信科电子 modbus 协议说明

V1.7

信科电子

本文档适用于信科电子出品的

支持 modbus 协议产品的使用

（适用于固件版本号：0.122 或以上产品）

一、概述

本公司出品的支持“3.0 内核工具软件”编程的产品，可通过编程设置“使能 modbus”，支持功能码：01、02、03、05、06、15、16，设备的板地址出厂设置默认为 1，用户可以根据需要进行地址修改(注意：模块上电 10 秒内写地址有效)。

二、功能码说明及举例

（1）功能码 01 - 读离散线圈状态

功能描述：读取从机离散线圈（位）的状态。

指令格式:[设备地址][功能码 01][起始地址高字节][起始地址低字节][线圈数量高字节][线圈数量低字节][CRC 校验低字节][CRC 校验高字节]

举例：

①读取从设备地址为 01 的前 10 个线圈状态

指令： 01 01 00 00 00 0A BC 0D

解析：设备地址 功能码 起始地址 线圈数量 CRC 校验

②读取从设备地址为 02 的从线圈地址 5 开始的 8 个线圈状态

指令： 02 01 00 05 00 08 2D FE

解析：设备地址 功能码 起始地址 线圈数量 CRC 校验

③读取从设备地址为 03 的从线圈地址 10 开始的 12 个线圈状态

指令： 03 01 00 0A 00 0C 1D EF

解析：设备地址 功能码 起始地址 线圈数量 CRC 校验

（2）功能码 02 - 读离散输入状态

功能描述：读取从机离散输入（位）的状态。

指令格式:[设备地址][功能码 02][起始地址高字节][起始地址低字节][输入数量高字节][输入数量低字节][CRC 校验低字节][CRC 校验高字节]

举例：

①读取从设备地址为 01 的前 15 个离散输入状态。

指令： 01 02 00 00 00 0F 38 0E

解析：设备地址 功能码 起始地址 输入数量 CRC 校验

②读取从设备地址为 02 的从离散输入地址 8 开始的 10 个输入状态。

指令： 02 02 00 08 00 0A 79 FC

解析：设备地址 功能码 起始地址 输入数量 CRC 校验

③读取从设备地址为 03 的从离散输入地址12开始的6个输入状态。
指令： 03 02 00 0C 00 06 39 E9
解析：设备地址 功能码 起始地址 输入数量 CRC 校验

（3）功能码 03 - 读保持寄存器

功能描述：读取从机保持寄存器中的内容。
指令格式:[设备地址][功能码 03][起始地址高字节][起始地址低字节][寄存器数量高字节][寄存器数量低字节][CRC 校验低字节][CRC 校验高字节]
举例：
①读取从设备地址为 01 的从寄存器地址10开始的3个寄存器内容。
指令： 01 03 00 0A 00 03 25 C9
解析：设备地址 功能码 起始地址 寄存器数量 CRC 校验
②读取从设备地址为 02 的从寄存器地址20开始的2个寄存器内容。
指令： 02 03 00 14 00 02 84 3C
解析：设备地址 功能码 起始地址 寄存器数量 CRC 校验
③读取从设备地址为 03 的从寄存器地址30开始的4个寄存器内容。
指令： 03 03 00 1E 00 04 25 ED
解析：设备地址 功能码 起始地址 寄存器数量 CRC 校验

（4）功能码 05 - 写单个线圈

功能描述：强制单个线圈为 ON 或 OFF。
指令格式:[设备地址][功能码 05][线圈地址高字节][线圈地址低字节][输出值高字节][输出值低字节][CRC 校验低字节][CRC 校验高字节]
举例：
①将从设备地址为 01 的线圈地址 5 设置为 ON。
指令： 01 05 00 05 FF 00 9C 3B
解析：设备地址 功能码 线圈地址 输出值FF 00（ON） CRC 校验
②将从设备地址为 02 的线圈地址 8 设置为 OFF。
指令： 02 05 00 08 00 00 4C 3B
解析：设备地址 功能码 线圈地址 输出值00 00（OFF） CRC 校验
③将从设备地址为 03 的线圈地址 12 设置为 ON。
指令： 03 05 00 0C FF 00 4D DB
解析：设备地址 功能码 线圈地址 输出值FF 00（ON） CRC 校验

（5）功能码 06 - 写单个寄存器

功能描述：将一个值写入单个保持寄存器。

指令格式:[设备地址][功能码 06][寄存器地址高字节][寄存器地址低字节][写入值高字节][写入值低字节][CRC 校验低字节][CRC 校验高字节]

