPC 触摸屏或通网版软件(Modbus 主站)

MCGS TPC 触摸屏(Modbus 从站数据转发)

六、 Modbus 驱动常见问题处理

本章主要针对 Modbus 主从驱动常见问题的判断和处理进行分析讲解。

1、Modbus 主站驱动问题

Modbus 主站驱动在调试和测试过程中出现通讯不正常(通讯状态非 0)的现象时，此时则需要对通讯状态的不同情况进行判断处理。

故障现象	原因分析	判断步骤及处理建议
通讯状态 为 1 或 2	属于通讯硬件连接、 或参数设置问题	1、检查串口父设备参数设置是否正确
		2、检查串口是否被其他程序占用(设备调试、模拟运行)
		3、检查通讯电缆是否正确连接(超长电缆也可能有此问题)
		4、检测设备设置，并使用厂家测试程序或第三方 Modbus 主站确保通讯正常。并确认设备设置项与帮助中要求相同
		5、检查“设备地址”与 PLC 设置是否一致
		6、适当延长“通讯等待时间”
		7、读取数据地址超范围
通讯状态为 3	采集数据校验错误 (包括应答数据不完整或校验错误两种情况)	1、检查父设备串口校验位设置是否正确
		2、适当延长“通讯等待时间”
		3、更改驱动基本属性“校验方式”，排除校验高低位颠倒问题
		4、通讯电缆太长，换成短距离电缆测试
		5、现场干扰太大，排除周围环境干扰后再测试
		6、RS485 通讯方式，信号变弱，使用有源 RS232/485 模块
通讯状态在 0 与非 0 之间跳变	通讯不稳定	1、适当延长“通讯等待时间”
		2、通讯电缆太长，换成短距离电缆测试
		3、现场干扰太大，排除周围环境干扰后再测试
		4、RS485 通讯方式，信号变弱，使用有源 RS232/485 模块
添加某通道后，通讯状态变非 0	读取地址超范围	1、尝试将分块采集方式改为“按连续地址分块”
		2、使用通用设备目录下的主站设备，并尝试改小最大分块长度。
通讯状态为 0，数据不正确	解码顺序错误 或实际数据大于 999999	1、尝试修改驱动基本属性的解码顺序 (如果实际数据大于 999999，显示有精度丢失或科学计数法显示)
设备调试正常，模拟或实际运行时通讯状态非 0	实际运行与设备调试分块机制不同的原因	1、尝试将分块采集方式改为“按连续地址分块”
		2、请确认父设备通讯端口参数设置是否正确 (注意 TPC 触摸屏实际运行环境与模拟环境的区别)
设备调试正常，模拟或实际运行时，通讯状态为 0,但数据不正确	组态工程问题	1、检测通道是否连接变量
		2、关联变量的最大最小值设置是否过小
		3、检测工程是否对数据进行处理
		4、新建工程进行驱动测试，排除工程问题
通讯速度太慢	通讯数据量过大 或采集周期设置过长	1、将“采集优化”属性设置为“1-优化”
		2、减小父设备及子设备的最小采集周期(最小可设置为 20ms)
		3、使用设备命令，减少实时采集的数据
		4、通过设备命令获取 PLC 延时，判断是否 PLC 响应时间过长
	通讯次数过多	5、将采集数据放到同一寄存器连续的地址块中，提高采集效率
	设备命令或写操作频繁	6、检查工程循环策略等是否有频繁通道赋值及设备命令操作
		7、将频繁写操作转为通过批量写设备命令实现，减少操作次数

注意：

1、 如用户使用 Modbus 主站驱动，与之通讯的设备是莫迪康 PLC，有一点值得注意下，保证用户想要读取的所有通道中，最大的地址必须小于 PLC 程序中相应区的最大地址。例如：用户想读取 4 区的地址 1 到地址 200 之间的 200 个数据，那么 PLC 程序中用到的所有 4 区地址里面，最大的地址必须大于 200。目前 TWD 系列的 PLC 至少是这种情况，其它系列的 PLC 还没有确认。

2、 莫迪康 ModbusRTU 和莫迪康 ModbusTCP 等主站驱动，在第 1 次运行时，会固定发 1 帧读取 4 区寄存器地址为 1(即：40001)的数据帧，其目的是为了计算 PLC（或其他设备）的响应时间，以用于动态分块的分块计算判断的。此后不会再发此帧，在测试尤其是截获数据包时要注意排除掉此帧的干扰，以避免造成驱动发送数据帧错误的不正确判断。

