

附录 A Modbus 通讯协议

300 系列变频器提供 RS485 通信接口，并支持 Modbus-RTU 从站通讯协议。用户可通过计算机或 PLC 实现集中控制，通过该通讯协议设定变频器运行命令，修改或读取功能码参数，读取变频器的工作状态及故障信息等。

A.1 协议内容

该串行通信协议定义了串行通信中传输的信息内容及使用格式。其中包括：主机轮询（或广播）格式；主机的编码方法，内容包括：要求动作的功能码，传输数据和错误校验等。从机的响应也是采用相同的结构，内容包括：动作确认，返回数据和错误校验等。如果从机在接收信息时发生错误，或不能完成主机要求的动作，它将组织一个故障信息作为响应反馈给主机。

应用方式

变频器接入具备 RS485 总线的“单主多从”PC/PLC 控制网络，作为通讯从机。

总线结构

(1) 硬件接口

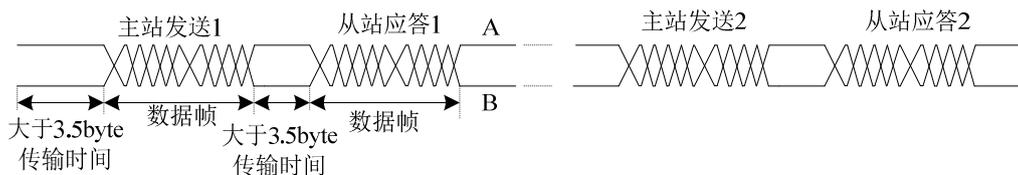
变频器端子 485+、485-为 Modbus 通信接口。

(2) 拓扑结构

单主机多从机系统。网络中每一个通讯设备都有一个唯一的从站地址，其中有一个设备作为通讯主机（常为 PC 上位机、PLC、HMI 等），主动发起通讯，对从机进行参数读或写操作，其他设备在为通讯从机，响应主机对本机的查询或通讯操作。在同一时刻只能有一个设备发送数据，而其他设备处于接收状态。从机地址的设定范围为 0~247，0 为广播通信地址。网络中的从机地址必须是唯一的。

(3) 通讯传输方式

异步串行，半双工传输方式。数据在串行异步通信过程中，是以报文的形式，一次发送一帧数据，Modbus-RTU 协议中约定，当通讯数据线上无数据的空闲时间大于 3.5Byte 的传输时间，表示新的一个通讯帧的起始。

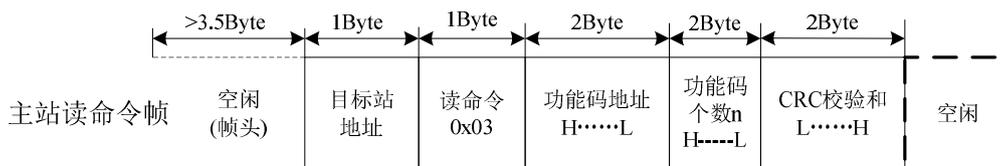


300 系列变频器内置的通信协议是 Modbus-RTU 从机通信协议，可响应主机的“查询/命令”，或根据主机的“查询/命令”做出相应的动作，并通讯数据应答。

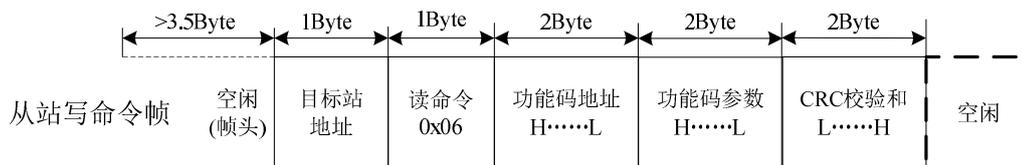
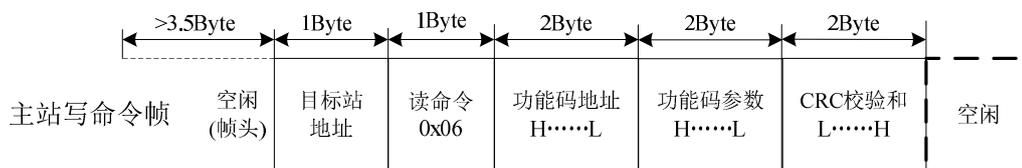
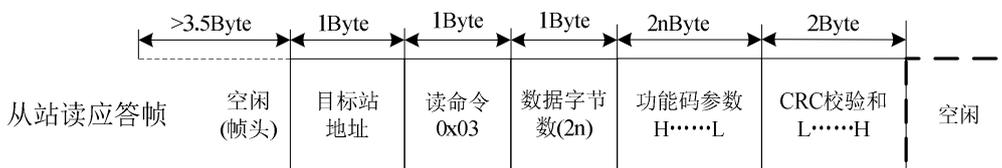
主机可以是指个人计算机（PC），工业控制设备或可编程逻辑控制器（PLC）等，主机既能对某个从机单独进行通信，也能对所有下位从机发布广播信息。对于主机的单独访问“查询/命令”，被访问从机要返回一个应答帧；对于主机发出的广播信息，从机无需反馈响应给主机。

