# Modbus 协议简单讲解和测试

扶程星云 20210313

## 前言

首先,以一张图来说明 Modbus 在和灯具交互的说明



寄存器地址概念; 一个地址即所谓的控制回路,可以理解为一个地址控制一条线。 但是1和2分别是该寄存器所有控制回路全关和全开,给寄存器1写入0,表示全关,给寄存器2写入1表示全开,,该寄存器地址内的内容属于无效数据。 剩下的地址是每条回路,读取的时候值为1表示开,0表示关,写入1控制该回路的灯全开,写入0控制该回路的灯全关。

刚开始接触 Modbus 协议有个思维误区,以为从站是接收的和被动的,实际上在某种角度看是有误会的,从站上的寄存器地址存放的是设备传过来的值,我们读取的也是从站寄存器地址上的值,特别是单向设备的值:即仅发送自身的值,比如温湿度,电表的电压、电流等。从站上的寄存器是和最终设备互动的,比如灯开了,从站寄存器对应的值就是1,灯灭了,从站寄存器地址的值就是0。

我们可以通过寄存器地址的值来控制这个设备开关,比如设置为1,灯就会执行开灯动 作,设置为0,灯就会执行关灯动作。

### 简易测试

ModbusSlave 是一个从站设备仿真软件,它用于接收主设备的命令包,并回送数据包; 可用于测试和调试 Modbus 主站设备,便于观察 Modbus 通信过程中的各种报文。

Modbus Poll: Modbus 主机仿真器,用于测试和调试 Modbus 从设备。

1、我们用 Modbus Slave 做一个设备仿真器。

1.1 我们设置从站信息:

💰 Modbus Slave - M	bslave1					
File Edit Connection	Setup Display	View Window	Help			
D 🛩 🖬 🕾 🗖 🗒 🚊	Slave Defini	ition F8				
🗒 Mbslave1	Use as Defa	ult				
ID = 5: F = 03						
Alias	00100					
0	2323					
1	22					
2	3434					
3	111					
4	32323					
5						
6						
7						
8						
9						

#### 1.2 设置从站信息如下:

Slave Definition	×
Slave ID:	ОК
Function: 03 Holding Register (4x)	<ul> <li>✓ Cancel</li> </ul>
Address: 100 Protocol addre	ess. E.g. 40011 = 10
Quantity: 5	
View Rows 10 0 20 0 50 0 100	) Fit to Quantity
Hide Alias Columns PLC A	ddresses (Base 1)
Error Simulation	
Skip response	Insert CRC/LRC error (Not when using TCP/IP) Return exception 06, Busy

**1.3** 我们需要设置从站地址->Slave ID,存放模式->Function,存放的起始地址->Address,数量->Quantity,其他的先用默认的设置。 然后点击 OK。

1.4 点击 Connection 设置连接。

👬 Modbus Slave - Mbslave1									
File	Edit	Connection	Setup	Display	View				
	🗳 🖬 i	Connect Disconne	ect	F3					
ID = No	= 5: F conn	Auto Co Quick Co	nnect	, F5					

1.5 主要设置的是连接方式->Connection,端口号->Port,然后点击 OK。

Connection Setup		×
Connection Modbus TCP/IP	→ OK	
Serial Settings		
COM1	$\sim$	
9600 Baud $\sim$	Mode RTU ASCII	
8 Data bits $\sim$	Flow Control	
Even Parity 💦 🗸 🗸		
1 Stop Bit	1 [ms] RTS disable delay	
TCP/IP Server		
IP Address	Port	
192.16.79.11	~ 503	
Any Address	IPv4	
Ignore Unit ID	○ IPv6	
	-	

#### 1.6 在列表中修改对应的值。

D = 5: F	= 03	
	Alias	00100
0		2323
1		22
2		3434
3		111
4		32323
5		
6		
7		
8		
9		

2、接着,我们设置 MOdbus Poll 来读取数据。

2.1 首先设置读取模式。

ଷିକ୍ର Modbus Poll - [Mbpoll1]											
🗒 File Edit Connection	Setup Functions Display	View Window Help									
D 📽 🖬 🚳 🗙 🗖 🗒 🎃	Read/Write Definition	F8									
Tx = 264: Err = 86: ID = 5	Read/Write Once	56									
No connection	Read/Write Disabled	Shift+F6									
Alias	Excel Log	Alt+X									
0	Excel Logging Off	Alt+Q									
1	Log	Alt+L									
2	Logging Off	Alt+O									
3	Reset Counters	F12									
4	Reset All Counters	Shift+F12									
5	Use as Default										
6											
7											
8											
9											

