

MODBUS® 通讯协议

MODBUS® 协议

DCRL 无功补偿功率因数控制器通过通讯扩展模块支持 Modbus RTU®, Modbus ASCII®, ModbusTCP® (仅 DCRL8) 通讯协议。通讯扩展模块如下:

EXP 10 10 USB

EXP 10 11 RS 232

EXP 10 12 RS485

EXP 10 13 Ethernet (仅DCRL8)

利用该协议可以使用第三方监控软件 (SCADA) 或者其他支持 Modbus® 的智能设备, 如 PLC 等读取设备状态和控制设备。

参数设置

进入 SETUP 菜单选择 ADV 菜单进行 Modbus® 协议配置: 仅可以配置 1 个通讯端口。

高级菜单

串口通讯

参数	功能	默认值	范围	注释
P.49	节点地址	01	01-255	
P.50	串口速率	9600	1200 2400 4800 9600 19200 38400 57600 115200	
P.51	数据格式	8bit - n	8 bit - no par. 8 bit, odd 8 bit, even 7 bit, odd 7 bit, even	8 位无奇偶校验 8 位, 奇校验 8 位, 偶校验 7 位, 奇校验 7 位, 偶校验
P.52	停止位	1	1-2	

P.53	协议	Modbus RTU	Modbus RTU Modbus ASCII Modbus TCP (仅 DCRL8)
------	----	------------	--

对于扩展模块 EXP1013（以太网模块，仅 DCRL8），进入 SETUP 菜单，选择 FUN，相应参数为：

参数	功能	默认值	范围	注释
F.01	IP 地址	IP1 192 IP2 168 IP3 001 IP4 001	000.000.000.000 - 255.255.255.255	
F.02	子网掩码	SUB1 0 SUB2 0 SUB3 0 SUB4 0	000.000.000.000 - 255.255.255.256	
F.03	IP 端口	1001	0-32000	
F.04	客户端/服务器	Server	Slave Server	从站 主站
F.05	远程 IP 地址	RIP1 0 RIP2 0 RIP3 0 RIP4 0	000.000.000.000 - 255.255.255.256	
F.06	远程 IP 端口	1001	0-32000	
F.07	IP 网关地址	GW1 0 GW2 0 GW3 0 GW4 0	000.000.000.000 - 255.255.255.256	

MODBUS® 遥控终端（RTU）协议

如果选择 Modbus®RTU 协议，通讯信息格式如下：

T1 T2 T3	地址 (8 位)	功能 (8 位)	数据 (Nx8 位)	CRC (16 位)	T1 T2 T3
----------	-------------	-------------	---------------	---------------	----------

地址域是从站目标串行地址

功能域是从站必须执行的功能码

数据域包含发往从站的数据或者从从站按照需求读取的数据

对于 DCRL 控制器，数据域长度最长为 80 个 16 位寄存器（160 个字节）

CRC 域允许主站和从站检查信息的完整性

如果一条信息被电气噪声或干扰破坏，CRC 域允许设备识别该错误然后忽略此信息

T1, T2, T3 顺序对应于时间，此时间内，通讯总线上数据不可以交换以允许设备识别一条信息的结束和另一条信息的开始。该时间至少是一个字符发送需要的时间的 3.5 倍。

DCRL8 测量时间是从一个字符接收开始，到下一个字符的接收为止。如果这个时间超过指定波特率发送 3.5 个字符所需时间，那么下一个字符将被认为是一条新消息的开始。

Modbus 功能

可用功能码如下：

03 = 读输入寄存器	允许读取设备测量值
04 = 读输入寄存器	允许读取设备测量值
06 = 预置单个寄存器	允许写参数
07 = 读异常	允许读取设备状态
10 = 预置多个寄存器	允许写几个参数
17 = 报告从站 ID	允许读取设备信息

例如：从 DCRL 串行地址 01 处读取柜内温度，其位于位置 14（16 进制 0E），信息发送如下：

01	04	00	2D	00	02	E0	08
----	----	----	----	----	----	----	----

这里：

01 = 从站地址

04 = Modbus®功能码“读输入寄存器”

