AMB100 通讯协议

AMB100 系列变频器，提供 RS485 通信接口，采用国际标准的 ModBus 通讯协议进行的主从通讯。用户可通过 PC/PLC、控制上位机等实现集中控制（设定变频器控制命令、运行频率、相关功能码参数的修改，变频器工作状态及故障信息的监控等），以适应特定的应用要求。

一、协议内容

该 Modbus 串行通信协议定义了串行通信中异步传输的帧内容及使用格式。其中包括：主机轮询及广播帧、从机应答帧的格式；主机组织的帧内容包括：从机地址(或广播地址)、执行命令、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。如果从机在接收帧时发生错误，或不能完成主机要求的动作，它将组织一个故障帧作为响应反馈给主机。

二、 应用方式

AMB100 系列变频器可接入具备 RS485 总线的“单主多从”控制网络。

三、总线结构

1.接口方式

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。网络中的每个从机的地址都具有唯一性。这是保证 ModBus 串行通讯的基础。

四、协议说明

AMB100 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”）。其它设备（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 AMB100 系列变频器或其它具有相同通讯协议的控制设备。主机既能对某个从机单独进行通信，也能对所有从机发布广播信息。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，从机无需反馈响应信息给主机。

五、 通讯帧结构

AMB100 系列变频器的 **ModBus** 协议通信数据格式分为 **RTU**（远程终端单元）模式和 **ASCII**（**American Standard Code for Information International Interchange**）模式两种。

RTU 模式中，每个字节的格式如下：

编码系统：**8** 位二进制，每个 **8** 位的帧域中，包含两个十六进制字符，十六进制 **0**～**9**、**A**～**F**。

ASCII 模式中，每个字节的格式如下：

编码系统：通讯协议属于 **16** 进制，**ASCII** 的信息字符意义：“**0**”…“**9**”，“**A**”…“**F**”每个 **16** 进制都用对应字符的 **ASCII** 信息表示。

字符	‘0’	‘1’	‘2’	‘3’	‘4’	‘5’
ASCII CODE	0x30	0x31	0x32	0x33	0x34	0x35
字符	‘6’	‘7’	‘8’	‘9’	‘A’	‘B’
ASCII CODE	0x36	0x37	0x38	0x39	0x41	0x42
字符	‘C’	‘D’	‘E’	‘F’		

ASCII CODE	0x43	0x44	0x45	0x46

数据格式：起始位、7/8 个数据位、校验位和停止位。
数据格式的描述如下表：

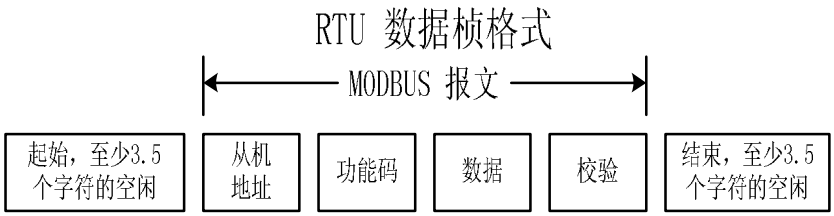
11-bit 字符帧：

起始位	BIT1	BIT2	BIT3	BIT4	BIT5	BIT6	BIT7	BIT8	校验位	停止位

10-bit 字符帧：

起始位	BIT1	BIT2	BIT3	BIT4	BIT5	BIT6	BIT7	校验位	停止位

在 RTU 模式中，新帧总是以至少 3.5 个字节的传输时间静默作为开始。在以波特率计算传输速率的网络上，3.5 个字节的传输时间可以轻松把握。紧接着传输的数据域依次为：从机地址、操作命令码、数据和 CRC 校验字，每个域传输字节都是十六进制的 0...9，A...F。网络设备始终监视着通讯总线的活动。当接收到第一个域（地址信息），每个网络设备都对该字节进行确认。随着最后一个字节的传输完成，又有一段类似的 3.5 个字节的传输时间间隔，用来表识本帧的结束，在此以后，将开始一个新帧的传送。

