upsViewer101 ModbusTCP 协议 Ver1.3

时间 2021 年 12 月

文档修订记录表

序号	版本	修订原因及修订内容	拟制人/修订人	修订时间
1	V1.1	新拟制	李春录 郭世军	2021-6-8
2	V1.2	更新告警数据说明		2021-8-24
3	V1.3	更新寄存器变量名称		2021-12-20

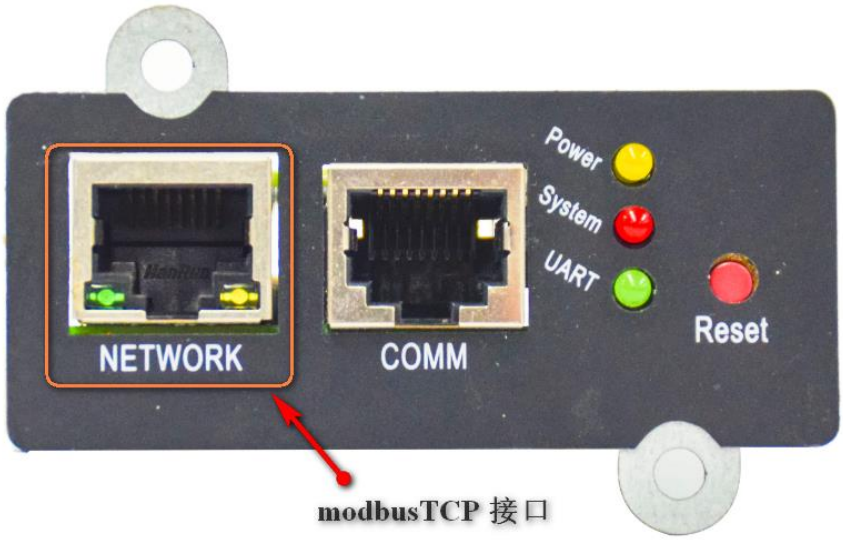
目录

1.1 协议简介 Protocol Introduction

Modbus 协议是应用于控制器上的一种通用语言。通过该协议使 upsViewer 经网络和其他设备之间可以进行通信。本通信采用应答方式，由主设备发起请求，从设备执行请求并且应答。在同一时间，总线上只能有一个主设备，但可以有一个或多个从设备，从设备需通过地址设置加以区分，从设备可设置的地址范围为 0x01~0xFF。

1.2 ModbusTCP 接口

ModbusTCP 接口如下图所示：upsViewer IP 地址可从搜索软件或管理网页读取、端口号（默认:502）



1.3 ModbusTCP 报文格式

ModbusTCP 协议格式如下：

MBAP	功能码	数据

实例：

请求报文：00 00 00 00 00 06 09 03 00 04 00 01

根据上面的协议格式从左到右：

00 00 为传输标识符； 00 00 协议标识符（这里是 modbus 协议）； 00 06 报文后边的字节数；

09 单元标识符 （比如 IP 地址：192.168.0.9 这个地址的从设备）；03 功能码（读保持寄存器的值）；00 04 Modbus 起始地址；00 01 读取寄存器的个数（这里读取一个寄存器 一个寄存器占 2 个字节）；

响应报文：00 00 00 00 00 05 09 03 02 00 05

从左到右：

00 00 为传输标识符（与请求报文一致）；00 00 协议标识符；00 05 报文后边的字节数；09 单元标识符；03 功能码； 02 后边的字节数；00 05 具体数据 。

1.4 响应信息分类

主机向从机设备发送查询并希望有一个正常响应，主机查询中有可能产生 4 种事件：

（1）从机接收查询，无通讯错误，正常处理信息，则返回一个正常响应事件。

（2）由于通讯出错，从机不能接收查询数据，因而不返回响应。此时，主机依靠处理程序判定为查询超时。

（3）若从机接收查询，发现有 (LRC 或 CRC) 通讯错误，不返回响应，此时依靠主机处理程序判定为查询超时。

（4）从机接收查询，无通讯错误，但无法处理(如读不存在的寄存器地址或错误的寄存器个数)时，向主机报告错误的性质。

向主机报告错误的响应信息有 2 个与正常响应不相同的区域：

功能代码区：正常响应时，从机的响应功能代码区，带原查询的功能代码。所有功能代码的 MSB 为 0(其值低于 80H)。不正常响应时，从机把功能代码的 MSB 置为 1，使功能代码值大于 80H，高于正常响应的值。这样，主机应用程序能识别不正常响应事件，能检查不正常代码的数据区。