00 2D = 所需寄存器地址（温度），减一

00 02 = 从地址 0 开始读取的寄存器数

E0 08 = CRC 校验和

DCRL 应答如下：

01	04	04	00	00	00	1C	FA	4D
----	----	----	----	----	----	----	----	----

这里：

01 = DCRL 地址（从站 01）

04 = 主站所需功能码

04 = DCRL 发送的字节数

00 00 00 1C = 温度的 16 进制数值 = 28 = 28°C

FA 4D = CRC 校验和

功能码 04：读取输入寄存器

Modbus®功能码 04 允许从从站存储单元读取一个或多个连续寄存器。每一个测量值的地址如表 2。按照 Modbus®标准，队列消息的地址必须是表中有效地址**减一**。

如果测量值地址不在表中或需求寄存器数量超过可接受最大值，DCRL 将返回错误代码（见错误列表）。

主站队列

从站地址	08h
功能码	04h
MSB 地址	00h
LSB 地址	0Fh
MSB 寄存器编号	00h
LSB 寄存器编号	08h
LSB CRC	C1h
MSB CRC	56h

在上表中，从站 08 被请求从地址 10h 开始的连续 8 个寄存器。这样，寄存器将返回从 10h 到 17H 的值。通常，信息以 CRC 校验和结尾。

从站应答：

从站地址	08h
功能码	04h
字节数	10h
MSB 寄存器 10h	00h
LSB 寄存器 10h	00h
-----	----
MSB 寄存器 17h	00h
LSB 寄存器 17h	00h
LSB CRC	5Eh
MSB CRC	83h

应答总是包含主站请求的从站地址、功能码和请求寄存器的内容。应答以 CRC 结束。

功能码 06：预置单个寄存器

该功能允许写寄存器。仅限地址大于 1000h 的寄存器。例如：可以改变设置参数。如果数值不在有效范围，DCRL 将报错。同样方式，如果参数地址无法被识别，DCRL8 将发送错误应答。

主站信息：

从站地址	08h
功能码	06h
MSB 寄存器地址	2Fh
LSB 寄存器地址	0Fh
MSB 数据	00h
LSB 数据	0Ah
LSB CRC	31h
MSB CRC	83h

从站应答：

从站应答是对请求的回应，即：从站向主站发回地址和变量新值。

功能码 07：读异常状态

该功能码允许读取控制器工作状态。

主站请求：

从站地址	01h
功能码	07h
LSB CRC	41h
MSB CRC	E2h

下表给出了由 DCRL 应答发送的状态字节的含义：

位	含义
0	操作模式 AUT
1	操作模式 MAN

功能码 17：报告从站 ID

该功能码允许识别设备型号。

主站队列	
从站地址	01h
功能码	11h

从站应答	
从站地址	01h
功能码	11h

LSB CRC	C0h
MSB CRC	2Ch

字节数	08h
数据 01 (型号) ①	49h
数据 02 (软件版本)	00h
数据 03 (硬件版本)	00h
数据 04 (参数版本)	00h
数据 05 (设备类型) ②	00h
数据 06 (预留)	00h
数据 07 (预留)	00h
LSB CRC	00h
MSB CRC	F7h

① 67 – 43h = DCRL3

69 – 45h = DCRL5

73 – 49h = DCRL8

② 1 – 01h = DCRL 系列

错误

一旦从站接收到一条错误信息，它回应的信息包括队列功能码（与 80h 取或），并加上一个错误代码字节。下表是从站发向主站的错误码列表。

表 1：错误代码

代码	错误
01	无效功能码
02	无效地址
03	参数超限
04	功能无法执行
06	从站忙，功能暂不可用

MODBUS® ASCII 协议

Modbus®ASCII 协议通常用于几个调制解调器的通讯。

功能码和地址码的使用与 RTU 协议一样，但传输字符串使用 ASCII 格式，信息结尾由回车/换行分隔，而不是传输中断分隔。

如果参数 P16.n.05 设置为 Modbus®ASCII 协议，相应通讯端口的通讯信息格式如下：

.	地址 (2 字符)	功能 (2 字符)	数据 (N 个字符)	LRC (2 字符)	CR LF
---	--------------	--------------	---------------	---------------	-------