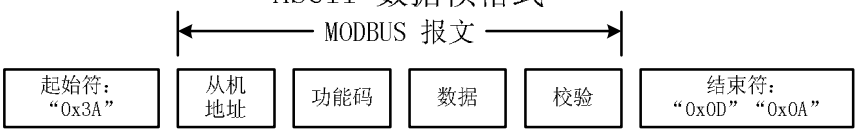


一个帧的信息必须以一个连续的数据流进行传输，如果整个帧传输结束前有超过 1.5 个字节以上的间隔时间，接收设备将清除这些不完整的信息，并错误认为随后一个字节是新一帧的地址域部分，同样的，如果一个新帧的开始与前一个帧的间隔时间小于 3.5 个字节时间，接收设备将认为它是前一帧的继续，由于帧的错乱，最终 CRC 校验值不正确，导致通讯故障。RTU 帧的标准结构：

帧头START	T1-T2-T3-T4（3.5个字节的传输时间）
从机地址域ADDR	通讯地址：0～247（十进制）（0为广播地址）
功能域CMD	03H：读从机参数； 06H：写从机参数
数据域 DATA（N-1） … DATA（0）	2*N个字节的数据，该部分为通讯的主要内容，也是通讯中，数据交换的核心。
CRC CHK 低位	检测值：CRC校验值（16BIT）
CRC CHK 高位	
帧尾END	T1-T2-T3-T4（3.5个字节的传输时间）

在 ASCII 模式中，帧头为“：”（“0x3A”）,帧尾缺省为“CRLF”（“0x0D”“0x0A”）。在 ASCII 方式下，除了帧头和帧尾之外，其余的数据字节全部以 ASCII 码方式发送，先发送高 4 位位元组，然后发送低 4 位位元组。ASCII 方式下数据为 8 位长度。对于‘A’～‘F’，采用其大写字母的 ASCII 码。此时数据采用 LRC 校验，校验涵盖从从机地址到数据的信息部分。校验和等于所有参与校验数据的字符和(舍弃进位位)的补码。

ASCII 数据桢格式



ASCII 帧的标准结构：

START	**‘:’（0x3A）**
Address Hi	通讯地址：**8-bit** 地址由**2**个**ASCII**码组合
Address Lo	
Function Hi	功能码：**8-bit** 地址由**2**个**ASCII**码组合
Function Lo	
DATA（N-1） … **DATA（0）**	数据内容：**nx8-bit** 数据内容由**2n**个**ASCII**码组合 **n<=16**，最大**32**个**ASCII**码
LRC CHK Hi	**LRC**检查码：**8-bit** 检验码由**2**个**ASCII**码组合
LRC CHK Lo	
END Hi	结束符：**END Hi=CR（0x0D），END Lo=LF（0x0A）**
END Lo	

六、命令码及通讯数据描述

1.命令码：03H（0000 0011），读取 N 个字（Word）(最多可以连续读取 16 个字)

例如：从机地址为 01H 的变频器，内存启始地址为 0004，读取连续 2 个字，则该帧的结构描述如下：

RTU 主机命令信息

START	**T1-T2-T3-T4**
ADDR	**01H**
CMD	**03H**
启始地址高位	**00H**
启始地址低位	**04H**
数据个数高位	**00H**
数据个数低位	**02H**
CRC CHK 低位	**85H**
CRC CHK 高位	**CAH**
END	**T1-T2-T3-T4**

RTU 从机回应信息

START	**T1-T2-T3-T4**
ADDR	**01H**
CMD	**03H**
字节个数	**04H**
数据地址**0004H**高位	**13H**
数据地址**0004H**低位	**88H**
数据地址**0005H**高位	**13H**
数据地址**0005H**低位	**88H**
CRC CHK 低位	**73H**
CRC CHK 高位	**CBH**
END	**T1-T2-T3-T4**

ASCII 主机命令信息

START	**‘:’**

ADDR	‘0’
	‘1’
CMD	‘0’
	‘3’
启始地址高位	‘0’
	‘0’
启始地址低位	‘0’
	‘4’
数据个数高位	‘0’
	‘0’
数据个数低位	‘0’
	‘2’
LRC CHK Hi	‘F’
LRC CHK Lo	‘6’
END Hi	CR
END Lo	LF

ASCII 从机回应信息

START	‘:’
ADDR	‘0’
	‘1’
CMD	‘0’
	‘3’
字节个数	‘0’
	‘4’
数据地址 0004H高位	‘1’
	‘3’
数据地址 0004H低位	‘8’
	‘8’
数据地址 0005H高位	‘1’
	‘3’
数据地址 0005H低位	‘8’
	‘8’
LRC CHK Hi	‘C’
LRC CHK Lo	‘2’
END Hi	CR
END Lo	LF