数据区：正常响应中，数据区含有(按查询要求给出的) 数据或统计值，在不正常响应中，数据区为一个不正常代码，它说明从机产生不正常响应的条件和原因。

1.5 功能码

功能码	名称	作用
0x01	读线圈	在一个远程设备中，使用该功能码读取线圈(作为获取告警状态功能码)
0x05	写单个线圈	在一个远程设备上，使用该功能码写单个输出为 ON 或 OFF。
0x03	读取保持寄存器	在一个或多个保持寄存器取得当前的二进制值（作为获取模拟量功能码）
0x06	预置单寄存器	把具体二进制值装入一个保持寄存器（作为写入工装设置数据）

1.6 通信寄存器地址

1.6.1 设备信息

0x01 功能码查询；

实际查询地址 = 地址偏移+寄存器 ID

地址偏移 = 0

寄存器 ID	变量名	类型	权限	描述
0	系统运行状态	bit	只读	0：正常； 1：告警；
1	内存剩余空间不足告警	bit	只读	0：正常； 1：告警；
2	数据存储失败告警	bit	只读	0：正常； 1：告警；

0x03 功能码查询；

实际查询地址=地址偏移+寄存器 ID

地址偏移= 0

寄存器 ID	变量名	类型	权限	系数	描述
0	IP 控制方式	int16	只读	1	0：手动；1：DHCP；
1	IP 地址 1	int16	只读	1	一个 IP 地址占用四个寄存器，每个寄存器存储一段，例如：192.168.1.5，那么“IP 地址 1”存放（192），“IP 地址 2” 存放（168），“IP 地址 3” 存放（1），“IP 地址 4” 存放（5）；子网掩码和网关以此类推； **寄存器范围：0-255；**
2	IP 地址 2	int16	只读	1	
3	IP 地址 3	int16	只读	1	
4	IP 地址 4	int16	只读	1	
5	子网掩码 1	int16	只读	1	
6	子网掩码 2	int16	只读	1	
7	子网掩码 3	int16	只读	1	
8	子网掩码 4	int16	只读	1	
9	网关 1	int16	只读	1	
10	网关 2	int16	只读	1	
11	网关 3	int16	只读	1	
12	网关 4	int16	只读	1	

1.6.2 UPS

0x01 功能码查询；

实际查询地址=地址偏移+寄存器 ID

地址偏移= 100

寄存器 ID	变量名	类型	权限	描述
1. 机柜告警量				
0	使能状态	bit	只读	0：系统中无此设备； 1：系统中存在此设备；
1	通信状态	bit	只读	0：通信断开； 1：通信正常；
机柜告警量				
2	综合告警	bit	只读	0：正常； 1：告警；
3	紧急关机	bit	只读	0：正常； 1：告警；
4	逆变器启动容量不足	bit	只读	0：正常； 1：告警；
5	市电异常	bit	只读	0：正常； 1：告警；
6	旁路故障	bit	只读	0：正常； 1：告警；
7	旁路相序故障	bit	只读	0：正常； 1：告警；
8	旁路电压故障	bit	只读	0：正常； 1：告警；
9	旁路超跟踪	bit	只读	0：正常； 1：告警；
10	旁路过载	bit	只读	0：正常； 1：告警；
11	旁路过载超时	bit	只读	0：正常； 1：告警；
12	旁路风扇故障	bit	只读	0：正常； 1：告警；
13	切换次数到	bit	只读	0：正常； 1：告警；
14	输出短路	bit	只读	0：正常； 1：告警；
15	电池 EOD	bit	只读	0：正常； 1：告警；
16	电池低压	bit	只读	0：正常； 1：告警；
17	电池接反	bit	只读	0：正常； 1：告警；
18	输入 N 线断开	bit	只读	0：正常； 1：告警；
19	失去 N+X 冗余	bit	只读	0：正常； 1：告警；
20	禁止开机	bit	只读	0：正常； 1：告警；
21	EOD 系统禁止	bit	只读	0：正常； 1：告警；
22	UPS 过温	bit	只读	0：正常； 1：告警；
23	手动旁路	bit	只读	0：正常； 1：告警；
24	发电机接入	bit	只读	0：正常； 1：告警；

