

MODBUS 串口通讯

初级入门手册

注：该手册仅针对维控产品中 Modbus 协议的解读和初级入门指导。（维控技术部宣）

目录

一、 modbus 的寄存器的代码格式	1
1、 字地址的读写	1
2、 位地址的读写	1
二、 代码格式	2
1、 字地址读：	2
2、 字地址写：（单字）	2
3、 字地址写：（多字：连写）	2
4、 位地址读：	2
5、 位地址写：（单个位）	2
6、 位地址写：（多个位：：连写）	3
三、 modbus 通讯中的使用	4
1、 Modbus 协议选择	4
2、 通讯配置	5
3、 通讯地址的格式	6
4、 地址的读写	7
5、 地址的读写长度设置	9
6、 多设备连接的配置	10

一、modbus 的寄存器的代码格式

1、字地址的读写

字地址的功能码

字寄存器类型	功能码 (十六进制)	描述	读写模式
3	04	读取设备的数据寄存器	只读
4	03	读取设备的数据寄存器	可读可写
	06	预置单寄存器，即写单个寄存器的数据	
	10	写入多个寄存器，即连写多个寄存器的数据	
W6	03	读取设备的数据寄存器	可读可写
	06	预置单寄存器，即写单个寄存器的数据	
W16	03	读取设备的数据寄存器	可读可写
	10	写入多个寄存器，即连写多个寄存器的数据	

2、位地址的读写

位地址的功能码

位寄存器 类型	功能码 (十六进制)	描述	读写模式
0	01	读取设备的线圈状态，取得一组逻辑线圈的当前状态。	可读可写
	05	强置单线圈，强置一个逻辑线圈的通断状态，即写单个寄存器。	
	0F	写多个位寄存器，即连写。	
1	02	读取设备的输入状态，取得一组开关输入的当前状态。	只读
W5	01	读取设备的线圈状态，取得一组逻辑线圈的当前状态。	可读可写
	05	强置单线圈，强置一个逻辑线圈的通断状态，即写单个寄存器。	
W15	01	读取设备的线圈状态，取得一组逻辑线圈的当前状态	可读可写
	0F	写多个位寄存器，即连写。	

注：modbus 协议还增加了字中取位的功能，可以访问像地址如 100.1 等格式的地址，发出去的功能码跟字读写的是一样的！

二、代码格式

1、字地址读：

寄存器读（3 功能码）：

主机发送：01 04 00 00 00 01 31 ca

从机返回：01 04 02 00 00 b9 30

寄存器读（4 功能码）：

主机发送：01 03 00 00 00 01 84 0a

从机返回：01 03 02 00 00 b8 44

2、字地址写：（单字）

主机发送：01 06 00 00 00 01 48 0a

从机返回：01 06 00 00 00 01 48 0a

3、字地址写：（多字：连写）

主机发送：01 10 00 00 00 02 04 00 00 00 00 f3 af

从机返回：01 10 00 00 00 02 41 c8

4、位地址读：

寄存器读（0 功能码）：

主机发送：01 01 00 00 00 01 fd ca

从机返回：01 01 01 00 51 88

寄存器读（1 功能码）：

主机发送：01 02 00 00 00 01 b9 ca

从机返回：01 02 01 00 a1 88

5、位地址写：（单个位）

主机发送：01 05 00 00 00 00 cd ca

从机返回：01 05 00 00 00 00 cd ca

6、位地址写：（多个位：连写）

主机发送：01 0f 00 00 00 0a 02 01 00 e4 a8

从机返回：01 0f 00 00 00 0a d5 cc

Modbus 协议读格式为 从机站号 功能码 起始地址 读取的长度 CRC 校验

 从机站号 功能码 数据个数 数据 CRC 校验

Modbus 协议写格式为 从机站号 功能码 起始地址 写的长度 数据个数

 数据 CRC 校验

 从机站号 功能码 起始地址 读取的长度 CRC 校验

Modbus 协议写格式为 从机站号 功能码 地址 数据 CRC 校验

（单字或者单位）

 从机站号 功能码 地址 数据 CRC 校验

三、modbus 通讯中的使用

Modbus 通讯使用注意的有以下几点。

1、Modbus 协议选择

(1) HMI 作为主站

当 HMI 作为 Modbus 主站的配置(主动发送请求信息) , 与 HMI 通讯的设备作为 modbus 从站, 这时 HMI 的通讯口协议选择 Modbus slave , 从站的站号是通过通讯口配置中的 HMI 站号进行设置。

