TOKY®

DR9 Series

Intelligent Power Recorder

Communication Protocol

KKDR9-B21E/A0/20211018

I. MODBUS serial communication protocol

DR9 series energy meter adopts Modbus RTU communication protocol RS485 half duplex communication , read function code 0x03, write function code 0x10 , adopts 16 digit CRC check, the energy meter does not feedback the check error.

Start bit	Data bit	Stop bit	Check bit
1	8	1	No

(1) All the RS485 communication should comply with host/slave method. Under this method, information and data is transmitted between one host and maximum 32 slaves (monitoring equipment);
(2) Host will initialize and control all information transmitted in RS485 communication circuit.
(3) In any case, communication can never be started from a slave.
(4) All the RS485 communication is sending by packet . One data packet is a simple string (every string has 8 bit). One packet include 128 byte at most. The bytes in the packet formed in standard asynchronous serial data , and transmitting in the mode of 8 data bits, 1 stop bit, no check bit.
(5) Host sending is called request, slave sending is called response.
(6) In any case, slave can only respond to one request of host.

2. Each MODBUS cdata packet is consisted several parts as below:
(1) Slave address; (2) Function code to be executed; (3) Register address (variate address); (4) Data; (5) CRC check;
(1) Slave address: address length is 1 byte, effective slave address range is 1-247, if slave receives a data packet, whose frame address information is consonant with its own address information , it will execute the order of data packet.
(2) Function code length in MODBUS data packet is one byte, used to inform the slave what kind of operation needs to be executed. The slave response data packet should have the same function code byte of the operation requested by host.
Please refer to below table for related function code:

Function code	Meaning	Function
0x03	Read register	Read one or more present register value
0x06	Write single-register	Write specified value into one internal register
0x10	Write multi-register	Write specified value into several internal registers (Factory default write single register)

(3) Register address variable: data area storage location when slave executes effective order. Different variable seizes differents numbers of register, some address variable seizes two register, 4 byte data, somevariable seizes one register, 2 byte data, please use according to actual situation.
(4) Data area: data area includes the data required by terminal to execute specified function or collected data when terminal respond to query. The content of the data could be numerical value, reference address or set value; for example: function code tells terminal to read a register, data area needs to indicate which register to started from and how much data to be read, embedded address and data will be different according to different content between type and slave; register numerical value send sequence : high byte in the front, low byte in the back.
(5) CRC check: MODBUS-RTU mode adopts 16 bit CRC check. Sending equipment should do CRC16 calculation for each data of packet, final result is stored in check area. Receiving equipment also make CRC16 calculation for each data of packet (except check area), and compare result area with check area; only the same packet can be accepted, for the specific CRC check algorithm please refer to appendix.

II. Network time consideration

Transmitting package in RS485 network should follow the time regulation as follows:
(1) When baud rate set as 9600, the delay time between two host request is recommended to be 300ms or more, lesser time may cause the loss of data packet.
(2) When the recommended baud rate is 9600, if use smaller baud rate, please enlarge delay time properly. For example, when baud rate is 2400, two request should be set as more than 500ms.

III. Abnormal communication processing

If host send a illegal data packet or host request a invalid data register, abnormal data response will happen. This abnormal data response is consisted of slave address, function code, error code and check area. When the high bit position of function code area is 1, it means the present data frame is abnormal response.
Below table illustrates the meaning of abnormal function code:
According to MODBUS communication requirement, abnormal response function code=request function code+0x80; when abnormal response, put 1 on the highest bit of function code. For example: if host request function code is 0x04, slave response function code is 0x84.

Error code type	Name	Contents illustration
0x01	Function code error	Meter received the unsupported function code
0x02	Variable address error	Data location designated by host exceeds range of meter, or receive illegal register operation.
0x03	Variable value error	Data value sent from host exceeds the corresponding data range of meter, or data structure is incomplete

IV. Communication frame format illustration

1. Read multi-register

For example, host reads UA (A phase voltage), suppose measured A phase voltage is 220.0V.

The address code of UA is 0x4000, because UA is fixed data (4 byte), seizes 2 data register, the hexadecimal data of 220.0V is 0x0000898 (2200).