0x03 功能码查询；

实际查询地址=地址偏移+寄存器 ID

地址偏移= 100

寄存器 ID	变量名	类型	权限	系数	单位	描述
1. 机柜模拟量						
0	旁路电压 ph_A	int16	只读	0.1	V	
1	Reserved	int16	只读			
2	Reserved	int16	只读			
3	旁路电流 ph_A	int16	只读	0.1	A	
4	Reserved	int16	只读			
5	Reserved	int16	只读			
6	旁路频率 ph_A	int16	只读	0.01	Hz	
7	Reserved	int16	只读			
8	Reserved	int16	只读			
9	旁路 PF ph_A	int16	只读	0.01		
10	Reserved	int16	只读			
11	Reserved	int16	只读			
12	输入电压 ph_A	int16	只读	0.1	V	
13	Reserved	int16	只读			
14	Reserved	int16	只读			
15	输入电流 ph_A	int16	只读	0.1	A	
16	Reserved	int16	只读			
17	Reserved	int16	只读			
18	输入频率 ph_A	int16	只读	0.01	Hz	
19	Reserved	int16	只读			
20	Reserved	int16	只读			
21	输入 PF ph_A	int16	只读	0.01		
22	Reserved	int16	只读			
23	Reserved	int16	只读			
24	输出电压 ph_A	int16	只读	0.1	V	
25	Reserved	int16	只读			
26	Reserved	int16	只读			
27	输出电流 ph_A	int16	只读	0.1	A	
28	Reserved	int16	只读			
29	Reserved	int16	只读			
30	输出频率 ph_A	int16	只读	0.01	Hz	
31	Reserved	int16	只读			
32	Reserved	int16	只读			
33	输出 PF ph_A	int16	只读	0.01		

34	Reserved	int16	只读			
35	Reserved	int16	只读			
36	输出视在功率 ph_A	int16	只读	0.1	kVA	
37	Reserved	int16	只读			
38	Reserved	int16	只读			
39	输出有功功率 ph_A	int16	只读	0.1	kW	
40	Reserved	int16	只读			
41	Reserved	int16	只读			
42	输出无功功率 ph_A	int16	只读	0.1	kVar	
43	Reserved	int16	只读			
44	Reserved	int16	只读			
45	负载百分比 ph_A	int16	只读	0.1	%	
46	Reserved	int16	只读			
47	Reserved	int16	只读			
48	环境温度	int16	只读	0.1	℃	
49	电池温度	int16	只读	0.1	℃	
50	正电池组电压	int16	只读	0.1	V	
51	负电池组电压	int16	只读	0.1	V	
52	正电池组电流	int16	只读	0.1	A	
53	负电池组电流	int16	只读	0.1	A	
54	电池剩余时间	int16	只读	0.1	分钟	
55	电池容量百分比	int16	只读	0.1	%	
56	旁路风扇运行时间	int16	只读	1	h	
57	Reserved	int16	只读			
58	Reserved	int16	只读			
59	Reserved	int16	只读			
60	Reserved	int16	只读			
61	Reserved	int16	只读			
62	Reserved	int16	只读			
63	Reserved	int16	只读			
64	Reserved	int16	只读			
65	Reserved	int16	只读			
66	Reserved	int16	只读			
67	Reserved	int16	只读			
68	Reserved	int16	只读			
69	Reserved	int16	只读			
70	Reserved	int16	只读			
2. 机柜状态量						
71	供电方式	uint16	只读	1		0：均不供电；1：UPS 供电； 2：旁路供电

