

## RF800 Modbus 通讯协议

RF800 系列变频器提供 RS232/RS485 通信接口，并支持 Modbus 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。

### 一、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 RS232/RS485 总线的“单主多从”PC/PLC 控制网络。

总线结构

#### （1）接口方式

RS232/RS485 硬件接口

#### （2）传输方式

异步串行，半双工传输方式。在同一时刻主机和从机只能有一个发送数据而另一个只能接收数据。数据在串行异步通信过程中，是以报文的形式，一帧一帧发送。

#### （3）拓扑结构

单主机多从机系统。从机地址的设定范围为 1~247，0 为广播通信地址。网络中的从机地址必须是唯一的。

### 二、协议说明

RF800 系列变频器通信协议是一种异步串行的主从 Modbus 通信协议，网络中只有一个设备（主机）能够建立协议（称为“查询/命令”）。其他设备（从机）只能通过提供数据响应主机的“查询/命令”，或根据主机的“查询/命令”做出相应的动作。主机在此是指个人计算机（PC），工业控制设备或可编程逻辑控制器（PLC）等，从机是指 RF800 变频器。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。对于单独访问的主机“查询/命令”，从机都要返回一个信息（称为响应），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 RF800 系列变频器的 Modbus 协议通讯数据格式如下：使用 RTU 模式，消息发送至少要以 3.5 个字符时间的停顿间隔开始。在网络波特率下多样的字符时间，这是最容易实现的。传输的第一个域是设备地址，可以使用的传输字符是十六进制的 0..9, A..F。网络设备不断侦测网络总线，包括停顿间隔时间内。当第一个域（地址域）接收到，每个设备都进行解码以判断是否是发往自己的。在最后一个传输字符之后，一个至少 3.5 个字符时间的停顿标定了消息的结束，一个新的消息可在此停顿后开始。

整个消息帧必须作为一连续的流传输。如果在帧完成之前有超过 1.5 个字符时间的停顿时间，接收设备将刷新不完整的消息并假定下一字节是一个新消息的地址域。同样地，如果一个新消息在小于 3.5 个字符时间内接着前个消息开始，接收的设备将认为它是前一消息的延续。这将导致一个错误，因为在最后的 CRC 域的值不可能是正确的。

RTU 帧格式：

|                 |                               |
|-----------------|-------------------------------|
| 帧头 START        | 3.5 个字符时间                     |
| 从机地址 ADR        | 通讯地址：1~247                    |
| 命令码 CRF         | 03：读从机参数；06：写从机参数             |
| 数据内容 DATA (N-1) | 资料内容：功能码参数地址，功能码参数个数，功能码参数值等。 |
| 数据内容 DATA (N-2) |                               |
| .....           |                               |
| 数据内容 DATA0      |                               |
| CRC CHK 高位      | 检测值：CRC 值。                    |
| CRC CHK 低位      |                               |
| END             | 3.5 个字符时间                     |

CRF（命令指令）及 DATA（资料字描述）

命令码：03H，读取 N 个字（Word）（最多可以读取 12 个字）例如：从机地址为 01 的变频器的起始地址 F002 连续读取连续的 2 个值。

主机命令信息

|            |                  |
|------------|------------------|
| ADR        | 01H              |
| CRF        | 03H              |
| 起始地址高位     | F0H              |
| 起始地址低位     | 02H              |
| 寄存器个数高位    | 00H              |
| 寄存器个数低位    | 02H              |
| CRC CHK 低位 | 有待计算其 CRC CHK 的值 |
| CRC CHK 高位 |                  |

从机回应信息

FD-05 设为 0 时：

|             |                  |
|-------------|------------------|
| ADR         | 01H              |
| CRF         | 03H              |
| 字节个数高位      | 00H              |
| 字节个数低位      | 04H              |
| 资料 F002H 高位 | 00H              |
| 资料 F002H 低位 | 00H              |
| 资料 F003H 高位 | 00H              |
| 资料 F003H 高位 | 01H              |
| CRC CHK 低位  | 有待计算其 CRC CHK 的值 |
| CRC CHK 高位  |                  |

FD-05 设为 1 时

|      |     |
|------|-----|
| ADR  | 01H |
| CRF  | 03H |
| 字节个数 | 04H |

|             |                  |
|-------------|------------------|
| 资料 F002H 高位 | 00H              |
| 资料 F002H 低位 | 00H              |
| 资料 F003H 高位 | 00H              |
| 资料 F003H 低位 | 01H              |
| CRC CHK 低位  | 有待计算其 CRC CHK 的值 |
| CRC CHK 高位  |                  |

