Appendix 3: RS485 Communication Protocol

ZVF300H series inverter adopts the popular MODBUS communication protocol under RS485 communication control. Before using RS485 communication, inverter address, communication baud rate and data format must be manually set, and these parameters cannot be modified during the communication process.

MODBUS communication protocol uses two codes: ASCII (American Standard Code for Information Interchange) or RTU (Remote Terminal Unit). ASCII code is to convert the data to be transmitted into the corresponding ASCII before transmission, while RTU is to transmit the data directly without conversion.

ASCII encoding format:

Each Byte data is composed of two ASCII codes, for example: 0x1F, ASCII is represented by '1F', which is composed of '1' (31Hex) and 'F' (46Hex) respectively. The following is the ASCII code of 0-9, A-F.

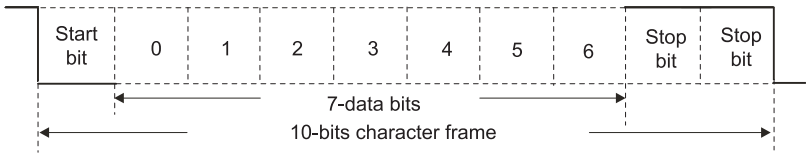
Character	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'
ASCII code	30H	31H	32H	33H	34H	35H	36H	37H
Character	'8'	'9'	'A'	'B'	'C'	'D'	'E'	'F'
ASCII code	38H	39H	41H	42H	43H	44H	45H	46H

RTU encoding format, each Byte data is composed of two 4-bit hexadecimal characters, for example: 0x1F RTU means '1FH'.

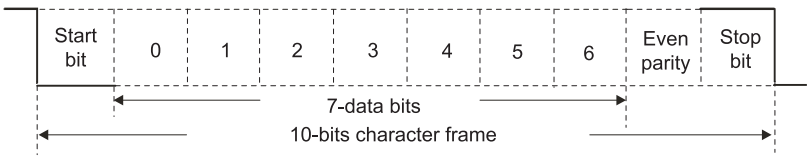
Character structure

10-bit character box (for 7-bit characters):

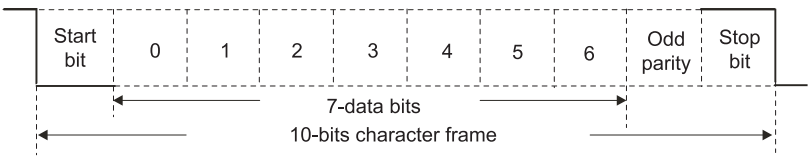
(7, N, 2)



(7, E, 1)

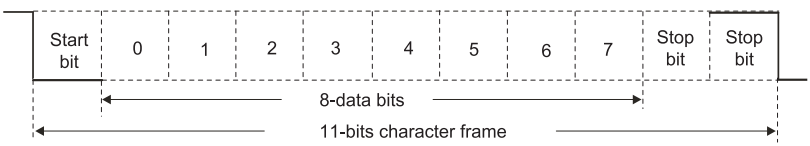


(7, O, 1)

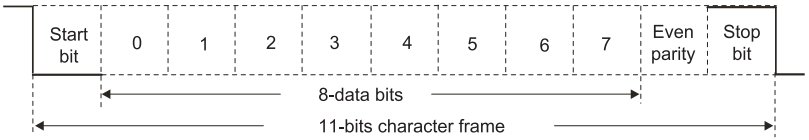


11-bit character box (for 8-bit characters):

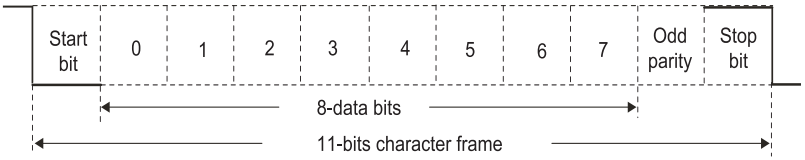
(8, N, 2)



(8, E, 1)



(8, O, 1)



Communication data structures

Communication data format box:

ASCII mode:

STX	Start character ':' (3AH)
ADR 1	Communication address:
ADR 0	8-bit address contains 2 ASCII codes
CMD 1	Command code:
CMD 0	8-bit command contains 2 ASCII codes
DATA (n-1)	Data content:
…….	n×8-bit data contains 2n ASCII codes
DATA 0	n<=16, up to 32 ASCII codes
LRC CHK 1	LRC value:
LRC CHK 0	The 8-bit check sum contains 2 ASCII codes
END 1	END character:
END 0	END1= CR (0DH), END0= LF(0AH)

RTU Mode:

START	More than 10 ms static time or 3.5 bytes transmission time
ADR	Communication address: 8-bit address
CMD	Command code: 8-bit instruction
DATA (n-1)	Data content:
…….	N×8-bit data, n<=32
DATA 0	
CRC CHK Low	CRC check value:
CRC CHK High	The 16-bit check sum consists of 2 characters of 8-bit
END	More than 10 ms static time or 3.5 bytes transmission time

ADR (Communication Address)

The range of legal communication addresses is between 1 and 247. If the communication address is 0, it means to broadcast to all the inverters. In this case, the inverter will not respond to any information to the host.

For example, communication to the inverter with address 16 decimal:

ASCII Mode: (ADR 1, ADR 0) = '1', '0' => '1'=31H, '0'=30H

RTU Mode: (ADR) = 10H

Function code (Function) and data content (Data Characters)

03: Read the data from the inverter register

06: Write a WORD to the inverter register

08: Loop detection

10: Write multiple WORDs to the inverter register

Instruction code: 03H, read the contents of the inverter register.

For example: read 2 words continuously from the address 01H and the starting address 2102H of the inverter.

RTU mode:

Command message：

Address	01H
Function	03H
Starting address	21H
	02H
Number of data (count by word)	00H
	02H
CRC CHK Low	6FH
CRC CHK High	F7H

Response message：

Address	01H
Function	03H
Number of data (count by byte)	04H
Content of data address 2102H	17H
	70H
Content of data address 2103H	00H
	00H
CRC CHK Low	FEH
CRC CHK High	5CH

ASCII Mode:

Command message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'3'
Starting address	'2'
	'1'
	'0'
	'2'
Number of data (count by word)	'0'
	'0'
	'0'
	'2'
LRC Check	'D'
	'7'
END	CR
	LF

Response message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'3'
Number of data (count by byte)	'0'
	'4'
Content of starting address 2102H	'1'
	'7'
	'7'
	'0'
Content of address 2103H	'0'
	'0'
	'0'
	'0'
LRC Check	'7'
	'1'
END	CR
	LF

Command code: 06H, write a word to the inverter register

For example: write 6000 (1770H) to address 0100H of the inverter with address 01H

RTU mode:

Command message:

Address	01H
Function	06H
Data address	01H
	00H
Data content	17H
	70H
CRC CHK Low	86H
CRC CHK High	22H

Response message:

Address	01H
Function	06H
Data address	01H
	00H
Data content	17H
	70H
CRC CHK Low	86H
CRC CHK High	22H

ASCII Code:

Command message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'6'
Data address	'0'
	'1'
	'0'
	'0'
Data content	'1'
	'7'
	'7'
	'0'
LRC Check	'7'
	'1'
END	CR
	LF

Response message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'6'
Data address	'0'
	'1'
	'0'
	'0'
Data content	'1'
	'7'
	'7'
	'0'
LRC Check	'7'
	'1'
END	CR
	LF

Command code: 08H, communication loop test

This command is used to test the communication between the host (usually PC or PLC) and the inverter is normal or not . and the inverter will return the received data content to the host intact.

RTU Mode

Command message:

Address	01H
Function	08H
Data addres	00H
	00H
Data content	17H
	70H
CRC CHK Low	EEH
CRC CHK High	1FH

Response message:

Address	01H
Function	08H
Data addres	00H
	00H
Data content	17H
	70H
CRC CHK Low	EEH
CRC CHK High	1FH

ASCII Code:

Command message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'8'
Data address	'0'
	'0'
	'0'
	'0'
Data content	'1'
	'7'
	'7'
	'0'
LRC Check	'7'
	'0'
END	CR
	LF

Response message:

STX	':'
Address	'0'
	'1'
Function	'0'
	'8'
Data address	'0'
	'0'
	'0'
	'0'
Data content	'1'
	'7'
	'7'
	'0'
LRC Check	'7'
	'0'
END	CR
	LF

Command code: 10H, write multiple words to the inverter register.
For example: write 5000 (1338H) and 4000 (0FA0H) to the 0500H and 0501H addresses of the inverter with address 01H.