72	电池状态	uint16	只读	1		0：电池未连接；1：电池未工作；2：电池浮充；3：电池均充；4：电池放电；5：电池未检测；
73	维修旁路空开状态	uint16	只读	1		0：断开; 1：闭合
74	电池自检状态	uint16	只读	1		0：未自检;1：成功; 2：失败; 3：自检中
75	电池维护状态	uint16	只读	1		0：未维护测试;1：成功; 2：失败; 3：维护测试中
76	整流器状态	uint16	只读	1		0：关闭；1：软启动；2：正常工作；
77	Reserved	uint16	只读			
78	Reserved	uint16	只读			
79	Reserved	uint16	只读			
80	Reserved	uint16	只读			
81	Reserved	uint16	只读			
82	Reserved	uint16	只读			
83	Reserved	uint16	只读			
84	Reserved	uint16	只读			
85	Reserved	uint16	只读			
86	Reserved	uint16	只读			
87	Reserved	uint16	只读			
88	Reserved	uint16	只读			
89	Reserved	uint16	只读			
90	Reserved	uint16	只读			
3. 机柜信息量						
91	UPS 输入输出相数	uint16	只读	1		0: 3 相进 3 相出; 1: 3 相进 1 相出; 2: 1 相进 1 相出;
92	电池数量	uint16	只读	1		
93	电池 AH	uint16	只读	1		
94	电池额定电压	uint16	只读	1		
95	电池类型	uint16	只读	1		0:铅酸电池, 1:锂电池, 2:镍锌电池
96	UPS 额定容量	uint16	只读	1	kVA	
97	UPS 额定输入电压	uint16	只读	1	V	
98	UPS 额定输入频率	uint16	只读	1	Hz	
99	UPS 额定输出电压	uint16	只读	1	V	
100	UPS 额定输出频率	uint16	只读	1	Hz	

1.6.3 温湿度

0x01 功能码查询；

实际查询地址=地址偏移+寄存器 ID+i*单个设备占用的寄存器总数

设备个数最多 4 个，i 为设备 ID 从 0 开始

地址偏移= 3271，单个设备占用的寄存器总数 = 10

寄存器 ID	变量名	类型	权限	描述
0	使能状态	bit	只读	0：系统中无此设备； 1：系统中存在此设备；
1	通信状态	bit	只读	0：通信断开； 1：通信正常；
2	综合告警	bit	只读	0：正常； 1：告警；
3	温度过高	bit	只读	0：正常； 1：告警；
4	温度过低	bit	只读	0：正常； 1：告警；
5	湿度过高	bit	只读	0：正常； 1：告警；
6	湿度过低	bit	只读	0：正常； 1：告警；
7				

0x03 功能码查询；

实际查询地址=地址偏移+寄存器 ID+i*单个设备占用的寄存器总数

设备个数最多 4 个，i 为设备 ID 从 0 开始

地址偏移= 3271，单个设备占用的寄存器总数 = 10

寄存器 ID	变量名	类型	权限	系数	单位	描述
0	温度	int16	只读	0.1	℃	
1	湿度	int16	只读	0.1	RH	
2						
3						

1.6.4 水浸

0x01 功能码查询；

实际查询地址=地址偏移+寄存器 ID+i*单个设备占用的寄存器总数

设备个数最多 1 个，i 为设备 ID 从 0 开始

地址偏移= 3311，单个设备占用的寄存器总数 = 10

寄存器 ID	变量名	类型	权限	描述
0	使能状态	bit	只读	0：系统中无此设备； 1：系统中存在此设备；
1	通信状态	bit	只读	0：通信断开； 1：通信正常；
2	漏水告警	bit	只读	0：正常； 1：告警；
3	线缆异常	bit	只读	0：正常； 1：告警；
4				