2、Modbus 从站驱动问题：

Modbus 从站驱动的通讯状态没有真正的意义，其工作状态的判断都是通过主站状态来判断，具体可参考上一小节。下面主要讲解使用数据转发驱动构件作为从站与第三方 Modbus 主站通讯时常见的问题处理。

故障现象	原因分析	判断步骤及处理建议
无法与主站正常通讯	通讯硬件连接、或参数设置问题	1、检查串口父设备参数设置是否正确
		2、检查串口是否被其他程序占用(设备调试、模拟运行)
		3、检查通讯电缆是否正确连接(超长电缆也可能有此问题)
		4、检测设备设置，并使用 MCGS 测试工程或第三方 Modbus 主站确保通讯正常
		5、检查“设备地址”与主站相关设置是否一致
		6、读取数据地址超范围
数据校验错误	校验位顺序原因	1、检查父设备串口校验位设置是否正确
		2、更改驱动基本属性“校验方式”，排除校验高低位颠倒问题
通讯不稳定	硬件干扰问题	1、通讯电缆太长，换成短距离电缆测试
		2、现场干扰太大，排除周围环境干扰后再测试
		3、RS485 通讯方式，信号变弱，使用有源 RS232/485 模块
部分数据值无法读取或无法写入	读取地址超范围或读写属性不正确	1、确认主站所读取寄存器地址通道已经添加
		2、确认添加的相关通道具有操作的读写属性。
读取数据值不正确	解码顺序错误或实际数据大于 999999	1、尝试修改驱动基本属性的解码顺序(如果实际数据大于 999999，显示有精度丢失或科学计数法显示)
通讯速度太慢	通讯数据量过大	1、减少主站实时采集的数据
	从站数据刷新周期过长	2、减小从站设备的最小采集周期(建议为默认的 100ms)
	通讯次数过多	3、将采集数据放到同一寄存器连续的地址块中，提高采集效率
	写入操作频繁	4、减少主站写入操作频率

注意：

对于实际数据大于 999999 时，显示精度有丢失或以科学计数方式显示的问题，主要是受 Windows 系统中对单精度浮点数（Float）显示精度的影响而引起。主要出现问题的是 32 位整数或浮点数，目前处理的方法是：将 32 位数拆分为两个 16 位数通道，然后在组态中通过组合计算，计算后的结果最终以字符串形式显示，以避开系统显示精度的影响。其组合规则为：