#### 2.2 参考之前从站信息来设置。

Slave Definition X	Read/Write Definition X
Slave ID: 5	Slave ID: Slave ID: OK Function: 03 Read Holding Registers (4x) V Cancel
Address: 100 Protocol address. E. or 10011 = 10	Address: 100 Protocol address. E.g. 40011 -> 10
Quantity: 5	Quantity: 5
View Rows Ill Ill Ill Ill Ill Ill Ill Ill Ill Il	Scan Rate:       1000       [ms]       Apply         Disable       Read/Write Disabled       Read/Write Once         Disable on error       Read/Write Once         View       Rows       010       50       100       Fit to Quantity
Error Simulation           Skip response         Insert CRC/LRC error           (Not when using TCP/IP)         Return exception 06, Busy	Hide Alias Columns PLC Addresses (Base 1) Address in Cell Enron/Daniel Mode

#### 2.3 打开连接。



2.4 设置连接信息,因为是本机所以 IP 地址是 127.0.0.1,服务器端口号也是之前设置的 503, 其余默认,点击 OK 键。

Connection		OK
Modbus TCP/IP	~	- OK
Serial Settings		Cancel
COM1	$\checkmark$	Mode
9600 Baud $\sim$		RTU OASCII
8 Data bits $\sim$		Response Timeout
Even Parity $\sim$		Delay Between Polls
1 Stop Bit	Advanced	20 [ms]
Remote Modbus Server		
IP Address or Node Name	)	
127.0.0.1		~
127.0.0.1 Server Port	Connect Timeout	
503	3000 [me]	01-04



#### 2.5 我们双击左边的值,在弹出的窗口填写值。

Enter signed int 16	×
Value: 82323	OK
Auto increment	Cancel

#### 2.6 右边的 Modbus Poll 会实时更新值。

as N	🕉 Modbus Slave - Mbslave1					ଷ୍ଟି Modbus Poll - [Mbpoll1]			
File	Edit Connectio	n Setup Display	View N	842	File	Edit Conr	ection Setup F	unctions	
D 🖬	880.	à 🕴 😵 😽			i 🖉 🕞	ax I	[봉희] 1   05 0	6 15 16 1	
	/bslave1			Тх	= 784	: Err = 89	ID = 5: F = 03:	SR = 10	
ID =	5: F = 03			h		Alias	00100		
	Alias	00100		0			2323		
0	test01	2323		1	-		444		
1	test02	444	-	1			3434		
2		3434		3			334		
3		334		4			32323		
4		32323		5					
5				6					
6				7					
7				8					
8				9					
9				L .					
-			-						

3、我们以 MThings 为例,开始做测试。

3.1 首先移除所有链接和设备

る。 链接	国数据	目目	① 统计	<i>②</i> 辅助								
恢复	禁止	移除	>>	***	全部链接 >	刷新	新增网络链	接 移除网	络链接			
序号		名称		^ +	链接	链接状态	链接参数	链接操作	设备起始地址	设备结束地址	设备操作	备注
				******								

3.2 新建网络连接(服务器)



3.2.1 先设置一个 TCP 服务器,采用 MODBUS-TCP 传输协议,本地端口是 502,然后点击确 认按钮。

88 网络参数配置	?	×
-----------	---	---

参数名	数值
链接名称	NET001
链接模式	TCP服务器 ▽
链接空闲保持时间 (秒)	6000
传输模式	MODBUS-TCP(同步) 🛛 🔻
本地端口	502
目标IP	127.0.0.1
目标端口	
确认	取消

3.3 新增设备

3.3.1 在链路上点击设备操作的添加按钮。

+++	全部链接 ~	刷新	新增网络链挂	妾 移除网络	络链接			
サチュ	链接	链接状态	链接参数	链接操作	设备起始地址	设备结束地址	<mark>设备</mark> 操作	备注
++	NET001	已关闭	配置	启动	1	1	添加	
++								