HMI 与设备的通讯连接示意图及引脚定义可参看通讯口配置右侧的配图说明, 如下图所示:

管脚	定义	管脚	定义
1	RS422 TX+ (RS485+)	2	RS232 RXD
3	RS232 TXD	5	GND
6	RS422 TX- (RS485-)	7	
8	RS422 RX-	9	RS422 RX+ ^①

(2) HMI 作为从站

当 HMI 作为 Modbus 从站的配置, 与 HMI 通讯的设备作为 modbus 主站 (主动发送请求

信息)，这时 HMI 的通讯口协议选择 Modbus maser，从站的站号是通过通讯口配置中的 HMI 站号进行设置。

选择 Modbus maser，通讯口配置中 HMI 站号与设备站号必须保持一致。



从站只有被读跟被写的功能，没有主动发送数据的功能，主站给从站发送代码，从站回复的一种功能。

2、通讯配置

串口参数的配置（波特率、数据位、停止位、校验位、）通讯口的配置是 RS232、RS485 还是 422，还有 Modbus 设备站号的配置，这些参数要对应上才能通讯。



3、通讯地址的格式

维控触摸屏的地址格式是十进制的地址格式，有的仪表地址格式是 16 进制的，屏上使用要把 16 进制的地址格式转换成十进制的地址格式使用。维控 HMI 上的地址编写基本上以 10 进制编写为主，有特殊地址编写格式时，可查看地址编辑器右侧的地址填写说明。



通讯数据地址 十六进制	含义	说明	操作
0000 _h ~ 03FF _h	参数区	对应参数表中的参数	可读可写
0400 _h ~ 0409 _h	报警信息存储区	10 个历史报警	只读
0410 _h	速度指令零点偏移量		只读
0411 _h	转矩指令零点偏移量		只读
0412 _h	Iu 零点偏移量		只读
0413 _h	Iv 零点偏移量		只读
0420 _h ~ 0437 _h	监控数据		只读
0420 _h	电机转速	单位: 1r/min	只读
0422 _h	旋转角 (电气角)	单位: 1deg	只读
0424 _h	输入指令脉冲速度	单位: 1kHz	只读
0426 _h	母线电压	单位: 1V	只读
0428 _h	模拟输入速度指令值	单位: 1 r/min	只读
042A _h	模拟输入转矩指令百分比	单位: 1%	只读
042C _h	内部转矩指令百分比	单位: 1%或 0.1A	只读
042E _h	输入信号监视	——	只读
0430 _h	输出信号监视	——	只读

表格是伺服驱动器的 Modbus 的地址，格式是 16 进制的，触摸屏使用旧要把 16 进制的地址格式转换成 10 进制的地址格式，

例如：0430（输出信号的监视）触摸屏的地址用 1072 地址，监控的地址才是（输出信号监视）

4、地址的读写

仪表中有的地址是只读或者只写，这种情况下，不能把触摸屏上的地址都配置成读写，否则将可能会造成通讯不上。

如下图表格中的地址有：可读可写，可写，只读三种模式，通讯的时候要注意下，触摸屏的地址编辑模式也有三种：读取地址（读），输入地址（写），读取跟输入同时使用（读写），通讯的时候要注意下，地址编辑的格式要配置成哪种模式。