2.命令码：06H（0000 0110），写一个字(Word)

例如：将 5000（1388H）写到从机地址 02H 变频器的 0008H 地址处。则该帧的结构描述如下：

RTU 主机命令信息

START	T1-T2-T3-T4
ADDR	02H
CMD	06H
写数据地址高位	00H
写数据地址低位	05H
数据内容高位	13H
数据内容低位	88H

CRC CHK 低位	**94H**
CRC CHK 高位	**AEH**
END	**T1-T2-T3-T4**

RTU 从机回应信息

START	**T1-T2-T3-T4**
ADDR	**02H**
CMD	**06H**
写数据地址高位	**00H**
写数据地址低位	**05H**
数据内容高位	**13H**
数据内容低位	**88H**
CRC CHK 低位	**94H**
CRC CHK 高位	**AEH**
END	**T1-T2-T3-T4**

ASCII 主机命令信息

START	**‘:’**
ADDR	**‘0’**
	‘2’
CMD	**‘0’**
	‘6’
写数据地址高位	**‘0’**
	‘0’
写数据地址低位	**‘0’**
	‘5’
数据内容高位	**‘1’**
	‘3’
数据内容低位	**‘8’**
	‘8’
LRC CHK Hi	**‘5’**
LRC CHK Lo	**‘8’**
END Hi	**CR**
END Lo	**LF**

ASCII 从机回应信息

START	**‘:’**
ADDR	**‘0’**
	‘2’
CMD	**‘0’**
	‘6’
写数据地址高位	**‘0’**
	‘0’
写数据地址低位	**‘0’**
	‘5’
数据内容高位	**‘1’**
	‘3’
数据内容低位	**‘8’**
	‘8’

LRC CHK Hi	‘5’
LRC CHK Lo	‘8’
END Hi	CR
END Lo	LF

3.命令码：08H（0000 1000），诊断功能
子功能码的意义：

子功能码	说明
0000	返回询问讯息数据

例如：对驱动器地址 01H 做回路侦测询问讯息字串内容与回应讯息字串内容相同，其格式如下所示：

RTU 主机命令信息

START	T1-T2-T3-T4
ADDR	01H
CMD	08H
子功能码高位	00H
子功能码低位	00H
数据内容高位	12H
数据内容低位	ABH
CRC CHK 低位	ADH
CRC CHK 高位	14H
END	T1-T2-T3-T4

RTU 从机回应信息

START	T1-T2-T3-T4
ADDR	01H
CMD	08H
子功能码高位	00H
子功能码低位	00H
数据内容高位	12H
数据内容低位	ABH
CRC CHK 低位	ADH
CRC CHK 高位	14H
END	T1-T2-T3-T4

ASCII 主机命令信息

START	‘:’
ADDR	‘0’
	‘1’
CMD	‘0’
	‘8’
子功能码高位	‘0’
	‘0’
子功能码低位	‘0’
	‘0’
数据内容高位	‘1’
	‘2’
数据内容低位	‘A’

	‘B’
LRC CHK Hi	‘3’
LRC CHK Lo	‘A’
END Hi	CR
END Lo	LF

ASCII 从机回应信息

START	‘:’
ADDR	‘0’
	‘1’
CMD	‘0’
	‘8’
子功能码高位	‘0’
	‘0’
子功能码低位	‘0’
	‘0’
数据内容高位	‘1’
	‘2’
数据内容低位	‘A’
	‘B’
LRC CHK Hi	‘3’
LRC CHK Lo	‘A’
END Hi	CR
END Lo	LF

4.通讯帧错误校验方式

帧的错误校验方式主要包括两个部分的校验，即字节的位校验（奇/偶校验）和帧的整个数据校验（CRC 校验或 LRC 校验）。

4.1 字节位校验

用户可以根据需要选择不同的位校验方式，也可以选择无校验，这将影响每个字节的校验位设置。

偶校验的含义：在数据传输前附加一位偶校验位，用来表示传输的数据中**"1"**的个数是奇数还是偶数，为偶数时，校验位置为**"0"**，否则置为**"1"**，用以保持数据的奇偶性不变。

奇校验的含义：在数据传输前附加一位奇校验位，用来表示传输的数据中**"1"**的个数是奇数还是偶数，为奇数时，校验位置为**"0"**，否则置为**"1"**，用以保持数据的奇偶性不变。