通讯资料结构

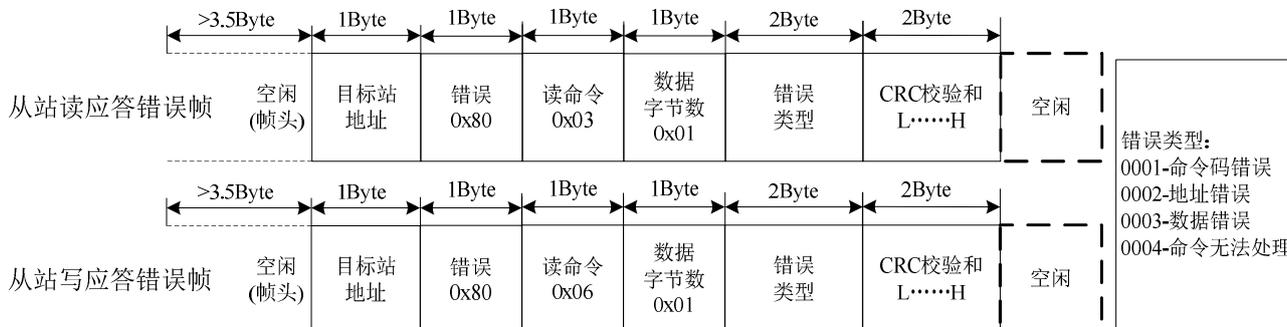
300 系列变频器的 Modbus 协议通讯数据格式如下，变频器只支持 Word 型参数的读或写，对应的通讯读操作命令为 0x03；写操作命令为 0x06，不支持字节或位的读写操作：



理论上，上位机可以一次读取连续的几个功能码（即其中 n 最大可达 12 个），但要注意不能跨过本功能码组的最后一个功能码，否则会答复出错。



若从机检测到通讯帧错误，或其他原因导致的读写不成功，会答复错误帧。



数据帧字段说明：

帧头 START	大于 3.5 个字符传输时间的空闲
从机地址 ADR	通讯地址范围：0~247；0=广播地址
命令码 CMD	03：读从机参数；06：写从机参数
功能码地址 H	变频器内部的参数地址，16 进制表示；分为功能码型和非功能码型（如运行状态参数、运行命令等）参数等，详见地址定义。传送时，高字节在前，低字节在后。
功能码地址 L	
功能码个数 H	本帧读取的功能码个数，若为 1 表示读取 1 个功能码。传送时，高字节在前，低字节在后。
功能码个数 L	
数据 H	应答的数据，或待写入的数据，传送时，高字节在前，低字节在后。

数据 L	
CRC CHK 低位	检测值：CRC16 校验值。传送时，低字节在前，高字节在后。
CRC CHK 高位	计算方法详见本节 CRC 校验的说明。
END	3.5 个字符时

CRC 校验方式：

CRC (Cyclical Redundancy Check) 使用 RTU 帧格式，消息包括了基于 CRC 方法的错误检测域。CRC 域检测了整个消息的内容。CRC 域是两个字节，包含 16 位的二进制值。它由传输设备计算后加入到消息中。接收设备重新计算收到消息的 CRC，并与接收到的 CRC 域中的值比较，如果两个 CRC 值不相等，则说明传输有错误。