举例：

①将值 100 写入从设备地址为 01 的寄存器地址 15。

指令： 01 06 00 0F 00 64 B8 22

解析：设备地址 功能码 寄存器地址 写入值 100（00 64）CRC 校验

②将值 200 写入从设备地址为 02 的寄存器地址 22。

指令： 02 06 00 16 00 C8 69 AB

解析：设备地址 功能码 寄存器地址 写入值 200（00 C8）CRC 校验

③将值 300 写入从设备地址为 03 的寄存器地址 35。

指令： 03 06 00 23 01 2C 79 AF

解析：设备地址 功能码 寄存器地址 写入值 300（01 2C）CRC 校验

（6）功能码 15 - 写多个线圈

功能描述：强制一系列线圈为 ON 或 OFF。

指令格式:[设备地址][功能码 15][起始地址高字节][起始地址低字节][线圈数量高字节][线圈数量低字节][字节数量][写入值][CRC 校验低字节][CRC 校验高字节]

举例：

①将从设备地址为 01 的从线圈地址 5 开始的 4 个线圈设置为 ON。

指令： 01 0F 00 05 00 04 01 FF B2 D6

解析：设备地址 功能码 起始地址 线圈数量 字节数量 写入值 FF（全为 ON） CRC 校验

②将从设备地址为 02 的从线圈地址 8 开始的 3 个线圈设置为 OFF。

指令： 02 0F 00 08 00 03 01 00 2E 83

解析：设备地址 功能码 起始地址 线圈数量 字节数量 写入值 00（全为 OFF） CRC 校验

③将从设备地址为 03 的从线圈地址 12 开始的 5 个线圈设置为交替 ON/OFF。

指令： 03 0F 00 0C 00 05 01 15 3F 41

解析：设备地址 功能码 起始地址 线圈数量 字节数量 写入值 15（交替 ON/OFF） CRC 校验

（7）功能码 16 - 写多个寄存器

功能描述：将一系列值写入多个保持寄存器。

指令格式:[设备地址][功能码 16][起始地址高字节][起始地址低字节][寄存器数量高字节][寄存器数量低字节][字节数量][写入值 1][写入值 2]...[CRC 校验低字节][CRC 校验高字节]

举例：

①将值 100、200、300 分别写入从设备地址为 01 的从寄存器地址 10、11、12。

指令： 01 10 00 0A 00 03 06 00 64 00 C8 01 2C 36 DB

解析：设备地址 功能码 起始地址 寄存器数量 字节数量 写入值 100 写入值 200 写入值 300 CRC 校验

②将值 400、500 分别写入从设备地址为 02 的从寄存器地址 15、16。

指令： 02 10 00 0F 00 02 04 01 90 01 F4 BD 6D

解析：设备地址 功能码 起始地址 寄存器数量 字节数量 写入值 400 写入值 500 CRC 校验

③将值 600、700、800 分别写入从设备地址为 03 的从寄存器地址 20、21、22。

指令： 03 10 00 14 00 03 06 02 58 02 BC 03 20 40 D9

解析：设备地址 功能码 起始地址 寄存器数量 字节数量 写入值 600 写入值 700 写入值 800 CRC 校验

三、modbus 寄存器说明及举例

在 modbu 中寄存器地址 0 代表 modbus 地址 1，以此类推，1000 代表 modbus 地址 1001。本文中的所有地址都采用实际寄存器地址。只有输入部分对应寄存器是只可读的，其它寄存器都是可读可写的。本文中的寄存器，支持 modbus 03 06 16 功能码。

（1）输出部分

输出部分寄存器从地址 1000 开始，可读写。

一个寄存器对应 16 个继电器的状态，bit0 代表第 1 路，bit1 代表第 2 路，依次类推。对于超过 16 路继电器的产品，寄存器地址依次往下推。

举例：

①读取地址为 01 的前 16 路继电器状态：

指令：　01　03　03 E8　00 01　04 7A

解析：设备地址 功能码 寄存器地址 1000 寄存器数量 CRC 校验

②设置地址为 01 的第 1 路继电器闭合：

指令：　01　06　03 E8　00 01　C8 7A

解析：设备地址 功能码 寄存器地址 1000 写入值 00 01 CRC 校验

③设置地址为 01 的第 16 路继电器闭合：

指令：　01　06　03 E8　80 00　68 7A

解析：设备地址 功能码 寄存器地址 1000 写入值 80 00 CRC 校验

（2）输入部分

输入部分寄存器地址为 500，只读。

输入的状态，从第 1 路输入到第 n 路输入，n 取决于具体产品的输入路数。寄存器地址 500 的 bit0 代表第 1 路输入，bit1 代表第 2 路输入，依次类推。