Host request

Slave address	Read function code	Register address (variable)		Register quantity		CRC check code	
1	2	3	4	5	6	7	8
Meter address	Function code	Start address high bit	Start address low bit	High bit	Low bit	CRC code low bit	CRC code high bit
0x01	0x03	0x40	0x00	0x00	0x02	0xD1	0xCB

Slave normal answers (high bit is in front)

Slave address	Read function code	Byte number (2 times of register quantity)	Register data		Register data		CRC check code	
1	2	3	4	5	6	7	8	9
Meter address	Function code	Data byte length	Data 1 high bit	Data 1 low bit	Data 2 high bit	Data 2 low bit	CRC code low bit	CRC code high bit
0x01	0x03	0x04	0x00	0x00	0x08	0x98	0xFC	0x59

Slave normal answers (low bit is in front)

Slave address	Read function code	Byte number (2 times of register number)	Register data		Register data		CRC check code	
1	2	3	4	5	6	7	8	9
Meter address	Function code	Data byte length	Data 2 high bit	Data 2 low bit	Data 1 high bit	Data 1 low bit	CRC code low bit	CRC code high bit
0x01	0x03	0x04	0x08	0x98	0x00	0x00	0x79	0xBC

Function code abnormal answer: (For example, host request function code is 0x04).

Slave abnormal answers (Read multi-register)				
1	2	3	8	9
Meter address	Function code	Error code	CRC code low bit	CRC code high bit
0x01	0x84	0x01	0x82	0xC0

For example: When present measured current value is: Ia=100 A, Ib=200 A, Ic=300 A, separately read three current value at a time. Host send read 01 address meter, read the current value data started from 400C (A phase current) register. Hexadecimal code of 100.000 is 000186A0; hexadecimal code of 200.000 is 00030D40; hexadecimal code of 300.000 is 000493E0; data adopts the 32-bit unsigned data representation, with three decimal point. For example, if data value is 12345, the actual value is 12.345.

Host send

Meter address	Function code	Address		Register quantity		CRC check code	
01	03	40	0C	00	06	10	0B

Meter return

Meter address	Function code	Read byte number	Data 1				Data 2				Data 3				CRC check code	
01	03	0C	00	01	86	A0	00	03	0D	40	00	04	93	E0	8F	1D

2. Write single-register

For example: Host writes fixed data, 1st alarm mode is AD1.

Suppose the address code of AD1 is 0x4900, because AD1 is fixed data, seizes 1 data register, decimalist code of 11 is 0X000B.

Host request (Write single-register)

Slave station address	Write function code	Register address (variable)		Register Data		CRC check code	
1	2	3	4	5	6	7	8
Meter address	Function code	Start address high 8 bit	Start address low 8 bit	High bit	Low bit	CRC code low bit	CRC code high bit
0x01	0x06	0x49	0x00	0x00	0X0B	0XDE	0x51

Slave normal answer (Write single-register)

Slave address	Write function code	Register address (variable)		Register number		CRC check code	
1	2	3	4	5	6	7	8
Meter address	Function code	Start address high 8 bit	Start address low 8 bit	High bit	Low bit	CRC code low bit	CRC code high bit
0x01	0x06	0x49	0x00	0x00	0x01	0x5E	0x56

3. Write multi-register

For example: Host writes fixed data, 1st alarm mode is AD1.

Suppose the address code of AD1 is 0x4900, because AD1 is fixed data, seizes 1 data register, decimalist code of 11 is 0X000B.

Host request (Write multi-register)										
1	2	3	4	5	6	7	8	9	10	11
Meter address	Function code	Start address high bit	Start address low bit	Data byte length high bit	Data byte length low bit	Data byte length	Data 1 high bit	Data 1 low bit	CRC code low bit	CRC code high bit
0x01	0x10	0x49	0x00	0x00	0x01	0x02	0x00	0x0B	0x3F	0x53

Slave normal answer (Write multi-register)							
1	2	3	4	5	6	7	8
Meter address	Function code	Start address high 8 bit	Start address low 8 bit	Data byte length high bit	Data byte length low bit	CRC code low bit	CRC code high bit
0x01	0x10	0x49	0x00	0x00	0x01	0x17	0x95

Data position error answer:(For example, host request write address index is 0x0050).