#### 3.3.2 模拟一个从机(设备仿真)

38 请选择添加的	<b>没</b>	?	×
○ 模拟主机	●樽	钠从	机
确定		取消	í
	_	_	_

#### 3.3.3 设置一些值,点击数据,点击配置。

MThings 高效工作, 快乐生活 ∞ 🗉 🗄 🕚 8 Ø 链接 数据 自定义 统计 辅助 关于 \* 輸入查找名称 0 恢复 禁止 移除 >> 配置 筛选列 筛选行 筛选区块 解析报文 曲线 \*\*\*\*\*\*\*\* 序号 名称 ID 名称 数值 单位 区块 地址 数量( 001 CO [S]NET001 001

#### 3.3.4 点击新增按钮

サササ	输入查找名称	<b>Q</b>	酉	置 筛选列	新增	删除	上移	下移	排序	高级	同步	导入	导出
^ + +	ID	名称		数值	单位	D	⊠块	地址	数量	位偏移	位数	系数	范围
+													

#### 3.3.5 配置 5 条数据, 起始地址是 100, 点击确定。

分 新增数据配置	? ×
参数	数值
配置条数	5
起始数据地址	100
插入模板行下方	山 选择
确定	取消

3.3.6 出来以下列表,继续点击配置按钮后保存当前配置。

输入到		配置 筛选列	新増	删除 上移	下移	排序	高级	同步	导入	导出						
ID	名称	数值	单位	区块	地址	数量	位偏移	位数	系数	范围	曲线	传输类型	呈现类型	字节序	字序	间隔时间(ms)
1		0		保持寄存器(RW) >	100	1	0	16	1		□ 未选择	UINT 🔍	FLOAT \vee	大端 🎽	大端	0
2		0		保持寄存器(RW) >	101	1	0	16	1		□ 未选择	UINT 👻	FLOAT 👻	大端 ~	大端	0
3		0		保持寄存器(RW) >	102	1	0	16	1		□ 未选择	UINT 👻	FLOAT 👻	大満 🔹	大端 🔹	0
4		0		保持寄存器(RW) >	103	1	0	16	1		□ 未选择	UINT 👻	FLOAT 🔻	大端 🗸	大端 🔹	0
5		0		保持寄存器(RW) >	104	1	0	16	1		□ 未选择	UINT 👻	FLOAT 🔻	大端 🔻	大端	0

3.3.7 要修改哪个值就双击数值列中的值。

#### 〕 关于

输入到	查找名称		置	选列	筛选行	筛选区块	解析报	文 曲約	è	
ID	名	称	数值	1	单位	区块		地址	数量	位偏
1			0			保持寄存器	(RW)	100	1	0
2			0			保持寄存器	(RW)	101	1	0
3		20 选择模拟数	如据方法							
4										
5		参数名	í		数值	İ	ì	兑明	示例	J
		<b>策略</b>		固定值	<u>i</u>					
	固定值				0					
		应	Z用		返回	ם				

3.3.8 选择值的策略和值,我们分别设置下如下图。

输入重		置    筛选列	筛选行	筛选区块 解析报	文 曲約	1			
ID	名称	数值	单位	区块	地址	数量	位偏移	位数	系数
1				保持寄存器(RW)	100	1	0	16	1
2		555		保持寄存器(RW)	101	1	0	16	1
3		6767		保持寄存器(RW)	102	1	0	16	1
4		6761		保持寄存器(RW)	103	1	0	16	1
5		9889		保持寄存器(RW)	104	1	0	16	1

**3.3.9** 我们也可以设置设备的从地址,双击[S]NET001-001,表示从站的设备,这里可以修改 设备地址,也就是从站地址。

序号	名称		<b>99</b> 变更设备关键信息		?	×
001	((•)) [S]NET001-001		参数名	数值		
		1	设备名称	[S]NET001-001		
	1		链接	NET001		$\sim$
			设备地址	1		
			同步链接至其它设备	确认	Ę	以消