举例：

①读取地址 01 的第 1-16 路输入状态：

指令：　01　03　01 F4　00 01　C4 04

解析：设备地址 功能码 寄存器地址 500 寄存器数量 CRC 校验

②读取地址 02 的第 1-16 路输入状态：

指令：　02　03　01 F4　00 01　C4 37

解析：设备地址 功能码 寄存器地址 500 寄存器数量 CRC 校验

③读取地址 03 的第 1-16 路输入状态：

指令：　03　03　01 F4　00 01　C5 E6

解析：设备地址 功能码 寄存器地址 500 寄存器数量 CRC 校验

（3）位变量部分

位变量部分寄存器地址为 2500，可读写。

从位变量 0 到位变量 n，n 可以用软件读取出来。

位变量 0 对应寄存器地址 2500 的 bit0，与继电器状态类似。公司产品一般至少有 32 个位变量（位变量 0 - 31），有的可能更多。

举例：

①读取地址 01 的位变量 0 - 15 的状态：

指令：　01　03　09 C4　00 01　C6 6B

解析：设备地址 功能码 寄存器地址 2500 寄存器数量 CRC 校验

②设置地址 01 的位变量 5 为 1：

指令：	01	06	09 C4	00 20	CA 73
解析：	设备地址	功能码	寄存器地址 2500	写入值 bit5 为 1 其余为 0	CRC 校验

③设置地址 01 的位变量 31 为 1：

指令：	01	06	09 C5	80 00	FB AB
解析：	设备地址	功能码	寄存器地址 2501	写入值 bit31 为 1 其余为 0	CRC 校验

（4）全局整数部分

全局整数从 modbus 寄存器地址 1600 开始。

每个整数 32 位，对应两个寄存器地址。寄存器 1600 对应全局整数 0 的低 16 位，寄存器 1601 对应全局整数 0 的高 16 位，寄存器 1602 对应全局整数 1 的低 16 位，依次类推。数量可以通过软件读取。

举例：

①读取地址 01 的全局整数 0：

指令：	01	03	06 40	00 02	C5 57
解析：	设备地址	功能码	寄存器地址 1600	寄存器数量	CRC 校验
指令：	01	03	06 41	00 02	94 97
解析：	设备地址	功能码	寄存器地址 1601	寄存器数量	CRC 校验

②设置地址 01 的全局整数 1 为 1000：

指令：	01	06	06 42	03 E8	29 E8
解析：	设备地址	功能码	寄存器地址低位 1602	写入值 1000	CRC 校验
指令：	01	06	06 43	03 E8	78 28
解析：	设备地址	功能码	寄存器地址高位 1603	写入值 1000	CRC 校验

③设置地址 01 的全局整数 2 为 2000：

指令：	01	06	06 44	07 D0	CA FB
解析：	设备地址	功能码	寄存器地址低位 1604	写入值 2000	CRC 校验
指令：	01	06	06 45	07 D0	9B 3B
解析：	设备地址	功能码	寄存器地址高位 1605	写入值 2000	CRC 校验

四、modbus 指令写地址说明及举例

功能描述：modbus 写地址功能主要用于修改从设备的特定地址信息，

写地址时， modbus 寄存器地址为 0（注意：模块上电 10 秒内写地址有效）。

指令格式:[原设备地址][功能码 0x06][寄存器地址高字节][寄存器地址低字节][写入值高字节][写入值低字节][CRC 校验低字节][CRC 校验高字节]

举例:

①使用 modbus 指令将 485 继电器板地址从 1 改为 2

指令: 01 06 00 00 00 02 08 0B

解析: 设备地址 功能码 寄存器地址 写入新地址 CRC 校验

②使用 modbus 指令将 485 继电器板地址从 2 改为 3

指令: 02 06 00 00 00 03 C9 F8

解析: 设备地址 功能码 寄存器地址 写入新地址 CRC 校验

③使用 modbus 指令将 485 继电器板地址从 3 改为 5

指令: 03 06 00 00 00 05 48 2B

解析: 设备地址 功能码 寄存器地址 写入新地址 CRC 校验