$D_{32} = D_{16}H \times 65536 + D_{16}L$

其中$D_{16}H$ 为拆分的高 16 位数，$D_{16}L$ 为拆分的低 16 位数，D_{32}为组合计算的结果。

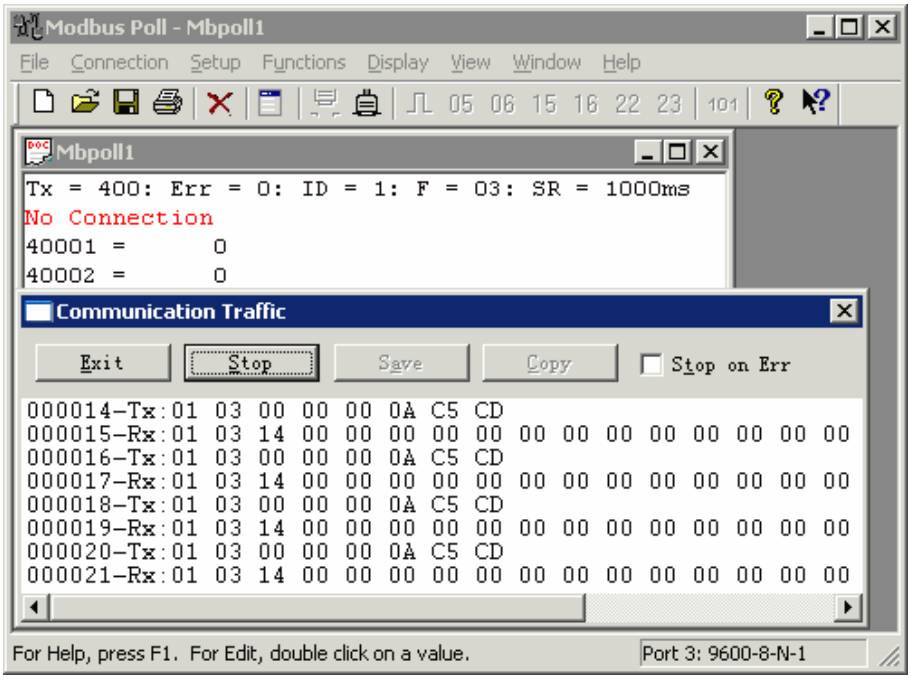
七、Modbus 协议分析技巧：

目前很多 PLC、仪表等设备都表示支持 Modbus 协议，并且通常都会提供协议的描述以及对应 Modbus 的寄存器地址对应表供用户使用。对于较为熟悉 Modbus 协议的用户，可以直接阅读厂家提供的协议描述，但大多用户通常无法直接判断出该设备是否是标准的 Modbus 协议，而提供寄存器地址对应表也不清楚如何使用。本章将讲解如何进行协议的分析以及相关技巧。

如果在阅读本章之前，您对 Modbus 协议还不熟悉，请先参看第一、二章节。

一般来说，用户可以先阅读厂家提供的协议，并与标准协议帧格式进行对比，以初步判断其协议格式是否符合标准。（标准协议格式可参考第二章相关内容），但很多厂家提供的协议很笼统，很多并没有提到协议数据单元（PDU）的具体格式，如数据地址的高低位、数据以及校验码的高低位顺序等，这样一来，导致用户无法判断是否是标准的协议，而且用户不借助工具，也无法判断校验码是否正确。但大多厂家协议都提供了通讯收发数据帧的例子，在这种情况下，最简单的办法，就是利用 Modbus 软件，实现与厂家协议描述中例子相同的读写寄存器，并截获对比其发出的数据帧，判断厂家协议例子是否与其一致，以及具体的关系。一般情况下，可以利用 MCGS 的 Modbus 主站驱动构件，按协议中例子，添加相同的通道并截获数据包判断是否是标准协议。对于 Modbus 串口设备，一般可以使用 PortMon 串口监听截获数据包。也可以使用串口调试助手等工具模拟从站直接接收主站发出的数据包。具体工具软件的使用请参考“常用通讯测试工具使用.doc”文档。

另外，也可以使用 Modbus Poll 测试软件，并利用其“Display”菜单中的“Communication…”查看收发数据帧，以辅助进行分析。Modbus Poll 如下图所示：



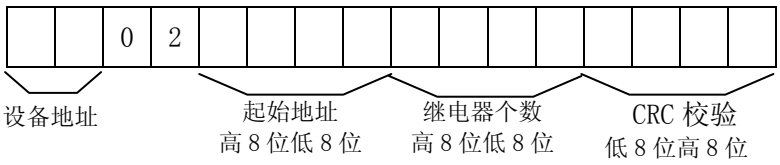
注：Modbus Poll 是一个第三方的 Modbus 主站测试软件，它可以作为一个主站和设备通讯。其具体使用请参见“常用通讯测试工具使用.doc”文档中 Modbus Poll 软件使用说明章节。

附录 1：Modbus 协议格式

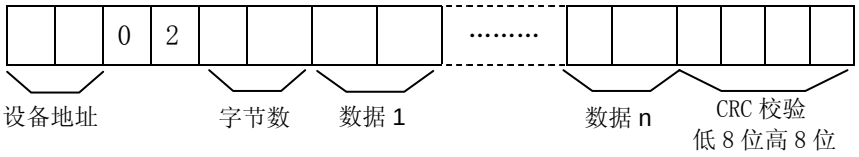
标准 Modbus 协议各寄存器读写的数据帧格式：

1. 读 1 区输入继电器(指令代码：0X02)