# 4、我们用 Modbus Poll 来测试 4.1 设置 IP 地址和 Port

onnection Setup		>
Connection		ОК
Modbus TCP/IP	~	
Serial Settings		Cancel
	$\sim$	Mode
9600 Baud $\sim$		ORIO OASUI
0 Dete bits		Response Timeout
8 Data bits 🗸 🗸		1000 [ms]
Even Parity $\sim$		
		Delay Between Polls
1 Stop Bit 🛛 🗸	Advanced	20 [ms]
Remote Modbus Server		
IP Address or Node Name		
127.0.0.1		~
Server Port	Connect Timeout	IPv4
502	3000 [ms]	

4.2 设置从站地址和起始地址。

Read/Write	e Definition		×
Slave ID:	1		ОК
Function:	03 Read Holding Reg	isters (4x) — 🖂	Cancel
Address:	100 Protoco	l address. E.g. 4001	1 -> 10
Quantity:	5		
Scan Rate:	1000 [ms]		Apply
Disable ReadA	Write Disabled e on error	F	Read/Write Once
View Rows ① 10	○20 ○50 ○	100 O Fit to Que	antity
Hide A	lias Columns ss in Cell	PLC Addresse	es (Base 1) Mode

4.3 记得点击连接。

4.4 然后,就可以看到 Modbus Poll 会随着从站里面寄存器的值的变化而变化了。

<ul> <li>         ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>					<sup>1</sup> Modbus Poll - [Mbpoll1] <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □					
^	ID	名称	数值							
to the	1		295		Alias	00100				
	2		555	0		295				
1.1.1	3		6767			555				
4				- 2		6/6/				
T. T.	4		6761	3		6761				
1.1	5		9889	4		9889				
1.1				5						
T. T.	-			6						
To Mark				7						

5、我们来看 MThings 的主站功能。

5.1 点击链接->新增网络链接,设置链接模式是 TCP 客户端,传输模式是 MODBUS-TCP (同步),目标地址是从站的地址,目前是本机,目标端口是 502,这些设置都要根据从站设 备来对应设置。

网络参数配置	? ×
参数名	数值
链接名称	NET002
链接模式	TCP客户端 ▽
重新建链周期 (秒)	0
链接空闲保持时间(秒)	6000
传输模式	MODBUS-TCP(同步) ~
传输模式 本地端口	MODBUS-TCP(同步) ×
<ul> <li>传输模式</li> <li>本地端口</li> <li>目标IP</li> </ul>	MODBUS-TCP(同步) ~  127.0.0.1
<ul> <li>传输模式</li> <li>本地端口</li> <li>目标IP</li> <li>目标端口</li> </ul>	MODBUS-TCP(同步) ~  127.0.0.1 502
本地端口 目标IP 目标端口	MODBUS-TCP(同步) ~  127.0.0.1 502

5.2 确认后,同样点击设备操作的添加按钮来添加设备,这里选择的是模拟主机。

<b>於</b> 请选	择添加的词	귳	?	×
●模	拟主机	01	莫拟人	、机
7		5	取消	当
1	用止			-
恢复	禁止	移	除	>>
恢复	禁止	移名称	除 、	>>
恢复 序号 001	₩AE 禁止 <mark>((○)) [S]</mark>	移 名称 NET(	除 、 )01-	>> •001
恢复 序号 001 002	無⋏上 禁止 ((o))[S] ᢏ☆́[M]	移 名称 NET( NET(	除 3001- 002-	.001

。 一 空更设备关键信息		?	×
参数名	数值		
设备名称	[M]NET002-001		
链接	NET002		$\sim$
设备地址	1		

注意从站地址要正确。

5.3 数据读取,点击数据,点击主站[M]NET002-001,点击配置和新增,在新增数据配置输入和从站相同的数据配置,然后再点击配置保存。

88 新增数据配置	?	$\times$
参数	数	值
配置条数	5	;
起始数据地址	10	0
插入模板行下方	i i	先择
确定	取消	í

7	ID	名称	数值	单位	读	指令	写	区块	地址	数量	位偏移	位数	系数	范围	批量读	批量写	曲线	传输类型	呈现类
++++	1				读		5	保持寄存器(RW)	100	1	0	16	1		🗹 已选择	- 未选择	- 未选择	UINT	FLOA
++	2				读		5	保持寄存器(RW)	101	1	0	16	1		🔽 已选择	未选择	- 未选择	UINT	FLOA
++++	3				读		5	保持寄存器(RW)	102	1	0	16	1		🔽 已选择	- 未选择	□ 未选择	UINT	FLOA
ナナ	4				读		写	保持寄存器(RW)	103	1	0	16	1		☑ 已选择	- 未选择	□ 未选择	UINT	FLOA
++	5				读		写	保持寄存器(RW)	104	1	0	16	1		🗹 已选择	- 未选择	□ 未选择	UINT	FLOA