CRC 是先存入 0xFFFF，然后调用一个过程将消息中连续的 8 位字节与当前寄存器中的值进行处理。仅每个字符中的 8Bit 数据对 CRC 有效，起始位和停止位以及奇偶校验位均无效。CRC 产生过程中，每个 8 位字符都单独和寄存器内容相异或 (XOR)，结果向最低有效位方向移动，最高有效位以 0 填充。LSB 被提取出来检测，如果 LSB 为 1，寄存器单独和预置的值相异或，如果 LSB 为 0，则不进行。整个过程要重复 8 次。在最后一位 (第 8 位) 完成后，下一个 8 位字节又单独和寄存器的当前值相异或。最终寄存器中的值，是消息中所有的字节都执行之后的 CRC 值。

CRC 添加到消息中时，低字节先加入，然后高字节。CRC 简单函数如下：

```
unsigned int crc_chk_value (unsigned char *data_value,unsigned char length)
```

```
{
    unsigned int crc_value=0xFFFF;
    int i;
    while (length--)
    {
        crc_value^=*data_value++;
        for (i=0;i<8;i++)
        {
            if (crc_value&0x0001)
            {
                crc_value= (crc_value>>1) ^0xa001;
            }
            else
            {
                crc_value=crc_value>>1;
            }
        }
    }
    return (crc_value) ;
}
```

通信参数的地址定义

读写功能码参数 (有些功能码是不能更改的，只供厂家使用或监视使用)：

以功能码组号和标号为参数地址表示规则：

高位字节：F0~FF(F0~FF 组)、d0~dF(d0~dF 组)

低位字节：00~FF

例如：若要范围功能码 F0-20，则功能码的访问地址表示为 0xF016；

注意：

有些参数在变频器处于运行状态时，不可更改；有些参数不论变频器处于何种状态，均不可更改；更改功能码参数，还要注意参数的范围，单位及相关说明。

功能码组号	通讯访问地址	通讯修改 RAM 访问地址
F0~FF	0xF000~0xFFFF	0x0000~0x0FFF
d0~dF	0xD000~0xDFFF	0x4000~0x4FFF

注意，由于 EEPROM 频繁被存储，会减少 EEPROM 的使用寿命，所以，有些功能码在通讯的模式下，无须存储，只要更改 RAM 中的值就可以了。

停机/运行参数部分：

参数地址	参数描述	参数地址	参数描述
1000	*通信设定值（十进制）-10000~10000	1011	PID 反馈
1001	运行频率	1012	PLC 步骤
1002	母线电压	1013	PULSE 输入脉冲频率 单位：0.01kHz
1003	输出电压	1014	反馈速度
1004	输出电流	1015	剩余运行时间
1005	输出功率	1016	AI1 校正前电压
1006	输出转矩	1017	AI2 校正前电压
1007	运行速度	1018	AI3 校正前电压
1008	DI 输入标志	1019	线速度
1009	DO 输出标志	101A	当前上电时间
100A	AI1 电压	101B	当前运行时间
100B	AI2 电压	101C	PULSE 输入脉冲频率，单位 1Hz
100C	AI3 电压	101D	通讯设定值
100D	计数值输入	101E	实际反馈速度
100E	长度值输入	101F	主频率 X 显示
100F	负载速度	1020	辅频率 Y 显示
1010	PID 设置		

注意：

通信设定值是相对值的百分数，10000 对应 100.00%，-10000 对应-100.00%。

控制命令输入到变频器：（只写）

命令地址	命令功能
2000	0001：正转运行
	0002：反转运行
	0003：正转点动
	0004：反转点动
	0005：自由停机
	0006：减速停机
	0007：故障复位

读取变频器状态：（只读）

命令地址	命令功能
3000	0001: 正转运行
	0002: 反转运行
	0003: 停机

参数锁定密码校验：（如果返回为 8888H，即表示密码校验通过）

密码地址	输入密码的内容
1F00	*****

数字输出端子控制：（只写）

命令地址	
2001	BIT0: DO1 输出控制 BIT1: DO2 输出控制 BIT2: RELAY1 输出控制 BIT3: RELAY2 输出控制 BIT4: FMR 输出控制