例如，需要传输**"11001110"**，数据中含 **5** 个**"1"**，如果用偶校验，其偶校验位为**"1"**，如果用奇校验，其奇校验位为**"0"**，传输数据时，奇偶校验位经过计算放在帧的校验位的位置，接收设备也要进行奇偶校验，如果发现接受的数据的奇偶性与预置的不一致，就认为通讯发生了错误。

4.2 CRC 校验方式**---CRC(Cyclical Redundancy check)**：

使用 **RTU** 帧格式，帧包括了基于 **CRC** 方法计算的帧错误检测域。**CRC** 域检测了整个帧的内容。**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帧中。接收设备重新计算收到帧的 **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帧中连续的 **6** 个以上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，是帧中所有的

字节都执行之后的 CRC 值。

CRC 的这种计算方法，采用的是国际标准的 CRC 校验法则，用户在编辑 CRC 算法时，可以参考相关标准的 CRC 算法，编写出真正符合要求的 CRC 计算程序。

现在提供一个 CRC 计算的简单函数给用户参考（用 C 语言编程）：

```
unsigned int crc_cal_value(unsigned char *data_value,unsigned char data_length)
{
    int i;
    unsigned int crc_value=0xffff;  while(data_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);
}
```

在阶梯逻辑中，CKSM 根据帧内容计算 CRC 值，采用查表法计算，这种方法程序简单，运算速度快，但程序所占用 ROM 空间较大，对程序空间有要求的场合，请谨慎使用。

4.3 ASCII 模式的校验（LRC check）

校验码（LRC check）由 Address 到 Data Content 结果加起来的值，例如上面 1.6.2 通讯信息的的校验码：0x02+0x06+0x00+0x08+
0x13+0x88=0xAB，然后取 2 的补码=0x55。

现在提供一个 LRC 计算和简单函数给用户参考（用 C 语言编程）：

```
Static unsigned char
LRC(auchMsg,usDataLen)
unsigned char *auchMsg;
unsigned short usDataLen;
{
  unsigned char uchLRC=0;
  while(usDataLen--)
    uchLRC+=*auchMsg++;
  return((unsigned char)(～((char)uchLRC)));
}
```

5.通信数据地址的定义

该部分是通信数据的地址定义，用于控制变频器的运行、获取变频器状态信息及变频器相关功能参数设定等。

(1)功能码参数地址表示规则

以功能码序号为参数对应寄存器地址，但要转换成十六进制，如 F5.05 的序号为 76，则用十六进制表示该功能码地址为 004CH。

高、低字节的范围分别为：高位字节——00～01；低位字节——00～FF。

注意：FE 组：为厂家设定参数，既不可读取该组参数，也不可更改该组参数；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，还要注意参数的设定范围，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，对于用户而言，有些功能码在通讯的模式下，无需存储，只需更改片内 RAM 中的值就可以满足使用要求。要实现该功能，只要把对应的功能码地址最高位由 0 变成 1 就可以实现。如：功能码 F0.01 不存储到 EEPROM 中，只修改 RAM 中的值，可将地址设置为 8007；该地址只能用作写片内 RAM 时使用，不能用做读的功能，如做读为无效地址。

（**2**）其他功能的地址说明：

功能说明	地址定义	数据意义说明	R/W 特性
通讯控制命令	**1000H**	**0001H**：正转运行	**W/R**
		0002H：反转运行	
		0003H：正转点动	
		0004H：反转点动	
		0005H：停机	
		0006H：自由停机（紧急停机）	
		0007H：故障复位	
		0008H：点动停止	
变频器状态	**1001H**	**0001H**：正转运行中	**R**
		0002H：反转运行中	
		0003H：变频器待机中	
		0004H：故障中	
通讯设定值地址	**2000H**	通信设定值范围（**-10000**～**10000**）**注意：**通信设定值是相对值的百分数（**-100.00%**～**100.00%**），可做通信写操作。当作为频率源设定时，相对的是最大频率（**P0.07**）的百分数；当作为转矩给定时，相对的是转矩上限（**P3.14**）的百分数。当作为 **PID** 给定或者反馈时，相对的是 **PID** 的百分数。	**W/R**
虚拟端子输入功能设定	**2001H**	保留	**W/R**
运行/停机参数地址说明	**3000H**	运行速度	**R**
	3001H	设定速度	**R**
	3002H	母线电压	**R**
	3003H	输出电压	**R**
	3004H	输出电流	**R**
	3005H	运行转速	**R**
	3006H	输出功率	**R**
	3007H	输出转矩	**R**
	3008H	**PID** 给定值	**R**
	3009H	**PID** 反馈值	**R**
	300AH	端子输入标志状态	**R**
	300BH	端子输出标志状态	**R**
	300CH	模拟量 **AI1** 值	**R**
	300DH	模拟量 **AI2** 值	**R**
	300EH	模拟量 **AI3** 值	**R**