5.4 我们可以看到左侧这个设备是没有连接的。

恢复	禁止移除>>	*
序号	名称	^ +
001	((•)) [S]NET001-001	+++
002	(M) NET002-001	+++++++++++++++++++++++++++++++++++++++
		+

5.5 继续点击链路菜单,点击该路链接的启动按钮。



这里需要注意的是,如果之前 MODBUS Poll 在连接中,请先中断连接。

显示已连接。

೫ MThings 高效工作,快乐生活

oo 链接	■ 数据	日二 自定义	小 统计	<b>②</b> 辅助	⑧ <sup>关于</sup>							
恢复	禁止	移除	>>		全部链接 >	刷新	新增网络链	妾 移除网络	络链接			
序号	名称 ^		^	链接	链接状态	链接参数	链接操作	设备起始地址	设备结束地址	设备操作		
001	<b>((•))</b> [S	]NET001	L-001		NET001	已连接	配置	关闭	1	1	添加	
				<b>NET002</b>	已连接	配置	关闭	1	1	添加		
002	((*)) [H					-						

5.6 点击主站设备,点击数据,然后点击读的按钮,就会读取数据出来。

88 WITTIN	I'YS IDXLIF, IXA	<b>王</b> /白															
∽ 链接	目 目: 数据 自定义	小 统计	<b>②</b> 辅助	(8) ¥:	) F												
恢复	禁止移除	>>	+++++++++++++++++++++++++++++++++++++++	输入	查找名称	_ ଦ୍	Ā	置 筛选列	筛选行	筛选区	块	解析报文	曲	线 批量读	批量写		
序号	名称		^ + + + + + + + + + + + + + + + + + + +	ID		名称		数值	单位	误	٦	指令	写	区块	地址	数量	位個
001	001 ((•)) [S]NET001-001		*	1				578		读			写	保持寄存器(RW)	100	1	(
	(a) MINETOO	2-001	+ + +	2				555		读			写	保持寄存器(RW)	101	1	(
002	(() [H]MHIOD	AJNETOO2 OOT		3						读			写	保持寄存器(RW)	102	1	(
			+++++++++++++++++++++++++++++++++++++++	4						读			写	保持寄存器(RW)	103	1	(
			+++++++++++++++++++++++++++++++++++++++	5						读			写	保持寄存器(RW)	104	1	(
			+++						I								
			+														

**5.7** 我们也可以点批量读,然后循环,这个设备就会不停的读数。我们可以通过修改从站寄存器地址的值来看是否变化。

	筛选⊵	マション マンチン マンチン マンチン マンチン マンチン アイティング ほうしん しんしょう しんしょ しんしょ	て曲	线 批量读 1	批量写	
_	读	指令	写	区块	地址	数
	读		写	保持寄存器(RW)	100	
	读		写	保持寄存器(RW)	101	
	读		写	保持寄存器(RW)	102	
	读		写	保持寄存器(RW)	103	
	读		写	保持寄存器(RW)	104	



,	大」												
ナナナ	输入到		配置 筛选列	筛选行	筛选⊵	区块 解析报文	て曲	线 批量读 🛛	批量写				
サナナ	ID	名称	数值	单位	读	指令	写	区块	地址	数量	位偏移	位数	系数
チチ	1		369		读		写	保持寄存器(RW)	100	1	0	16	1
ササ	2		555		读		写	保持寄存器(RW)	101	1	0	16	1
ササナ	3		666		读		写	保持寄存器(RW)	102	1	0	16	1
チナ	4		6761		读		写	保持寄存器(RW)	103	1	0	16	1
ナナ	5		9889		读		写	保持寄存器(RW)	104	1	0	16	1
2													