RTU mode:

Command message:

Address	01H
Function	10H
Data address	05H
	00H
Number of data (count by word)	00H
	02H
Number of data (count by byte)	04H
The first data content	13H
	88H
The second data content	0FH
	A0H
CRC CHK Low	4DH
CRC CHK High	D9H

Response message:

Address	01H
Function	10H
Starting data address	05H
	00H
Number of data (count by word)	00H
	02H
CRC CHK Low	41H
CRC CHK High	04H

ASCII mode:

Command message:

STX	':'
Address	'0'
	'1'
Function	'1'
	'0'
Starting data address	'0'
	'5'
	'0'
	'0'
Number of data (count by world)	'0'
	'0'
	'0'
	'2'
Number of data (count by byte)	'0'
	'4'
The first data content	'1'
	'3'
	'8'
	'8'
The second data content	'0'
	'F'
	'A'
	'0'
LRC Check	'9'
	'A'
END	CR
	LF

Response message:

STX	':'
Address	'0'
	'1'
Function	'1'
	'0'
Data address	'0'
	'5'
	'0'
	'0'
Number of data (count by world)	'0'
	'0'
	'0'
	'2'
LRC Check	'E'
	'8'
END	CR
	LF

3.5 CHK (check sum)

ASCII mode:

ASCII mode adopt LRC (Longitudinal Redundancy Check) check sum. The LRC check sum is ADR1 to the last data content and the results is 256 as one unit . the excess parts removes , (For example , the receiving results is hexadecimal 128H only take 28H), Then calculate the two times complement and the getting result is LRC check sum.

For example, the first example of inquiry information check sum: 01H +03 H +21 H+02 H+00 H+02 H = 29H, and then take 2's complement = D7H.

RTU mode

CRC (Cyclical Redundancy Check) is calculated by the following steps:

Step 1: Load a 16–bit register (called CRC register) with FFFFH.

Step 2: The first byte of the command message and 16–bit CRC make low byte XOR arithmetic .

Step 3: Shift the CRC register one bit to the right with MSB zero filling. Extract and examine the LSB.

Step 4: If the LSB of CRC register is 0, repeat step 3, else XOR or the CRC register with the polynomial value A001H.

Step 5: Repeat step 3 and 4 until eight shifts have been performed. When this is done, a complete 8–bit byte will have been processed.

Step 6: Repeat steps 2 to 5 for the next 8–bit byte of the command message.

Continue doing this until all bytes have been processed. The final contents of the CRC register is the CRC value. When transmitting the CRC value in the message, the upper and lower bytes of the CRC value must be swapped. i.e. the lower order byte will be transmitted first.

The following is an example of CRC generation using C language. The function takes two arguments:

Unsigned char* data ←a pointer to the message

Unsigned char length ←the quantity of bytes in the message. The function returns the CRC value as a type of unsigned int.

```
Unsigned int crc_chk(unsigned char* data, unsigned char length){
  int j;
  unsigned int reg_crc=0xFFFF;
  while(length--){
    reg_crc ^= *data++;
    for(j=0;j\<8;j++){
      if(reg_crc & 0x01){  /* LSB(b0)=1 */
        reg_crc=(reg_crc>>1) ^ 0xA001;
      }else{
        reg_crc=reg_crc >>1;
      }
    }
  }
 return reg_crc;
}
```

The definition of the communication data address

The communication data address is used to control the operation of the inverter, get the state information and the rated function parameter setting.

The serial number of the function code is corresponding to the register address, but it should convert to hexadecimal number (except group parameters, as they are hexadecimal number), For example , FA.12 hexadecimal number express the function address is 0A0CH.

In addition, the EEPROM are frequently stored , will reduce the life of the EEPROM , For the users , No need to store for some function code in the mode of communication. Only change the value of RAM to meet the requirements.