0x03 功能码查询；

实际查询地址=地址偏移+寄存器 ID+i*单个设备占用的寄存器总数

设备个数最多 1 个，i 为设备 ID 从 0 开始

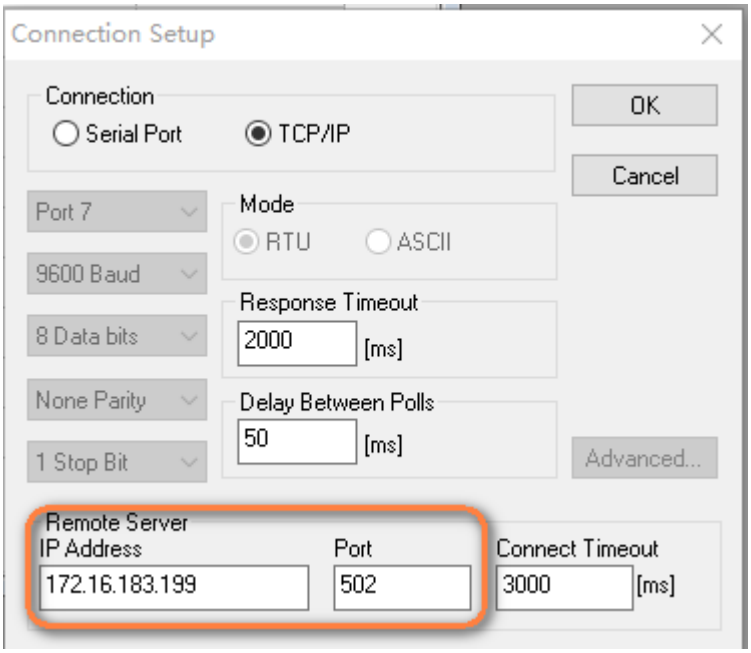
地址偏移= 3311，单个设备占用的寄存器总数 = 10

寄存器 ID	变量名	类型	权限	系数	单位	描述
0	漏水位置	int16	只读	0.1	m	此值为 0 表示未漏水，或者不支持漏水定位；

1.7 ModbusTCP 查询实例

1.打开查询工具 mbpoll 

2.检查网络是否畅通，输入 upsViewer IP，检查端口信息,端口号默认为 502



3、从“旁路电压 ph_A”开始查询 100 数据

①到 UPS 通讯寄存器地址信息页。

0x03 功能码查询；

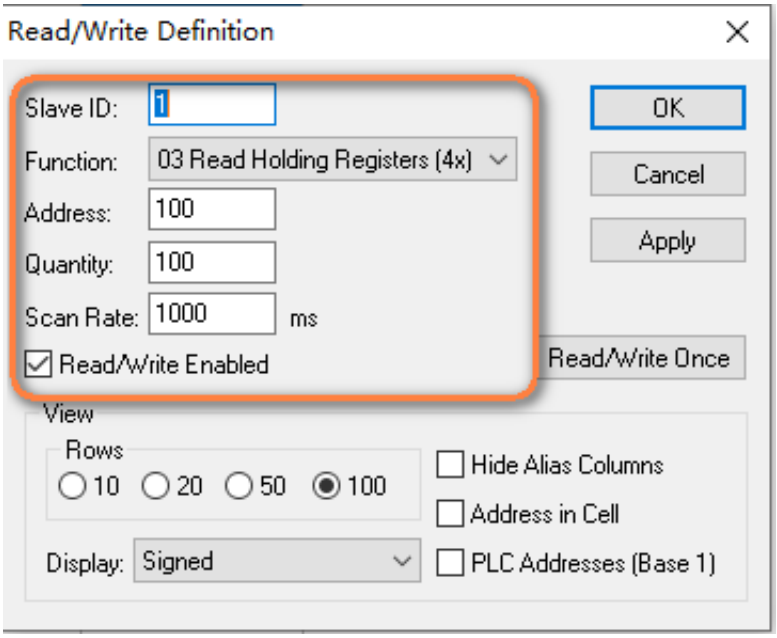
实际查询地址=地址偏移+寄存器 ID

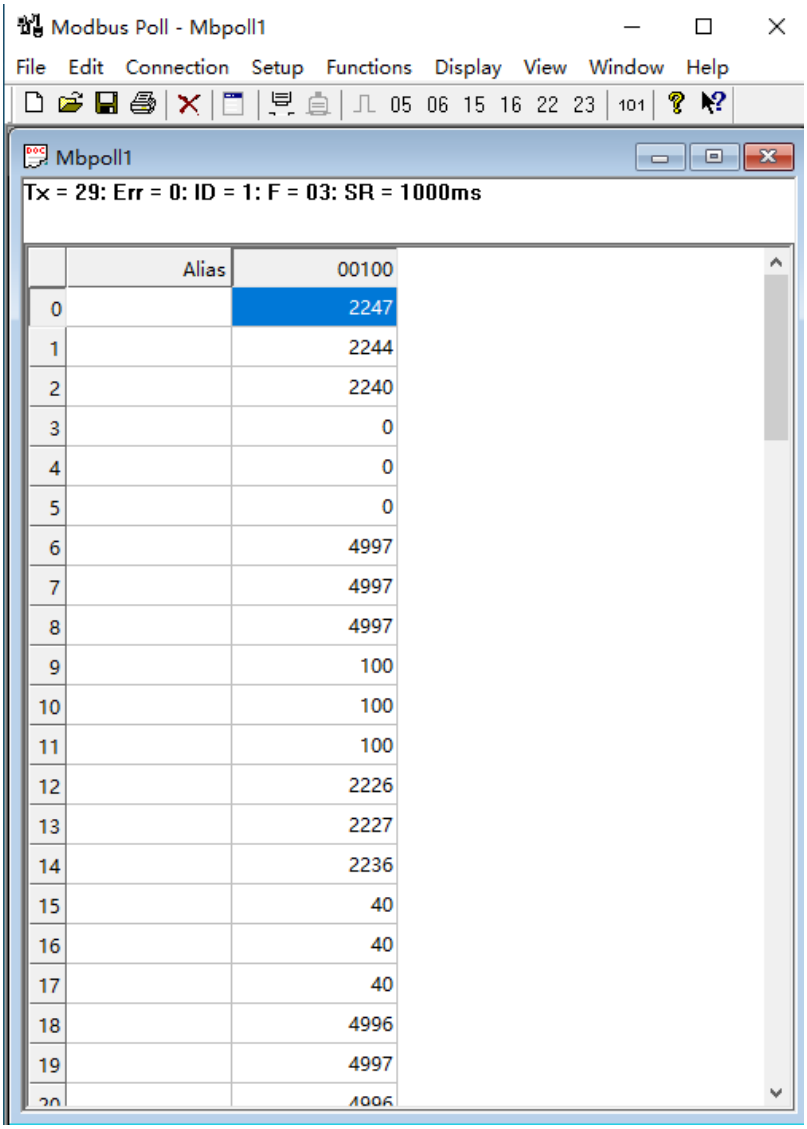
地址偏移= 100

寄存器 ID	变量名	类型	权限	系数	单位	描述
1. 机柜模拟量						
0	旁路电压 ph_A	int16	只读	0.1	V	
1	旁路电压 ph_B	int16	只读	0.1	V	
2	旁路电压 ph_C	int16	只读	0.1	V	
3	旁路电流 ph_A	int16	只读	0.1	A	

②获取查询功能码为 0X03，实际查询地址 =100+0 = 100

③输入功能码、查询地址，查询。


Read/Write Definition
Slave ID: 1
Function: 03 Read Holding Registers (4x)
Address: 100
Quantity: 100
Scan Rate: 1000 ms
Read/Write Enabled
OK
Cancel
Apply
Read/Write Once
View
Rows
10 20 50 100
Hide Alias Columns
Address in Cell
Display: Signed
PLC Addresses (Base 1)


Modbus Poll - Mbpoll1
File Edit Connection Setup Functions Display View Window Help
05 06 15 16 22 23 101
Mbpoll1
Tx = 29: Err = 0: ID = 1: F = 03: SR = 1000ms
Alias 00100
0 2247
1 2244
2 2240
3 0
4 0
5 0
6 4997
7 4997
8 4997
9 100
10 100
11 100
12 2226
13 2227
14 2236
15 40
16 40
17 40
18 4996
19 4997