5.8 我们可以在指令里面填数,然后点击写的按钮,回写从站寄存器中对应的值,同时读回 来该值。

8
关于

	输入重		這 筛选列	筛选行	筛选⊵	区块 解析报文	曲	线 批量读	批量写	
	ID	名称	数值	单位	读	指令	写	区块	地址	数量
	1		255		读		写	保持寄存器(RW)	100	1
	2		22		读	22	5	保持寄存器(RW)	101	1
	3		666		读	/	写	保持寄存器(RW)	102	1
	4		6761		读	/	写	保持寄存器(RW)	103	1
	5		9889		读		写	保持寄存器(RW)	104	1

附录: 以下信息来自网络搜索结果。 Modbus 调试工具之 ModbusPoll 的使用方法

1: 打开软件进入主页面后点击该软件页面第二行"Connection"并选择"Connect.. F3"

2:(1)执行上一步操作后会弹出"Connection Setup"界面,在"Connection"下拉框根据对接文档选择对应的协议(一般为 Modbus TCP/IP)

- (2) 在"IP Adddress or Node Name"下的输入框中输入网关的 IP 地址
- (3) 在"Server Port"根据对接文档输入对应端口(默认为 502),点击"OK"

<b>P</b> • • •	💯 Mbpoll1						
Тх	Tx = 286: Err = 0: ID = 1: F = 06: SR = 1000ms						
No	No connection						
	Alias	00000					
0							
1		1					
2							
3							
4							
5							
6							
7							
8							
9							

如果连接效果如上图,显示红色"No connection",可能是地址输入错误或者端口有误,如果 对照文档确认无误仍是这样,那基本上就是设备出了问题,如电线未连接好等原因,可以联 系设备厂家或者安装方询问原因并协调解决

3: 在主页面"Setup"下选择第一个"Read/Write Definition..."

Read/Write Definition X					
Slave ID: 1	机地址 ок				
Function: 03 Read Holding Reg	isters (4x) 🗸 🔶 📊 🎼 🔤 cel 👘				
Address: 0	器也能。 address.e.g. 40011 -> 10				
Quantity: 4 🔶 访问数	建				
Scan Rate: 1000 [ms] 🔶	· 轮询时间 Apply				
Disable Read/Write Disabled Disable on error	Read/Write Once				
View Rows ● 10 ○ 20 ○ 50 ○ 1	100 🔘 Fit to Quantity				
Hide Alias Columns	PLC Addresses (Base 1) Enron/Daniel Mode				

	Alias	00000	Slave Definition	×
0 1 2 3 4 5 6 7 8 9	高存器1 寄存器1 寄存器10	0 0 16 32 48 0 0 0 0 0 0 0 0 0 0 0	Slave Definition Slave ID: IMULTION IMULT	OK 功能码ancel 的起始地址 Quantity s (Base 1) C/LRC error en using TCP/IP) xception 06, Busy

- (1) "Slave ID" 为从站地址,按照对接文档输入相应的值
- (2) "Function" 为寄存器功能码的选择

代码	中文名称	寄存器PLC地址	位操作/字操作	操作数量
01	读线圈状态	00001-09999	位操作	单个或多个
02	读离散输入状态	10001-19999	位操作	单个或多个
03	读保持寄存器	40001-49999	字操作	单个或多个
04	读输入寄存器	30001-39999	字操作	单个或多个
05	写单个线圈	00001-09999	位操作	单个
06	写单个保持寄存器	40001-49999	字操作	单个
15	写多个线圈	00001-09999	位操作	多个
16	写多个保持寄存器	40001-49999	字操作	多个

目前只做通过 Modbus 实现对寄存器的开关操作,所以下拉选择"06 Write Sxxx"

(3) "Address" 为寄存器起始地址(默认从1开始),同样按照对接文档进行输入

(4) "Quantity" 操作数量,因为"06 Write xxx"为操作单个,所以值只能为1,其他都会提示错误,输入完后点击"OK"

👺 Mbpoll1					
Tx = 31: Err = 0: ID = 1: F = 06: SR = 1000ms					
L					
L	Alias	00000			
0					
1		1			
2					
3					
4					
5					
6					
7					
8					
9					

