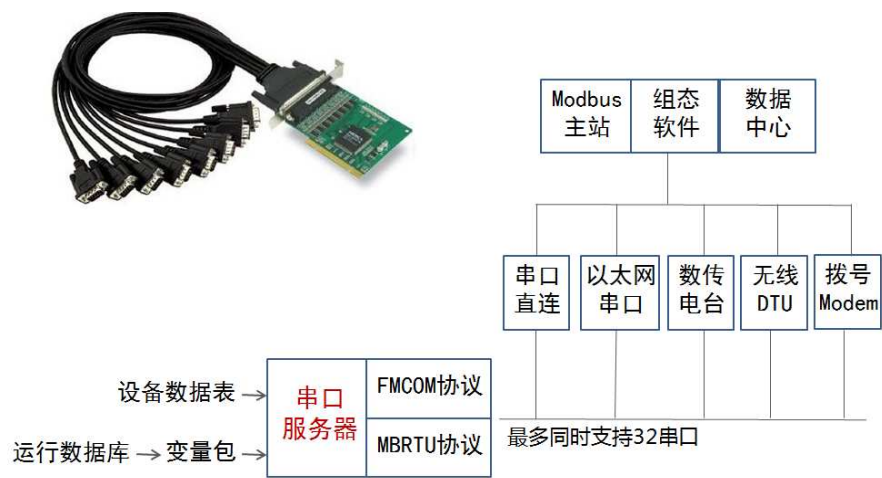


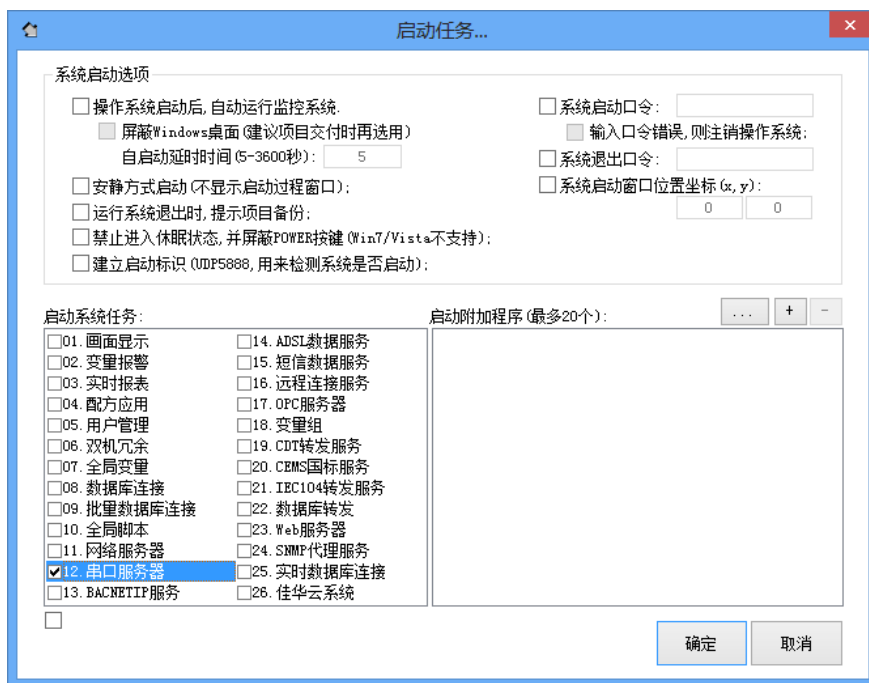
29. 串口服务器

编号	内容	页码
29.1	启动串口服务器	29-2
29.2	设置串口服务器	29-2
29.3	定义数据变量包	29-4
29.4	监视串口服务器	29-7
29.5	FMCOM 通讯协议	29-8
29.6	MODBUSRTU 协议	29-11



## 29.1 启动串口服务器

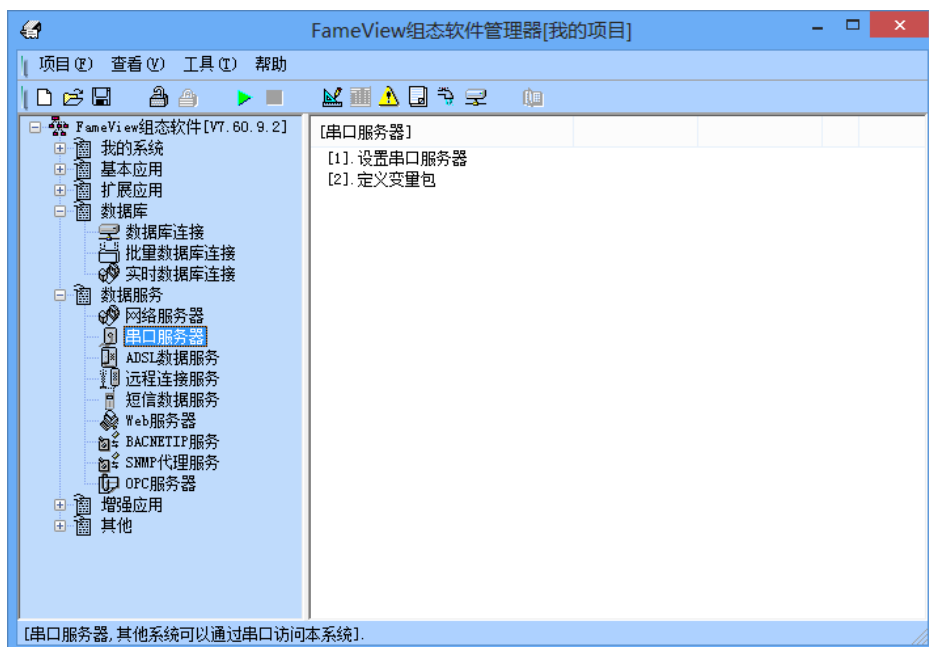
- 选择[我的系统->设置]功能, 执行[启动任务]:



