

信捷人机界面 Modbus RTU 功能码

一、Modbus 协议简介

Modbus 协议是应用于电子控制器上的一种通用语言。通过此协议，控制器相互之间、控制器经由网络和其它设备之间可以通信，它已经成为一通用工业标准。有了它，不同厂商生产的控制设备可以连成工业网络，进行集中监控。此协议定义了一个控制器能认识使用的消息结构，而不管它们是经过何种网络进行通信的，它描述了一控制器请求访问其它设备的过程，如何回应来自其它设备的请求，以及怎样侦测错误并记录，它制定了消息域格局和内容的公共格式。

当在一个 Modbus 网络上通信时，此协议决定了每个控制器须要知道它们的设备地址，识别按地址发来的消息，决定要产生何种行动。如果需要回应，控制器将生成反馈信息并用 Modbus 协议发出。在其它网络上，包含了 Modbus 协议的消息被转换为在此网络上可使用的帧或包结构，这种转换也扩展了根据具体的网络解决节地址、路由路径及错误检测的方法。

二、在 Modbus 网络上传输

标准的 Modbus 口是使用 RS-232C 兼容串行接口，它定义了连接口的针脚、电缆、信号位、传输波特率、奇偶校验。控制器能直接或经由 Modem 组网。控制器通信使用主-从技术，即某一设备（主设备）能初始化传输（查询），其它设备（从设备）根据主设备查询提供的数据做出相应反应。典型的主设备：主机和可编程仪表；典型的从设备：可编程逻辑控制器。

主设备可单独和从设备通信，也能以广播方式和所有从设备通信。如果单独通信，从设备返回一个消息作为回应；如果是广播方式查询的，则不作任何回应。Modbus 协议建立了主设备查询的格式：设备地址、功能代码、所有要发送的数据、错误检测域。从设备回应消息也由 Modbus 协议构成，包括确认要行动的域、任何要返回的数据和错误检测域。如果在消息接收过程中发生错误，或从设备不能执行其命令，从设备将建立错误消息并把它作为回应发送出去。

三、Modbus-RTU 功能码

测试工具：信捷 T-com 串口调试工具或其它串口调试工具。信捷人机界面 Modbus 功能代码如下：

功能码（16 进制）	功能
01	读取线圈状态，读取一组逻辑线圈的当前状态（ON/OFF）
02	读取输入状态，读取一组开关输入的当前状态（ON/OFF）
03	读取保持寄存器，在一个或多个保持寄存器中取得当前二进制值
04	读取输入寄存器，在一个或多个输入寄存器中取得当前二进制值
05	强制（写）单线圈，强制（写）一个逻辑线圈的通断状态（ON/OFF）
06	预置（写）单寄存器，把具体二进制值写入一个保持寄存器
0F	强制（写）多线圈，强制（写）一串连续逻辑线圈的通断状态（ON/OFF）
10	预置（写）多寄存器，把具体二进制值写入一串连续的保持寄存器

注意：以下测试地址都是十六进制地址，实际操作需将十六进制地址转换成十进制地址输入到人机界面中。**06 和 10 功能码通过人机界面内部地址 PFW36.2 进行切换，PFW36.2=0 时发 0x06 功能码，PFW36.2=1 时发 0x10 功能码，PFW36.2 的状态需重新上电才会生效。**

1. 01 功能码：读取线圈状态

读取线圈状态，读取一组逻辑线圈的当前状态（ON/OFF），对应人机界面上地址类型 0X。

例：以信捷 XC PLC 为例，读取线圈 0X4800~0X4815（即 PLC 地址 Y0~Y17）的位状态。

发送：01 01 48 00 00 10 2A 66

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址高 位(1 Byte)	起始地址低 位(1 Byte)	数据总位数 高位(1 Byte)	数据总位数 低位(1 Byte)	CRC (1 Byte)	(1 Byte)
发送	01	01	48	00	00	10	2A	66

动作	站点号 (1 Byte)	功能码 (1 Byte)	字节数 (1 Byte)	位状态 (ON/OFF)	位状态 (ON/OFF)	CRC (1 Byte)	(1 Byte)
返回 ON	01	01	02	FF	FF	B8	4C
返回 OFF	01	01	02	00	00	B9	FC