正确连接后的效果如上图,可以点击"00000"下方的"1"双击改Value为"0"实现设备的开和关,当然,具体问题要具体分析,这里只能作为示例进行参考

👺 Mbpoll1						
Tx Tin	Tx = 5: Err = 5: ID = 1: F = 04: SR = 1000ms Timeout error					
	Alias	00000				
0						
1		0				
2						
3						
4						
5						
6						
7						
8						
9						

如果效果如上图,可能是从站地址、寄存器功能码或者寄存器起始地址输入错误,可对照文 核实从站地址、寄存器起始地址等,做到具体问题具体分析。

.通讯开始,主机端显示: TX=11, Err=0, ID=1, F=03, SR=1000ms。意思是,发送 11 次命令,错误次数 0,从机 ID,功能号 03,轮询间隔 1000ms。

🛍 Modbus Poll - Mbpoll1	🔏 Modbus Slave - Mbslave1	
File Edit Connection Setup Functions Display View Window Help	File Edit Connection Setup Display View Window Help	
🗅 🗃 🖬 🎒 🗙 🛅 🚆 🎰 🕮 05 06 15 16 17 22 23   TC 🗵   🤋 🌾		
Mbpoli1	💬 Mbslave1	
Tx = 11: Err = 0: ID = 1: F = 03: SR = 1000ms	ID = 1: F = 03	
Alias 00000	Alias 00000	
00	0 0	
1 16	1 16	
2 32	2 32	
3 48	3 48	
4	4 0	
5	5 0	
6	6 0	
		'xuw_xy

使用工具栏的"Communication Traffic"按钮,可以显示出当前发送命令和接受的数据,如下图:

<sup>1</sup> Modbus Poll - Mbpoll1           − <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> Mbpoll1 <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> Mbpoll1 <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> Mbpoll1 <sup>1</sup> File Edit Connection Setup Functions Display View Window Help <sup>1</sup> Mbpoll1 <sup>1</sup> File Edit Connection Setup Functions Display View Window Help					
Alias 00000 0 0 0 1 1 1 1 1 1 1 1 1 1 1 2 3 3 4 8 4 5 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Exit         Stop         Clear         Save         Copy         Log         Stop on Error         Time stamp           Transfer         Transfer				
再加一条数据解析: TX发送数据 01: 从机地址					

03: 功能码 00 00: 寄存器地址 00 06: 读取数据个数 6个 C5 C8: CRC校验 000066-Tx:01 03 00 00 00 06 C5 C8 000067-Rx:01 03 0C 00 0A 00 02 00 04 00 06 00 08 00 00 E7 CA 10 2 4 6 8 0 RX接收数据 01: 从机地址 03: 功能码 0C:返回字节数 (16进制数) 12字节 00 0A: 10 00 02: 2 00 04: 4 00 06: 6 00 08: 8 00 00: 0 E7 CA: CRC校验

ModbusSlave 是一个从站设备仿真软件,它用于接收主设备的命令包,并回送数据包;可用于测试和 调试 Modbus 主站设备,便于观察 Modbus 通信过程中的各种报文。

Modbus Poll : Modbus 主机仿真器,用于测试和调试 Modbus 从设备。该软件支持 ModbusRTU、 ASCII、TCP/IP。用来帮助开发人员测试 Modbus 从设备,或者其它 Modbus 协议的测试和仿真。 它支持多文档接口,即,可以同时监视多个从设备/数据域。每个窗口简单地设定从设备 ID,功能, 地址,大小和轮询间隔。你可以从任意一个窗口读写寄存器和线圈。如果你想改变一个单独的寄存器, 简单地双击这个值即可。或者你可以改变多个寄存器/线圈值。提供数据的多种格式方式,比如浮点、 双精度、长整型 (可以字节序列交换)。

Modbus Slave: Modbus 从设备仿真器,可以仿真32个从设备/地址域。每个接口都提供了对EXCEL

报表的 OLE 自动化支持。主要用来模拟 Modbus 从站设备,接收主站的命令包,回送数据包。帮助 Modbus 通讯设备开发人员进行 Modbus 通讯协议的模拟和测试,用于模拟、测试、调试 Modbus 通讯设备。可以 32 个窗口中模拟多达 32 个 Modbus 子设备。与 Modbus Poll 的用户界面相同, 支持功能 01, 02, 03, 04, 05, 06, 15, 16, 22 和 23,监视串口数据。