功能说明	地址定义	数据意义说明	R/W 特性
	300FH	模拟量 AI4 值	R
	3010H	高速脉冲频率（HDI1）	R
	3011H	高速脉冲频率（HDI2）	R
	3012H	多段速及 PLC 当前段数	R
	3013H	长度值	R
	3014H	外部计数器输入值	R
	3015H	转矩方向（0：正向，1：反向）	R
	3016H	设备代码	R
参数锁定密码校验地址	4000H	****	
参数锁定密码命令地址	4001H	55AAH	W
变频器故障地址	5000H	故障信息代码与功能码菜单中故障类型的序号一致，只不过该处给上位机返回的是十六进制的数据，而不是故障字符。	R

注意：从 5000H 中读取的数字与实际故障对照表如下：

数字	故障类型
0x00	无故障
0x01	逆变单元保护（E.SC）
0x02	加速过电流（E.OCA）
0x03	减速过电流（E.OCd）
0x04	恒速过电流（E.OCC）
0x05	加速过电压（E.OVA）
0x06	减速过电压（E.OVd）
0x07	恒速过电压（E.OUC）
0x08	母线欠压故障（E.LV）
0x09	电机过载（E.OL1）
0x0A	变频器过载（E.OL2）
0x0B	输出侧缺相（E.SPO）
0x0C	整流模块过热（E.OH1）
0x0D	逆变模块过热故障（E.OH2）
0x0E	外部故障（E.EF）
0x0F	通讯故障（E.CE）
0x10	电流检测故障（E.It）
0x 11	电机自学习故障（E.tU）
0x 12	EEPROM 操作故障（E.EP）
0x 13	PID 反馈断线故障（E.PID）

从变频器中读取参数全部为 16 进制表示，且数值都为：实际值*10^{K}，其中 K 为该参数小数点后的位数。

6. 错误消息的回应

当从设备回应时，它使用功能代码域与故障地址来指示是正常回应（无误）还是有某种错误发生（称作异议回应）。对正常回应，从设备回应相应的功能代码和数据地址或子功能码。对异议回应，从设备返回一等同于正常代码的代码，但最首的位置为逻辑 1。

例如：一主设备发往从设备的消息要求读一组变频器功能码地址数据，将产生如下功能代码：

0 0 0 0 0 0 1 1 （十六进制 **03H**）

对正常回应，从设备回应同样的功能码。对异议回应，它返回：

1 0 0 0 0 0 1 1 （十六进制 **83H**）

除功能代码因异议错误作了修改外，从设备将回应一字节异常码，这定义了产生异常的原因。

主设备应用程序得到异议的回应后，典型的处理过程是重发消息，或者针对相应的故障进行命令更改。

错误代码的含义

Modbus 异常码		
代码	名称	含　义
01H	非法功能	当从上位机接收到的功能码是不允许的操作；也可能从机在错误状态中处理这种请求。
02H	非法数据地址	上位机的请求数据地址是不允许的地址；特别是，寄存器地址和传输的字节数组合是无效的。
03H	非法数据值	当接收到的数据域中包含的是不允许的值。注意：它决不意味着寄存器中被提交存储的数据项有一个应用程序期望之外的值。
06H	从属设备忙	变频器忙（**EPPROM** 正在存储中）
10H	密码错误	密码效验地址写入的密码与 **F7.00** 用户设置的密码不同
11H	校验错误	当上位机发送的帧信息中，**RTU** 格式 **CRC** 校验位或 **ASCII** 格式 **LRC** 校验位与下位机的校验计算数不同时，报校验错误信息。
12H	参数更改无效	上位机发送的参数写命令中，所发的数据在参数的范围以外或写地址当前为不可改写状态。
13H	系统被锁定	上位机进行读或写时，当设置了用户密码，又没有进行密码锁定开锁，将报系统被锁定。