命令码：06H 写一个字（Word）例如：将 5000（1388H）写到从机地址 02H 变频器的 F00AH 地址处。

#### 主机命令信息

|            |                 |
|------------|-----------------|
| ADR        | 02H             |
| CRF        | 06H             |
| 资料地址高位     | F0H             |
| 资料地址低位     | 0AH             |
| 资料内容高位     | 13H             |
| 资料内容低位     | 88H             |
| CRC CHK 低位 | 有待计算 CRC CHK 的值 |
| CRC CHK 高位 |                 |

#### 从机回应信息

|            |                 |
|------------|-----------------|
| ADR        | 02H             |
| CRF        | 06H             |
| 资料地址高位     | F0H             |
| 资料地址低位     | 0AH             |
| 资料内容高位     | 13H             |
| 资料内容低位     | 88H             |
| CRC CHK 低位 | 有待计算 CRC CHK 的值 |
| CRC CHK 高位 |                 |

校验方式——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

该部分是通信的内容，用于控制变频器的运行，变频器状态及相关参数设定。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）。

### 三、功能码参数地址标示规则

以功能码组号和标号为参数地址表示规则：

高位字节：F0~FF（F组）、A0~AF（A组）、70~7F（U组）

低位字节：00~FF

如：F3-12，地址表示为F30C；

注意：

FF组：既不可读取参数，也不可更改参数；

U组：只可读取，不可更改参数。

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。另外，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。

如果为 F 组参数，要实现该功能，只要把该功能码地址的高位 F 变成 0 就可以实现。

如果为 A 组参数，要实现该功能，只要把该功能码地址的高位 A 变成 4 就可以实现。

相应功能码地址表示如下：

高位字节：00~0F（F 组）、40~4F（A 组）

低位字节：00~FF

如：

功能码 F3-12 不存储到 EEPROM 中，地址表示为 030C；

功能码 A0-05 不存储到 EEPROM 中，地址表示为 4005；该地址表示只能做写 RAM，不能做读的动作，读时，为无效地址。

对于所有参数，也可以使用命令码 07H 来实现该功能。

停机/运行参数部分：

| 参数地址  | 参数描述                      |
|-------|---------------------------|
| 1000H | *通信设定值（-10000~10000）（十进制） |
| 1001H | 运行频率                      |
| 1002H | 母线电压                      |
| 1003H | 输出电压                      |
| 1004H | 输出电流                      |
| 1005H | 输出功率                      |
| 1006H | 输出转矩                      |
| 1007H | 运行速度                      |
| 1008H | DI 输入标志                   |
| 1009H | DO 输出标志                   |
| 100AH | AI1 电压                    |
| 100BH | AI2 电压                    |
| 100CH | AI3 电压                    |
| 100DH | 计数值输入                     |
| 100EH | 长度值输入                     |
| 100FH | 负载速度                      |
| 1010H | PID 设置                    |
| 1011H | PID 反馈                    |
| 1012H | PLC 步骤                    |
| 1013H | PULSE 输入脉冲频率，单位 0.01kHz   |
| 1014H | 反馈速度，单位 0.1Hz             |
| 1015H | 剩余运行时间                    |
| 1016H | AI1 校正前电压                 |
| 1017H | AI2 校正前电压                 |

|       |                      |
|-------|----------------------|
| 1018H | A13 校正前电压            |
| 1019H | 线速度                  |
| 101AH | 当前上电时间               |
| 101BH | 当前运行时间               |
| 101CH | PULSE 输入脉冲频率, 单位 1Hz |
| 101DH | 通讯设定值                |
| 101EH | 实际反馈速度               |
| 101FH | 主频率 X 显示             |
| 1020H | 辅频率 Y 显示             |

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%。对频率量纲的数据, 该百分比是相对最大频率 (F0-10) 的百分数; 对转矩量纲的数据, 该百分比是 F2-10、A2-48、A3-48、A4-48 (转矩上限数字设定, 分别对应第一、二、三、四电机)。

控制命令输入到变频器: (只写)

| 命令字地址 | 命令功能       |
|-------|------------|
| 2000H | 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)

| 状态字地址 | 状态字功能      |
|-------|------------|
| 3000H | 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 |
|-------|---------|
| 1F00H | *****   |

数字输出端子控制: (只写)

| 命令地址  | 命令内容              |
|-------|-------------------|
| 2001H | BIT0: DO1 输出控制    |
|       | BIT1: DO2 输出控制    |
|       | BIT2: RELAY1 输出控制 |
|       | BIT3: RELAY2 输出控制 |

模拟输出 AO1 控制: (只写)

| 命令地址  | 命令内容              |
|-------|-------------------|
| 2002H | 0~7FFF 表示 0%~100% |

模拟输出 AO2 控制：（只写）

| 命令地址  | 命令内容              |
|-------|-------------------|
| 2003H | 0~7FFF 表示 0%~100% |