Slave abnormal answer (Write multi-register)				
1	2	3	4	5
Meter address	Function code	Error code	CRC code low bit	CRC code high bit
0x01	0x90	0x02	0xCD	0xC1

Parameter address reflection table (Note: address code is the index of variable array)

No.	Address reflection	Variable name	Byte length	Date type	Read/Write	Remark
1	0x4000	Phase voltage A	2	long	R	0.1V Note ⑦
2	0x4002	Phase voltage B	2	long	R	
3	0x4004	Phase voltage C	2	long	R	
4	0x4006	Line voltage AB	2	long	R	
5	0x4008	Line voltage BC	2	long	R	
6	0x400a	Line voltage CA	2	long	R	
7	0x400c	A phase current	2	long	R	0.001A Note ⑦
8	0x400e	B phase current	2	long	R	
9	0x4010	C phase current	2	long	R	
10	0x4012	Active power A	2	long	R	0.1W Note ⑦
11	0x4014	Active power B	2	long	R	
12	0x4016	Active power C	2	long	R	
13	0x4018	Total active power	2	long	R	
14	0x401a	Reactive power A	2	long	R	0.1KW Note ⑦
15	0x401c	Reactive power B	2	long	R	
16	0x401e	Reactive power C	2	long	R	

17	0x4020	Total reactive power	2	long	R	0.1kVA Note ⑦
18	0x4022	Apparent power A	2	long	R	
19	0x4024	Apparent power B	2	long	R	
20	0x4026	Apparent power C	2	long	R	
21	0x4028	Total apparent power	2	long	R	
22	0x402a	Power factor A	2	long	R	0.001 Note⑦
23	0x402c	Power factor B	2	long	R	
24	0x402e	Power factor C	2	long	R	
25	0x4030	Total power factor	2	long	R	
26	0x4032	Frequency	2	long	R	0.001Hz Note⑦
27	0x4034	Total Kwh	2	long	R	0.001kWh Note⑦
28	0x4036	Total Kvarh	2	long	R	
29	0x4038	Forward Kwh	2	long	R	
30	0x403a	Backward Kwh	2	long	R	
31	0x403c	Forward Kvarh	2	long	R	
32	0x403e	Backward Kvarh	2	long	R	
33	0x4046	active power demand	2	long	R	0.001
34	0x4048	active power maximum demand	2	long	R	
35	0x404A	reactive power demand	2	long	R	
36	0x404C	reactive power maximum demand	2	long	R	
37	0x4052	A phase voltage harmonic content	2	long	R	0.1 Note⑦
38	0x4054	B phase voltage harmonic content	2	long	R	
39	0x4056	C phase voltage harmonic content	2	long	R	
40	0x4058	A phase current harmonic content	2	long	R	
41	0x405a	B phase current harmonic content	2	long	R	
42	0x405c	C phase current harmonic content	2	long	R	
43	0x405E	netural line current	2	long	R	0.001
extend						
44	0x4100	Total kwh	2	long	R	0.001kWh Note⑦
45	0x4102	Total Tine tariff kwh	2	long	R	
46	0x4104	Total Peak tariff kwh	2	long	R	
47	0x4106	Total middle tariff kwh	2	long	R	
48	0x4108	Total vale tariff kwh	2	long	R	
49	0x410a	Total kwh this month	2	long	R	
50	0x410c	Total Tine tariff kwh this month	2	long	R	
51	0x410e	Total Peak tariff kwh this month	2	long	R	
52	0x4110	Total middle tariff kwh this month	2	long	R	
53	0x4112	Total vale tariff kwh this month	2	long	R	
54	0x4114	Total kwh last month	2	long	R	
55	0x4116	Total Tine tariff kwh last month	2	long	R	
56	0x4118	Total Peak tariff kwh last month	2	long	R	
57	0x411a	Total middle tariff kwh last month	2	long	R	
58	0x411c	Total vale tariff kwh last month	2	long	R	
59	0x411e	Total kwh last II month	2	long	R	
60	0x4120	Total Tine tariff kwh last II month	2	long	R	0.001kWh Note⑦
61	0x4122	Total Peak tariff kwh last II month	2	long	R	
62	0x4124	Total middle tariff kwh last II month	2	long	R	
63	0x4126	Total vale tariff kwh last II month	2	long	R	