045Fh	FPGA 版本号		只读
0520h	清除历史报警	1: 清除历史报警	可读可写
0521h	清除当前报警	1: 清除当前报警	可读可写
0522h	清除总线编码器报警	1: 清除总线编码器报警	可读可写
0523h	清除总线编码器多圈数据	1: 清除总线编码器多圈数据	可读可写
0528h	速度 JOG (转速为 P□304 设置)	BIT15:1 JOG 伺服使能 BIT01:1 JOG- (JOG 正转) BIT00:1 JOG+ (JOG 反转)	可读可写
0529h	位置 JOG (转速为 P□304 设置)	BIT15:1 进入位置点动模式 BIT01:1 JOG- BIT00:1 JOG+	可读可写
0540h	恢复出厂值	1: 恢复出厂值	可写
0541h	复位	1: 复位	可写
05F0h	当前正在运行数据组号		只读
05F1h	即将运行数据组号		只读
05F2h	实际位置低 16 位	位置接点电子齿轮后的位置	只读
05F3h	实际位置高 16 位		只读
05F4h	位置节点方式	0: 任务 1: 外部	只读
05F5h	加速度	10rpm/s/s	可读可写
05F6h	减速度	10rpm/s/s	可读可写
05F7h	紧急减速度	10rpm/s/s	可读可写
05F8h	位置接点电子齿轮分子		可读可写

数值输入/显示

基本 图形 扩展 高级 动画

基本功能

读取地址

40

地址编辑

☒ 输入
☒ 输入地址与读取地址相同

输入地址

40

地址编辑

键盘画面

1000: BuilNum

▼

键盘备注

显示

☐ 快速更新
☐ 透明显示
☐ 内容显示 '*' 号

☐ 不开启弹出式键盘

☐ 显示自然小数

文字对齐

居中

▼

设置显示字体

5、地址的读写长度设置

Modbus 协议多用于仪器仪表、单片机等开放性设备的通讯，维控支持的 MODBUS 协议是国际标准的接口通讯设备。目前市面上很多仪器仪表的通讯协议都基于标准的 modbus 协议进行二次开发，在数据的读写长度上会进行自定义配置。为了满足市面上各种基于标准 modbus 协议而进行读写长度限制的功能，开放读写长度的配置地址。

用单片机举例，有的单片机的地址读取的长度的配置是固定的，读取的地址只能是 10 个长度的读（这是一个固定的长度的读才能通讯上），这种情况下，触摸屏只能发送：01 03 00 00 00 0a C5 CD 才能通讯上。当触摸屏上只放 40/30 这个地址，发送的代码格式是：01 03 00 00 00 01 84 0a（发这种指令下位机是不给返回的）。这种情况下也会造成通讯不上的，可以通过 Modbus 协议中有个 readlen 的地址配置连续的长度。

Readlen 的地址的值配置的是 10，触摸屏发送读取的代码为：01 03 00 00 00 0a C5 CD。注意：readlen 地址编号只有 0，最大值设置要小于 128。



6、多设备连接的配置

当 MODBUS 通讯选 RS485 通讯的方式可以接多台从站设备，设备可以设置不同的站号，触摸屏通过地址编辑中有个 PLC 站号（预设站号），对不同的站号进行区分。

（1）若使用 modbus 协议连接多台设备时，在【工程参数】中设备站号可默认，无需对应。但在界面上对不同站号的从站设备监控地址进行配置，必须配置对应的从站站号。

例如：从站的设备站号是 5，要读取的地址是 0；触摸屏的地址编辑方式如下图所示：

（2）若是从站只接一台，可通过通讯口配置的界面，设备站号进行区分，地址编辑就可以不用配置 PLC 站号（预设站号）。

通讯口配置

请选择设备类型:

编号	通讯口	串口协议	设备类型
1	COM1	RS485	ModBus RTU Slave(All Fuct...

添加新连接
删除连接
更改连接

预设地址/站号

HMI站号: 0

设备站号: 1

所选的通讯口: COM1

协议: ModBus RTU Slave(All Fuction)

所使用的HMI型号: PI8070

串口参数设置: (RS485, 9600, 1, 8, NONE) 设置...

以太网参数设置: 无 设置...

超时设置: (300, 50, 2, 3, 0, 0) 设置...

☐ 修改配置不改变参数

用户自定义协议
确定修改
取消
帮助

与PLC连线示意图:

ModBus 485 通讯线接法

HMI com1
9针 (female)

RS485

1 RX+ ————— A+
6 RX- ————— B-
5 GND ————— GND

HMI串口引脚定义:

COM1 引脚定义原理图

管脚	定义	管脚	定义
1	RS422 TX+ (RS485+)	2	RS232 RXD
3	RS232 TXD	5	GND
6	RS422 TX- (RS485-)	8	RS422 RX-
9	RS422 RX+		