指令

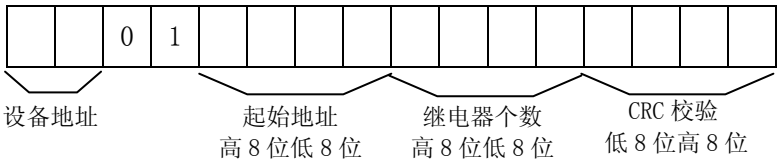


应答

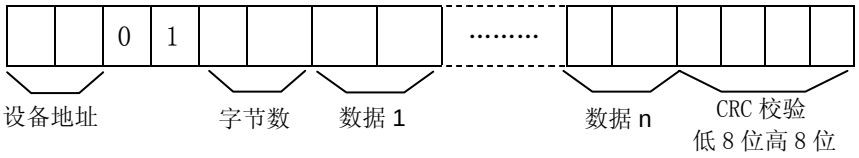


2. 读 0 区输出继电器(指令代码：0X01)

指令

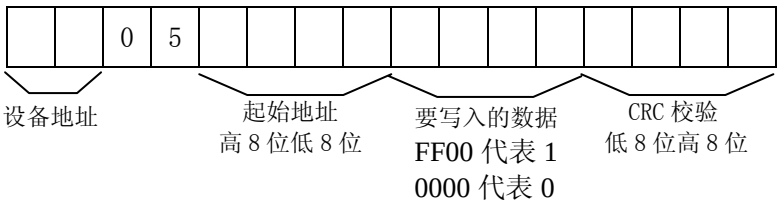


应答

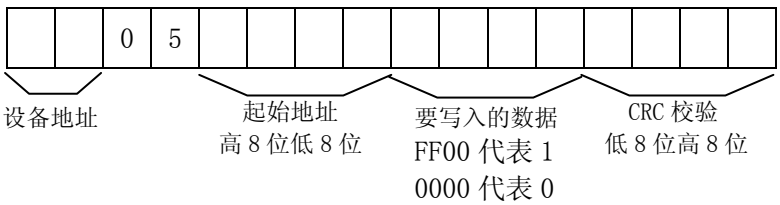


3. 单个写 0 区输出继电器(指令代码：0X05)

指令

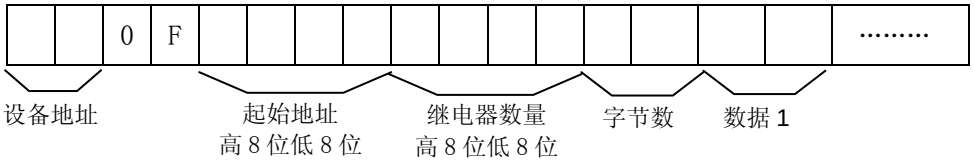


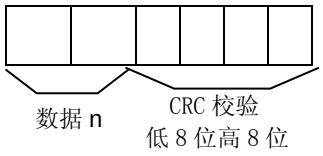
应答



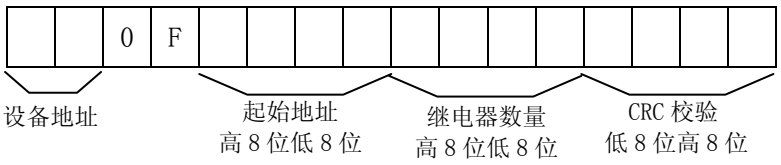
4. 多个写 0 区输出继电器(指令代码：0X0F)

指令



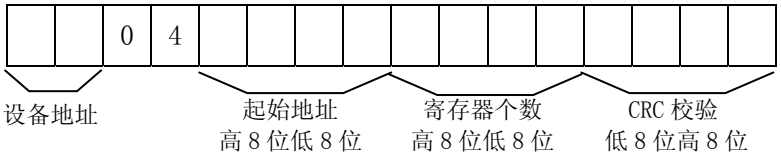


应答

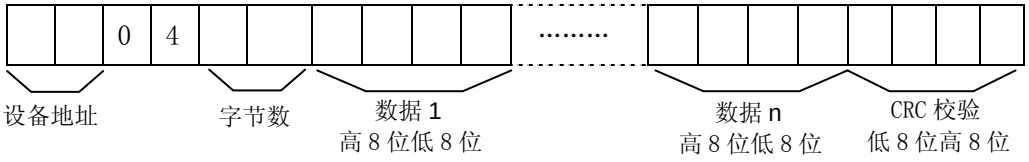


5. 读 3 区输入寄存器(指令代码：0X04)