extend						
64	0x4800	Primary coil voltage PT1	2	long	R/W	0.001 Note ⑦
65	0x4802	secondary coil voltage PT2	2	long	R/W	
66	0x4804	primary coil current CT1	2	long	R/W	
67	0x4806	secondary coil current CT2	2	long	R/W	
68	0x4808	1st Alarm value	2	long	R/W	
69	0x480a	1st Alarm hysteresis value	2	long	R/W	
70	0x480c	2nd Alarm value	2	long	R/W	
71	0x480e	2nd Alarm hysteresis value	2	long	R/W	
72	0x4818	Transmit 1 high limit value	2	long	R/W	
73	0x481a	Transmit 1 low limit value	2	long	R/W	
extend						
74	0x4900	1st Alarm mode (refer to table 1)	1	int	R/W	No decimal point
75	0x4901	1st Alarm unit Note ④	1	int	R/W	
76	0x4902	1st alarm start delay	1	int	R/W	
77	0x4903	1st alarm finish delay	1	int	R/W	
78	0x4904	2nd Alarm mode (refer to table 1)	1	int	R/W	
79	0x4905	2nd Alarm unit Note ④	1	int	R/W	
80	0x4906	2nd alarm start delay	1	int	R/W	
81	0x4907	2nd alarm finish delay	1	int	R/W	
extend						
82	0x4980	1st transmit mode (refer to table 1)	1	int	R/W	No decimal point
83	0x4981	1st transmit unit note④	1	int	R/W	
extend						
84	0x4a00	Link mode note ①	1	int	R	No decimal point
85	0x4a01	Communication address	1	int	R	
86	0x4a02	Baud rate note②	1	int	R	
87	0x4a03	Data format note⑧	1	int	R	No decimal point
88	0x4a07	switch output note③	1	int	R	
89	0x4a08	switch input note ⑤	1	int	R	
90	0x4a09	remote input note⑥	1	int	R/W	
extend						
91	0x4a80	Tariff Rate 1 time	1	int	R/W	No decimal point
92	0x4a81	Tariff Rate 2 time	1	int	R/W	
93	0x4a82	Tariff Rate 3 time	1	int	R/W	
94	0x4a83	Tariff Rate 4 time	1	int	R/W	
95	0x4a84	Tariff Rate 5 time	1	int	R/W	
96	0x4a85	Tariff Rate 6 time	1	int	R/W	
97	0x4a86	Tariff Rate 7 time	1	int	R/W	
98	0x4a87	Tariff Rate 8 time	1	int	R/W	
99	0x4a8c	time period 1	1	int	R/W	
100	0x4a8d	time period 2	1	int	R/W	
101	0x4a8e	time period 3	1	int	R/W	
102	0x4a8f	time period 4	1	int	R/W	
103	0x4a90	time period 5	1	int	R/W	
104	0x4a91	time period 6	1	int	R/W	
105	0x4a92	time period 7	1	int	R/W	
106	0x4a93	time period 8	1	int	R/W	

107	0x4c00	demand happen time: year	1	int	R	no decimal point
108	0x4c01	demand happen time: month	1	int	R	
109	0x4c02	demand happen time: day	1	int	R	
120	0x4c03	demand happen time: hour	1	int	R	
121	0x4c04	demand happen time: minute	1	int	R	
122	0x4c05	demand happen time: second	1	int	R	
123	0x4c06	active power maximum demand happen time: year	1	int	R	
124	0x4c07	active power maximum demand happen time: month	1	int	R	
125	0x4c08	active power maximum demand happen time: day	1	int	R	
126	0x4c09	active power maximum demand happen time: hour	1	int	R	
127	0x4c0A	active power maximum demand happen time: minute	1	int	R	
128	0x4c0B	active power maximum demand happen time: second	1	int	R	
129	0x4c0C	reactive power maxi demand happen time: year	1	int	R	
130	0x4c0D	reactive power maxi demand happen time: month	1	int	R	
131	0x4c0E	reactive power maxi demand happen time: day	1	int	R	
132	0x4c0F	reactive power maxi demand happen time: hour	1	int	R	
133	0x4c10	reactive power maxi demand happen time:minute	1	int	R	
134	0x4c11	reactive power maxi demand happen time: second	1	int	R	