地址域是从站目标设备的串行地址

功能域是从站必须执行的功能代码

数据域包含发送到从站的数据或是从从站接收到的从站对请求应答的数据。最大允许长度是（读取页 3）个连续寄存器。

LRC 域允许主站和从站检查信息的完整性。如果一条信息被电气噪声或干扰破坏，CRC 域允许设备识别该错误然后忽略此信息

CRLF，信息终止控制符（0D 0A）。

示例：

例如，读取 L3 的相电流值，它位于从站串行节点地址 08 的 12（0Ch）处，信息发送格式如下：

:	08	04	00	03	00	02	56	CRLF
---	----	----	----	----	----	----	----	------

其中：

: ASCII 3Ah 信息开始分隔符

08 = 从站地址

04 = 读输入寄存器 Modbus®功能码

00 03 = 被请求寄存器地址（L3 相电流），减一

00 02 = 从地址 04 开始读取的寄存器数量

56 = LRC 校验和

CRLF = ASCII 0Dh 0Ah = 信息结束分隔符。

DCRL 应答如下：

:	08	04	04	00	00	01	3D	9B	CRLF
---	----	----	----	----	----	----	----	----	------

其中：

: = ASCII 3Ah 信息开始分隔符

08 = DCRL 地址（从站 08）

04 = 主站请求的功能码

04 = 仪表发送的字节数

00 00 01 3D = 电流值 (=317A)

9B = LRC 校验码

CRLF = ASCII 0Dh 0Ah = 信息终止分隔符

表 2：串口通讯协议提供的测量值

(使用功能码 03 和 04)

地址	字	瞬时测量值 (IN)	单位	格式
02H	2	①实际 $\cos \phi$		无符号长整型
04H	2	电压	V	无符号长整型
06H	2	电流	A/1000	无符号长整型
08H	2	千乏差值②	kvar	有符号长整型
0AH	2	周平均功率因数	/100	无符号长整型
0EH	2	电气柜温度②	°C	有符号长整型
10H	2	输出状态		无符号长整型
12H	2	相角偏差	°/4	无符号长整型
14H	2	实际功率因数	/5000	有符号长整型
16H	2	误差位状态③		无符号长整型
18H	2	最高电压	V	无符号长整型
1AH	2	最大电流	A/100	无符号长整型
1CH	2	电容器过载最大值	%	无符号长整型
1EH	2	最高温度	°C	无符号长整型
32H	2	有功功率	W	有符号长整型
34H	2	无功功率	Var	有符号长整型
36H	2	视在功率	VA	无符号长整型
200H	2	步 1 投入时间	min	无符号长整型
---	---	---	---	---
21AH	2	步 14 投入时间	min	无符号长整型
2005H	2	电容器电流过载%	%	无符号整型
2020H	1	步 1 投入次数		无符号整型
---	---	---	---	---
202DH	1	步 14 投入次数		无符号整型
2040H	1	步 1 剩余功率	%	无符号整型
---	---	---	---	---
204DH	1	步 14 剩余功率	%	无符号整型
2008H	1	THDV	%/10	无符号整型
2080H	1	2 次电压谐波	%/10	无符号整型
---	---	---	---	---
208DH	1	15 次电压谐波	%/10	无符号整型
2009H	1	THDI	%/10	无符号整型

20A0H	1	2 次谐波电流	%/10	无符号整型
---	---	---	---	---
20ADH	1	15 次谐波电流	%/10	无符号整型
2007H	1	还需多少小时维护	h	有符号整型

①：位 31 表示正负号（0=正，1=负），位 30 表示感性/容性（0=IND 感性，1=CAP 容性）；

②：位 31 表示正负号（0=正，1=负）；

③：读取起始地址 16h 的字，返回的 32 位的含义如下：

表 3：

位	代码	含义
0	A01	欠补偿
1	A02	过补偿
2	A03	欠电流
3	A04	过电流
4	A05	欠电压
5	A06	过电压
6	A07	电容器过载
7	A08	温度超限
8	A09	无电压释放
9	A10	电压 THD 太大
10	A11	电流 THD 太大
11	A12	请求维护
12	A13	步故障
13...31	-	预留