脉冲（PULSE）输出控制：（只写）

| 命令地址  | 命令内容              |
|-------|-------------------|
| 2004H | 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        |
|------------------|----------------|
| 8000H            | 0000: 无故障      |
|                  | 0001: 保留       |
|                  | 0002: 加速过电流    |
|                  | 0003: 减速过电流    |
|                  | 0004: 恒速过电流    |
|                  | 0005: 加速过电压    |
|                  | 0006: 减速过电压    |
|                  | 0007: 恒速过电压    |
|                  | 0008: 缓冲电阻过载故障 |
|                  | 0009: 欠压故障     |
|                  | 000A: 变频器过载    |
|                  | 000B: 电机过载     |
|                  | 000C: 输入缺相     |
|                  | 000D: 输出缺相     |
|                  | 000E: 模块过热     |
|                  | 000F: 外部故障     |
|                  | 0010: 通讯异常     |
| 0011: 接触器异常      |                |
| 0012: 电流检测故障     |                |
| 0013: 电机调谐故障     |                |
| 0014: 编码器/PG 卡故障 |                |
| 0015: 参数读写异常     |                |
| 0016: 变频器硬件故障    |                |
| 0017: 电机对地短路故障   |                |

|  |   |
|--|---|
|  | <p>0018: 保留</p> <p>0019: 保留</p> <p>001A: 运行时间到达</p> <p>001B: 用户自定义故障 1</p> <p>001C: 用户自定义故障 2</p> <p>001D: 上电时间到达</p> <p>001E: 掉载</p> <p>001F: 运行时 PID 反馈丢失</p> <p>0028: 快速限流超时故障</p> <p>0029: 运行时切换电机故障</p> <p>002A: 速度偏差过大</p> <p>002B: 电机超速度</p> <p>002D: 电机过温</p> <p>005A: 编码器线数设定错误</p> <p>005B: 未接编码器</p> <p>005C: 初始位置错误</p> <p>005E: 速度反馈错误</p> |
|--|---|

通讯故障信息描述数据（故障代码）:

| 通讯故障地址 | 故障功能描述   |
|--------|--|
| 8001H  | <p>0000: 无故障</p> <p>0001: 密码错误</p> <p>0002: 命令码错误</p> <p>0003: CRC 校验错误</p> <p>0004: 无效地址</p> <p>0005: 无效参数</p> <p>0006: 参数更改无效</p> <p>0007: 系统被锁定</p> <p>0008: 正在 EEPROM 操作</p> |

#### 四、FD 组通讯参数说明

|       |     |     |      |
|-------|-----|-----|------|
| Fd-00 | 波特率 | 出厂值 | 6005 |
|-------|-----|-----|------|



|  |      |   |
|--|------|---|
|  | 设定范围 | 单位: MODBUS 波特率<br>0: 300BPS<br>1: 600BPS<br>2: 1200BPS<br>3: 2400BPS<br>4: 4800BPS<br>5: 9600BPS<br>6: 19200BPS<br>7: 38400BPS<br>8: 57600BPS<br>9: 115200BPS |
|--|------|---|

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。

|       |      |  |   |
|-------|------|--|---|
| Fd-01 | 数据格式 | 出厂值  | 0 |
|       | 设定范围 | 0: 无校验: 数据格式<8, N, 2><br>1: 偶校验: 数据格式<8, E, 1><br>2: 奇校验: 数据格式<8, O, 1><br>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。

|       |      |                |   |
|-------|------|----------------|---|
| Fd-02 | 本机地址 | 出厂值            | 1 |
|       | 设定范围 | 1~247, 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。

|       |      |        |     |
|-------|------|--------|-----|
| Fd-03 | 应答延时 | 出厂值    | 2ms |
|       | 设定范围 | 0~20ms |     |

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。

|       |        |                         |       |
|-------|--------|-------------------------|-------|
| Fd-04 | 通讯超时时间 | 出厂值                     | 0.0 s |
|       | 设定范围   | 0.0 s (无效)<br>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 (Err16)。通常情况下，都将其设置成无效。如果在连续通讯的系统中，设置该参数，可以监视通讯状况。

|       |        |                                       |   |
|-------|--------|---------------------------------------|---|
| Fd-05 | 通讯协议选择 | 出厂值                                   | 0 |
|       | 设定范围   | 0: 非标准的 Modbus 协议<br>1: 标准的 Modbus 协议 |   |

FD-05=1: 选择标准的 Modbus 协议。

FD-05=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“5 通讯资料结构”部分。

|       |           |                     |   |
|-------|-----------|---------------------|---|
| Fd-06 | 通讯读取电流分辨率 | 出厂值                 | 0 |
|       | 设定范围      | 0: 0.01A<br>1: 0.1A |   |

用来确定通讯读取输出电流时，电流值的输出单位。