指令

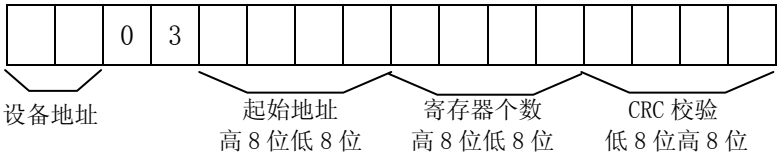


应答

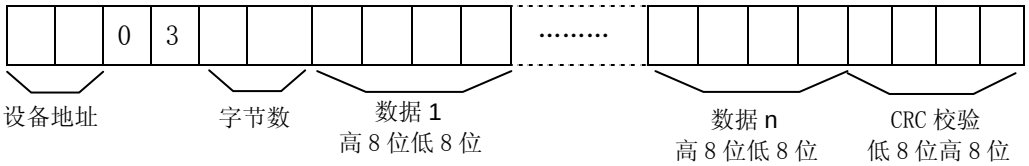


6. 读 4 区输出寄存器(指令代码：0X03)

指令

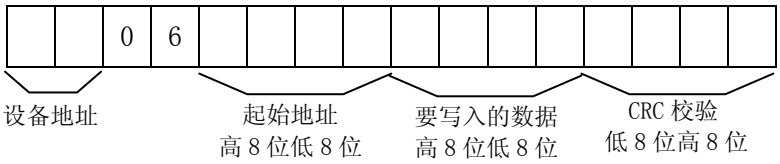


应答

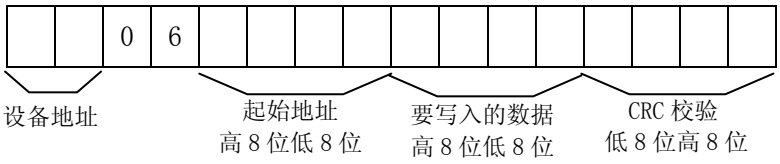


7. 单个写 4 区输出寄存器(指令代码：0X06)

指令

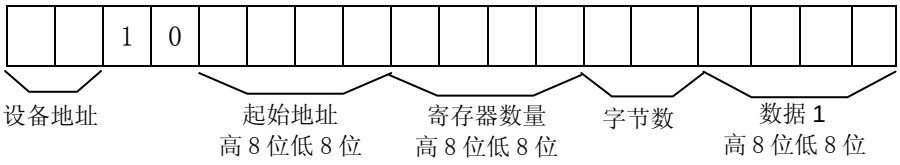


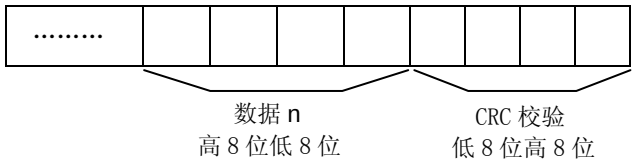
应答



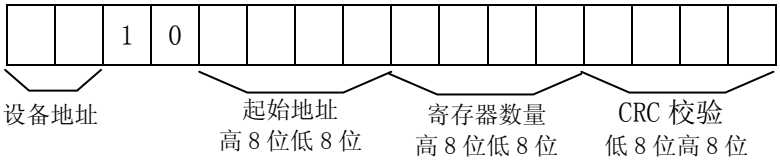
8. 多个写 4 区输出寄存器(指令代码：0X10)

指令



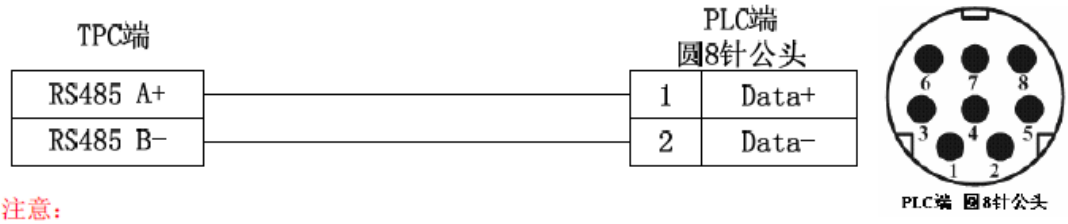


应答



附录 2：Modicon PLC 通讯接线图

Modicon TSX系列和Twido系列PLC的编程通讯口(Terminal Port)的通讯电缆图如下：



注意：

1.其他设备的通讯连接，具体请参考对应设备手册。

2.TPC 触摸屏的 RS485 接口的详细引脚定义请查阅 TPC 产品手册相关说明。