Note Explanation

Note: 1. Connection mode

Communication value	0	1
Menu display	3-4	3-3

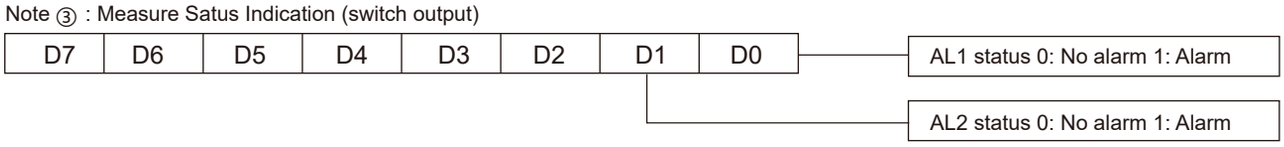
Note:2. Baud rate

Communication value	0	1
Menu display	4.8	9.6

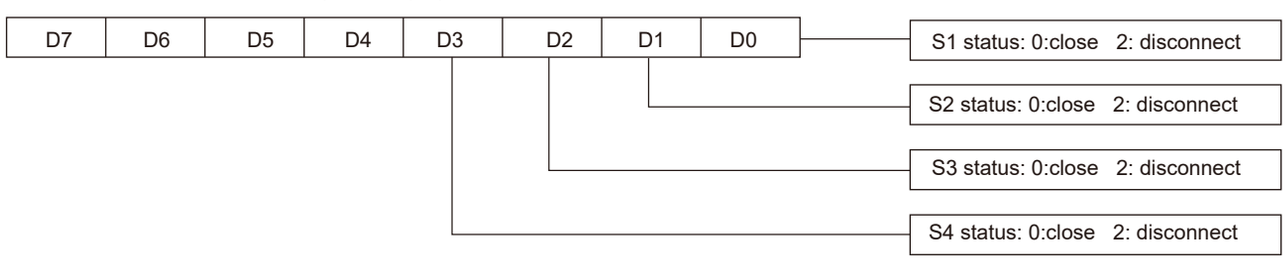
Note: 4. Alarm/Analog Unit

Communication value	0	1	2
Menu display	1	K	M

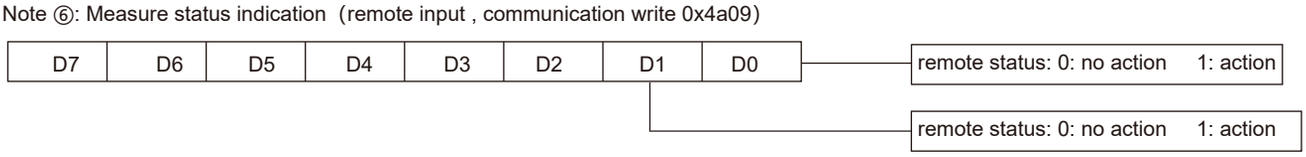
Note ③ : Measure Satus Indication (switch output)



Note ⑤: measure status indication(switch input)



Note ⑥: Measure status indication （remote input , communication write 0x4a09）



Note⑦: communication data reading value and corresponding actual value illustration:

Communication data using hexadecimal format, is divided into long-form shape (32) and a short-form shape (16) . Read data multiplied the corresponding unit is the actual measurement data. Eg. RS485 reading A phase volt is 0X00038E28, voltage unit is 0.001V , then the actual vlaue is 23300 (0x00038e28)X0.001V=233.0V

note ⑧:dataformat

1	0
LH	HL