模拟输出 AO1 控制：（只写）

命令地址	命令内容
2002	0~7FFF 表示 0%~100%

模拟输出 AO2 控制：（只写）

命令地址	命令内容
2003	0~7FFF 表示 0%~100%

脉冲（PULSE）输出控制：（只写）

命令地址	命令内容
2004	0~7FFF 表示 0%~100%

变频器故障描述：

变频器故障地址	变频器故障信息	
8000	0000: 无故障	0015: 参数读写异常
	0001: 保留	0016: 变频器硬件故障
	0002: 加速过电流	0017: 电机对地短路故障
	0003: 减速过电流	0018: 保留
	0004: 恒速过电流	0019: 保留
	0005: 加速过电压	001A: 运行时间到达
	0006: 减速过电压	001B: 用户自定义故障 1
	0007: 恒速过电压	001C: 用户自定义故障 2
	0008: 缓冲电阻过载故障	001D: 上电时间到达
	0009: 欠压故障	001E: 掉载
	000A: 变频器过载	001F: 运行时 PID 反馈丢失
	000B: 电机过载	0028: 快速限流超时故障
	000C: 输入缺相	0029: 运行时切换电机故障
	000D: 输出缺相	002A: 速度偏差过大
	000E: 模块过热	002B: 电机超速度

000F: 外部故障	002D: 电机过温
0010: 通讯异常	005A: 编码器线数设定错误
0011: 接触器异常	005B: 未接编码器
0012: 电流检测故障	005C: 初始位置错误
0013: 电机调谐故障	005E: 速度反馈错误
0014: 编码器/PG 卡故障	

FA 组通讯参数说明

FA-00	通讯类型选择	出厂值	0
	设定范围	0: Modbus	

目前仅支持串口实现 Modbus。

FA-01	波特率设置	出厂值	5
	设定范围	0: 300BPS 1: 600BPS 2: 1200BPS 3: 2400BPS	4: 4800BPS 5: 9600BPS 6: 19200BPS 7: 38400BPS

此参数用来设定上位机与变频器之间的数据传输速率。注意，上位机与变频器设定的波特率必须一致，否则，通讯无法进行。波特率越大，通讯速度越快。

FA-02	Modbus 数据格式	出厂值	0
	设定范围	0: 无校验: 数据格式<8,N,2> 1: 偶检验: 数据格式<8,E,1> 2: 奇校验: 数据格式<8,O,1> 3: 无校验: 数据格式<8,N,1>	

上位机与变频器设定的数据格式必须一致，否则，通讯无法进行。

FA-03	广播地址	出厂值	1
	设定范围	0~247, 0 为广播地址	

当本机地址设定为 0 时，即为广播地址，实现上位机广播功能。

本机地址具有唯一性（除广播地址外），这是实现上位机与变频器点对点通讯的基础。

FA-04	Modbus 应答时间	出厂值	2ms
	设定范围	0~20ms（仅 Modbus 有效）	

应答延时：是指变频器数据接受结束到向上位机发送数据的中间间隔时间。如果应答延时小于系统处理时间，则应答延时以系统处理时间为准，如应答延时长于系统处理时间，则系统处理完数据后，要延迟等待，直到应答延迟时间到，才往上位机发送数据。

FA-05	串口通讯超时时间	出厂值	0.0 s
	设定范围	0.0 s（无效）; 0.1~60.0s	

当该功能码设置为 0.0 s 时，通讯超时时间参数无效。

当该功能码设置成有效值时，如果一次通讯与下一次通讯的间隔时间超出通讯超时时间，系统将报通讯故障错误（Err.16）。通常情况下，都将其设置成无效。如果在连续通讯的系统中，设置此参数，可以监视通讯状况。

FA-06	Modbus 数据传送格式选择		出厂值	1
	设定范围	个位	Modbus	
		0	非标准的 Modbus 协议	
1	标准的 Modbus 协议			

FA-06=1: 选择标准的 Modbus 协议。

FA-06=0: 读命令时, 从机返回字节数比标准的 Modbus 协议多一个字节, 具体参见本协议“通讯资料结构”部分。

FA-07	通讯读取电流分辨率		出厂值	0
	设定范围	0	0.01A	
		1	0.1A	

用来确定通讯读取输出电流时, 电流值的输出单位。