2. 02 功能码：读取输入状态

读取输入状态，读取一组开关输入的当前状态（ON/OFF），对应人机界面上地址类型 1X，只读类型。

例：以人机界面为例，读取 1X16~1X31 的当前状态（信捷 PLC 暂不支持该功能码）。

发送：01 02 00 10 00 10 78 03

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址高 位(1 Byte)	起始地址低 位(1 Byte)	数据总位数 高位(1 Byte)	数据总位数 低位(1 Byte)	CRC (1 Byte)	(1 Byte)
发送	01	02	00	10	00	10	78	03

动作	站点号 (1 Byte)	功能码 (1 Byte)	字节数 (1 Byte)	位状态 (ON/OFF)	位状态 (ON/OFF)	CRC (1 Byte)	(1 Byte)
返回 ON	01	02	02	FF	FF	B8	08
返回 OFF	01	02	02	00	00	B9	B8

3. 03 功能码：读取保持寄存器

读取保持寄存器，在一个或多个保持寄存器中取得当前二进制值，对应人机界面上地址类型 4X。

例：以信捷 XC PLC 为例，读取 4X00~4X03（即 PLC 地址 D0~D3）中的数值，4X00（D0）= 4，4X01（D1）= 5，4X02（D2）= 1，4X03（D3）= 2。

发送：01 03 00 00 00 04 44 09

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址高 位(1 Byte)	起始地址低 位(1 Byte)	数据总位数 高位(1 Byte)	数据总位数 低位(1 Byte)	CRC (1 Byte)	(1 Byte)
发送	01	03	00	00	00	04	44	09

返回：01 03 08 00 04 00 05 00 01 00 02 CC 16

动作	站点号 (1 Byte)	功能码 (1 Byte)	字节数 (1 Byte)	寄存器值 高位 4X00	寄存器值 低位 4X00	寄存器值 高位 4X01	寄存器值 低位 4X01
返回	01	03	08	00	04	00	05
		寄存器值 高位 4X02	寄存器值 低位 4X02	寄存器值 高位 4X03	寄存器值 低位 4X03	CRC (1 Byte)	(1 Byte)
		00	01	00	02	CC	16

4. 04 功能码: 读取输入寄存器

读取输入寄存器, 在一个或多个输入寄存器中取得当前二进制值, 对应人机界面上地址类型 3X, 只读类型。

例: 以人机界面为例, 读取 3X00~3X03 中的数值 (信捷 PLC 暂不支持该功能码), 3X00 = 4, 3X01= 5, 3X02= 1, 3X03= 2。

发送: 01 04 00 00 00 04 F1 C9

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址高 位(1 Byte)	起始地址低 位(1 Byte)	数据总位数 高位(1 Byte)	数据总位数 低位(1 Byte)	CRC (1 Byte)	(1 Byte)
发送	01	04	00	00	00	04	F1	C9

返回: 01 04 08 00 04 00 05 00 01 00 02 7D CC

动作	站点号 (1 Byte)	功能码 (1 Byte)	字节数 (1 Byte)	寄存器值 高位 3X00	寄存器值 低位 3X00	寄存器值 高位 3X01	寄存器值 低位 3X01
返回	01	04	08	00	04	00	05
		寄存器值 高位 3X02	寄存器值 低位 3X02	寄存器值 高位 3X03	寄存器值 低位 3X03	CRC (1 Byte)	(1 Byte)
		00	01	00	02	7D	CC

5. 05 功能码: 强制 (写) 单线圈

强制 (写) 单线圈, 强制 (写) 一个逻辑线圈的通断状态 (ON/OFF), 对应人机界面上地址类型 0X。

例: 以信捷 XC PLC 为例, 置 ON/置 OFF 线圈 0X4800 (即 PLC 地址 Y0)。

发送 ON: 01 05 48 00 FF 00 9B 9A

发送 OFF: 01 05 48 00 00 00 DA 6A

动作	站点号 (1 Byte)	功能码 (1 Byte)	线圈地址高 位(1 Byte)	线圈地址低 位(1 Byte)	强制状态 (ON/OFF)		CRC (1 Byte)	(1 Byte)
发送 ON	01	05	48	00	FF	00	9B	9A
发送 OFF	01	05	48	00	00	00	DA	6A