To realize this function, you only need to turn the top digit of the function code address from 0 to 1.For example . the function code F0.07only modify the RAM value instead of storing it in the EEPROM. and can set the address set to 8007H. this address only use for writing on chip RAM. which can not do the read function . It's will be invalid address if read.

3.6 The definition of communication of Parameter address：

Definition	Parameter Address	Function Description		W/R Feature
Inverter setting parameters	Fx.xxH	x.xx stand for parameter number. For example: F5.05 is represented by 0505H.		
Control Command	1000H	0001H	Forward Running	W/R
		0002H	Reverse Running	
		0003H	JOG forward	
		0004H	JOG reverse	
		0005H	Stop	
		0006H	Coast to stop	
		0007H	Fault Reset	
		0008H	Jog stop	
Monitor State	1001H	0001H	Forward Running	R
		0002H	Reverse Running	
		0003H	Standby	
		0004H	Fault	
Communication setting value	2000H	Communication setting value range (-10000～10000) Note: The communication setting value is the percentage of the relative value (-100.00%～100.00%), which can be used for communication writing. When set as a frequency source, it is relative to the percentage of the maximum frequency (F0.04); when it is set as a torque, it is relative to the percentage of the torque upper limit (F3.07). When it set as PID given or feedback , the relative is the percentage of PID.		W/R
Monitor Parameter	3000H	Running frequency		R
	3001H	Setting frequency		R
	3002H	Output current		R
	3003H	Output voltage		R
	3004H	Output rotation speed		R
	3005H	Output power		R

Definition	Parameter Address	Function Description	W/R Feature
Monitor Parameter	3006H	Output torque	R
	3007H	DC bus voltage	R
	3008H	PID setting value	R
	3009H	PID feedback value	R
	300AH	Input terminal state	R
	300BH	Output terminal state	R
	300CH	Analog AVI value	R
	300DH	Analog ACI value	R
	3010H	The value of AVI	R
	3011H	The value of ACI	R
Inverter fault address	5000H	See the attached table Table:3–1	R
Communication fault address	5001H	See the attached table Table:3–2	R

Appendix Table :3-1 Data and fault type in 5000H

Data	Fault Type	Data	Fault Type
00H	No fault	0CH	Motor overload (OL1)
01H	Overcurrent when acceleration (ocA)	0DH	Inverter overload (OL2)
02H	Overcurrent when deceleration (ocd)	0EH	External fault (EF)
03H	Overcurrent when constant speed running (ocn)	0FH	RS485 communication fault (CE-1)
04H	Overvoltage when acceleration (ovA)	11H	Current detection fault (itE)
05H	Overvoltage when deceleration (ovd)	12H	Keypad communication fault (CE-4)
06H	Overvoltage when constant speed running (ovn)	13H	Motor auto tuning fault (tE)
07H	Overvoltage when stop(ovS)	14H	EEPROM operation fault (EEP)
08H	DC bus under voltage fault (Lv)	15H	PID feedback fault (PIDE)
09H	Iutput phase loss (LP)	16H	Inverter pre-overload (OL3)
0AH	Output short-circuit (SC)	10H，17H～1BH	Reserved
0BH	Over-heat (OH1)	1CH	Output phase loss (SPO)

Additional response to error communication:

When the inverter are communication connection. The inverter will response to the error code if the error caused, and the maximum unit (bit 7) of the command code set to 1 (Function code and 80H) and answer to the host The host will know there will be error.

ASCII mode

STX	':'
Address	'0'
	'1'
Function	'8'
	'6'
Fault address	'5'
	'0'
	'0'
	'1'
Fault code	'0'
	'1'
LRC Check	'2'
	'7'
END	CR
	LF

RTU mode

Address	01H
Function	86H
Fault address	50H
	01H
Fault code	01H
CRC CHK Low	F0H
CRC CHK High	C9H

Appendix Table :3-2 Data and fault type in 5001H

Communication fault address	5001H	00H	No fault
		01H	Command code error
		02H	Illegal address
		03H	Illegal data
		04H～05H	Reserved
		06H	Inverter is busy
		07H～09H	Reserved
		10H	Password error
		11H	Check error
		12H	Invalid modified parameters
		13H	System loacked
		14H	Illegal of data number

- The software detection is only valid for the model G030T4/P037T4and G015T2 and below power.No hardware detection.While there have software and hardware options when the inverter is power bigger than 30kW.