表 4：命令（使用功能码 06）

地址	字	状态	格式
2FF0H	1	命令列表①	无符号整型
3000H	1	操作模式变更②	无符号整型
3001H	1	控制器复位（热启动）③	无符号整型
3005H	1	步启用④	无符号整型
3006H	1	步禁用④	无符号整型
3007H	1	键盘锁启用/禁止⑤	无符号整型

①下表列出了地址 2FF0h 中各位的含义，有些功能可能同时发生。

值	功能
00h	C01 复位维护服务时间间隔
01h	C02 复位步操作计数器
02h	C03 复位步微调

03h	C04 复位步操作计时器
04h	C05 复位最大峰值
05h	C06 复位复位周功率因数
06h	C07 恢复设置为出厂默认值
07h	C08 备份用户设置参数
08h	C09 用用户设置参数回复设置参数

②下表列出地址 3000h 中各值相应功能：

值	功能
0	从自动 AUT 模式切换到手动 MAN 模式，或者相反
1	切换到手动 MAN 模式
2	切换到自动 AUT 模式

③向地址写入值 01，相应功能将被执行；

④对相应寄存器进行写操作，将启用或禁止步；如果激活重连接时间还没有到 0 的步，则此次命令则无效

⑤向地址写入 01 键盘被锁，写入 00 键盘解锁。

参数设置

使用 Modbus®协议可以访问菜单参数。DCRL8 操作手册给出了数值和所选功能以及测量单位之间的正确对应关系。

参数读取流程

1. 使用功能码 6，在地址 5002H 写入需要读取的参数①；
2. 在地址 5004H，执行功能码 4，寄存器数量接近参数的长度（见下表）；
3. 如果继续读取下一个参数（在同一个菜单或子菜单下），重复步骤 2，否则执行步骤 1。

参数写入的流程

1. 使用功能码 6，在地址 5001H 写入需要更改的参数①；
2. 在地址 5003H，执行功能码 16，寄存器数量接近参数的长度；
3. 如果继续写入下一个参数（在同一个菜单或子菜单下），重复步骤 2；否则执行步骤 1；不需要写入其他参数，执行步骤 4；
4. 要使设置参数的更改生效，需要将这些数值使用表 3 的专有命令存入 EEPROM（在地址 2F03H，使用功能码 4，写入数值 5）。

参数类型	寄存器数
数字值（数值）<= 65535（如：P. 30）	1 个寄存器（2 字节）

数字值 (数值) >65535 (如: P.6)	2 个寄存器 (4 字节)
--------------------------	---------------

④可以使用功能码 4 读取存储在地址 5002H 中的参数。

示例:

设定参数 P.01 (CT 一次侧) 的值为 250

步骤 1: 选定 P.01

主站 功能码 = 6 (06H)
 地址 = 5002H (5002H - 0001H = 5001H)
 数值 = 1 (01H)

01	06	50	01	00	01	08	CA
----	----	----	----	----	----	----	----

DCRL8 功能码 = 6 (06H)
 地址 = 5002H (5002H - 0001H = 5001H)
 数值 = 1 (01H)

01	06	50	01	00	01	08	CA
----	----	----	----	----	----	----	----

步骤 2: 设置 250

主站 功能码 = 16 (10H)
 地址 = 5003H (5003H - 0001H = 5002H)
 寄存器数 = 1 (02H)
 字节数 = 2 (04H)
 数值 = 250 (00000FAH)

01	10	50	02	00	02	04	00	00	00	FA	0E	36
----	----	----	----	----	----	----	----	----	----	----	----	----

DCRL8 功能码 = 16 (10H)
 地址 = 5002H (5003H - 0001H = 5002H)
 数值 = 250 (00000FAH)

01	10	50	02	00	02	F1	08
----	----	----	----	----	----	----	----

步骤 3: 保存和重启

主站 功能码 = 6 (06H)

地址 = 2F03H (2F03H - 0001H = 2F02H)

数值 = 4 (04H)

01	06	2F	02	00	04	21	1D
----	----	----	----	----	----	----	----

DCRL8 无应答。

词汇表

Modbus 协议- Modbus Protocol

功率因数控制器 – power factor controller

欠补偿 – under compensation

过补偿 – over compensation

欠电流 – low current

过电流 – high current

欠电压 – low voltage

过电压 – high voltage

无电压释放 – no-voltage release

步故障 – step failure