动作	站点号 (1 Byte)	功能码 (1 Byte)	线圈地址高 位(1 Byte)	线圈地址低 位(1 Byte)	返回状态 (ON/OFF)		CRC (1 Byte)	(1 Byte)
返回 ON	01	05	48	00	FF	00	9B	9A
返回 OFF	01	05	48	00	00	00	DA	6A

6. 06 功能码: 预置 (写) 单寄存器

预置 (写) 单寄存器, 把具体二进制值写入一个保持寄存器, 对应人机界面上地址类型 4X。

例: 以信捷 XC PLC 为例, 地址 4X00 (PLC 地址 D0) 写入数值 8。

发送: 01 06 00 00 00 08 88 0C

动作	站点号 (1 Byte)	功能码 (1 Byte)	寄存器地址 高位(1 Byte)	寄存器地址 低位(1 Byte)	寄存器值高 位(1 Byte)	寄存器值低 位(1 Byte)	CRC (1 Byte)	(1 Byte)
发送	01	06	00	00	00	08	88	0C

返回：01 06 00 00 00 08 88 0C

动作	站点号 (1 Byte)	功能码 (1 Byte)	寄存器地址 高位(1 Byte)	寄存器地址 低位(1 Byte)	寄存器值高 位(1 Byte)	寄存器值低 位(1 Byte)	CRC (1 Byte)	(1 Byte)
返回	01	06	00	00	00	08	88	0C

7. 0F 功能码：强制（写）多线圈

强制（写）多线圈，强制（写）一串连续逻辑线圈的通断状态（ON/OFF），对应人机界面上地址类型 0X。

例：以信捷 XC PLC 为例，置 ON/置 OFF 线圈 0X4800~4808（即 PLC 地址 Y0~Y7，Y10），线圈总数 9 位，占用一个寄存器（16 个位为一个字），即 2 个 Byte。线圈值排列规则如下：

Y0(0X4800)	Y1(0X4801)	Y2~Y6(0X4802~0X4806)	Y7(0X4807)	Y10(0X4808)
------------	------------	----------------------	------------	-------------

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址 高位 1 Byte	起始地址 低位 1 Byte	位总数 高位 1 Byte	位总数 低位 1 Byte	位总数 字节数 1 Byte	位的值 低位 1 Byte	位的值 高位 1 Byte	CRC 1 Byte	1 Byte
发送 ON	01	0F	48	00	00	09	02	FF	01	AD	48
发送 OFF	01	0F	48	00	00	09	02	00	00	2D	78

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址高 位(1 Byte)	起始地址低 位(1 Byte)	位总数高 位(1 Byte)	位总数低 位(1 Byte)	CRC (1 Byte)	(1 Byte)
返回	01	0F	48	00	00	09	82	6D

8. 10 功能码：预置（写）多寄存器

预置（写）多寄存器，把具体二进制值写入一串连续的保持寄存器，对应人机界面地址类型 4X。

例：以信捷 XC PLC 为例，地址 4X00~4X02（PLC 地址 D0~D2）写入数值，4X00（D0）= 10，4X01（D1）= 11，4X02（D2）= 12。

发送：01 10 00 00 00 03 06 00 0A 00 0B 00 0C 0F 46

动作	站点号 (1Byte)	功能码 (1Byte)	起始地址 高位 (1Byte)	起始地址 低位 (1 Byte)	寄存器 总数高位 (1 Byte)	寄存器 总数低位 (1 Byte)	寄存器 总字节数 (1 Byte)	寄存器 值高位 (1 Byte)	寄存器 值低位 (1 Byte)
发送	01	10	00	00	00	03	06	00	0A
				寄存器 值高位 (1 Byte)	寄存器 值低位 (1 Byte)	寄存器 值高位 (1 Byte)	寄存器 值低位 (1 Byte)	CRC (1 Byte)	(1 Byte)
				00	0B	00	0C	0F	46

返回：01 10 00 00 00 03 80 08

动作	站点号 (1 Byte)	功能码 (1 Byte)	起始地址 高位 (1 Byte)	起始地址 低位 (1 Byte)	寄存器 总数高位 (1 Byte)	寄存器 总数低位 (1 Byte)	CRC (1 Byte)	(1 Byte)
返回	01	10	00	00	00	03	80	08