Fb.09 Under load protection current	
Setting Range: 0～150.0	Factory Setting:0

Fb.10 Under load protection time	
Setting Range:5.0～6500.00s	Factory Setting:5.0s

FC Group Serial communication

FC.00 Local address	
Setting range: 0～247	Factory setting : 1

This parameter determines the slave address used for communication with master. The value "0" is the broadcast address.

FC.01 Baud rate selection	
Setting range: 0～5	Factory Setting: 4

This parameter can set the date transmission rate during serial communication. Note: The baud rate of master and slave address must be the same.

0：1200BPS
1：2400BPS
2：4800BPS
3：9600BPS
4：19200BPS
5：38400BPS

FC.02 Data bit check setting	
Setting Range : 0～17	Factory Setting :1

This parameter defines the baud rate in serial communication, and data format used in protocols , only a consistent format can be normal communication.

0:No parity check （N，8，1）for RTU
1: Even parity check（E，8，1）for RTU
2: Odd parity check（O，8，1）for RTU
3: No parity check（N，8，2）for RTU
4: Even parity check（E，8，2）for RTU
5: Odd parity check（O，8，2）for RTU
6: No parity check（N，7，1）for ASCII
7 Even parity check（E，7，1）for ASCII
8: Odd parity check（O，7，1）for ASCII
9: No parity check（N，7，2）for ASCII
10: Even parity check（E，7，2）for ASCII
11: Odd parity check（O，7，2）for ASCII
12: No parity check（N，8，1）for ASCII
13: Even parity check（E，8，1）for ASCII
14: Odd parity check（O，8，1）for ASCII
15: No parity check （N，8，2）for ASCII
16: Even parity check（E，8，2）for ASCII
17: Odd parity check（O，8，2）for ASCII

The upper computer and the data format of the inverter must be consistent . Otherwise , Communication can't work .

FC.03 Communication answer delay time	
Setting range: 0～200ms	Factory Setting: 5ms

Answer delay: The interval time between the data receiving of the inverter and data sending to the upper monitor. If the answer delay is shorter than the system time, then it is subject to the system time, and if the answer delay is longer than the system, then the waiting time should be prolonged after the data processing to achieve the answer delay and then to send data to the upper monitor.

FC.04 Communication timeout fault time	
Setting range: 0.0～200.0s	Factory Setting: 0.0s

If the function code is set to 0.0s, this parameter is invalid.

If the function code is set to a valid value, when the interval time exceeds the communication overtime, the system will report communication fault (CE 1).

Generally, the parameter is set to invalid. If the parameter is set in a continuous communication system, the communication state can be monitored.

If it doesn't receive correct data signal during the delay time of FC.04, the inverter will determine stop or remain the state according to the solution of communication fault.

FC.05 Communication error action	
Setting range: 0～3	Factory Setting: 1

0: Alarm and coast to stop

1: Do not alarm and keep running

2: Do not alarm and stop at the stopping method (only for communication control mode)

3: Do not alarm and stop at the stopping method (for all communication control modes)

In the abnormal situation, the inverter can act through setting communication fault processing. The selected running state of the inverter is: shield the CE fault, stop or keep running.

FC.06 Response action	
Setting range: 0～1	Factory Setting : 0

0: Response to reading and writing

1: No response to writing

FC.07 Communication parameters address mode	
Setting Range:0～1	Factory Setting :0

0: The address is calculated according to the parameter group.

1:The address is calculated in sequence.increased one by one since F0.00.

FC.08 Linkage proportion coefficient	
Setting Range:0.01～10.00	Factory Setting:1.00

when the local machine is set by the master inverter control . the setting frequency is given by the main station . the parameter is used to set the local machine as a slave via RS485/RS232 interface receiving the weight coefficient of the frequency command .

The actual setting frequency of the load machine is equal to the value of the parameter is multiplied by RS485 / 232 interface receives the frequency setting command value.

FC.09 Linkage proportion source selection	
Setting Range:0～4	Factory Setting:0