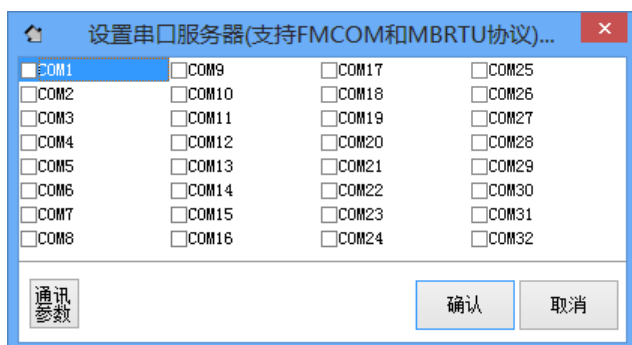
- 选择系统任务中的“串口服务器”;

## 29.2 设置串口服务器

- 选择[数据服务. 串口服务器]功能:



- 执行[设置串口服务器]:



[1]. 最多支持 32 个串口, 选择串口允许被打开进行数据访问;

[2]. 同时支持 FMCOM 和 MODBUS-RTU 通讯协议;

[3]. 多个串口允许设置不同串口参数;

[4]. 支持电话拨号连接串口服务器:

串口被打开时自动发送 3 条 AT 指令, 使串口连接 Modem 能够自动应答:

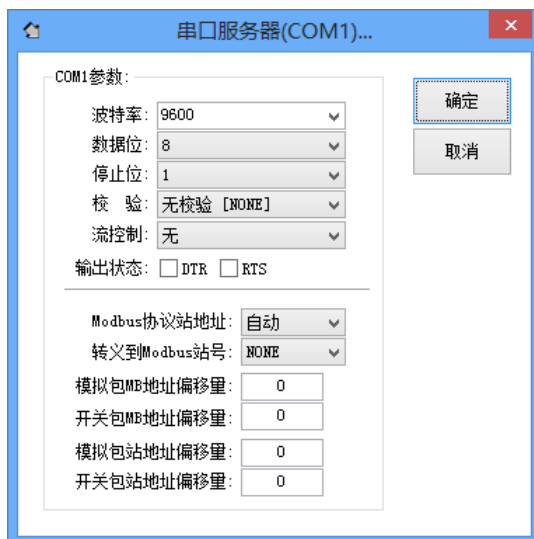
ATE0VQ1M1 - 初始化 Modem

ATS0=1 - 使 Modem 自动应答

AT&W - 保存设置

[5]. 串口服务器应答间隔 30-100 毫秒;

- 执行[通讯参数]按钮或鼠标双击串口名称, 设置串口通讯及 Modbus 协议参数:



[1]. 波特率: 100, 300, 600, 1200, 2400, 4800, 4800, 9600, 19200, 38400, 56000, 57600, ...

[2]. 数据位: 4, 5, 6, 7, 8(建议)

[3]. 停止位: 1, 1.5, 2

[4]. 校验: None, Even, Odd, Mark, Space

[5]. 流控制: No, Xon/Xoff, Hardware

[6]. 自定义 Modbus 协议参数, 内容见 29.6;

### 29.3 定义数据变量包

□ 串口服务器允许被访问的数据类型：

[1]. 设备数据表 (D1-D2000) ；

[2]. AI/AO/AR/VA 模拟变量, DI/DO/DR/VD 开关变量；

服务器设备数据表 (D1-D2000) 允许被客户端直接访问；

AI/AO/AR/VA 变量、DI/DO/DR/VD 变量则需要被打包, 才能被客户端访问；

□ 选择“串口服务器”功能, 执行“定义变量包”任务：

地址	AP - 模拟变量包:	数值[R4]	地址	DP - 开关变量包:	状态[位]
0	VA. %VA1		0.0	VD. %VD1	
1	VA. %VA2		0.1	VD. %VD2	
2	VA. %VA3		0.2	VD. %VD3	
3	VA. %VA4		0.3	VD. %VD4	
4			0.4	VD. %VD5	
5			0.5	VD. %VD6	
6			0.6	VD. %VD7	
7			0.7		
8			1.0		
9			1.1		
10			1.2		
11			1.3		
12			1.4		
13			1.5		
14			1.6		
15			1.7		
16			2.0		
17			2.1		
18			2.2		
19			2.3		
20			2.4		
21			2.5		
22			2.6		
23			2.7		

Excel 工具      保存      取消

[1]. 包含两个表格, 分别定义模拟变量包 (AP) 和开关变量包 (DP) ；

[2]. 模拟变量包 (AP), 最多包含 4096 个 32 位浮点数 (R4) ；

通过索引地址 0-4095 表示, 客户端通过索引地址访问模拟变量包；

[3]. 开关变量包 (DP), 最多包含 512\*8 共 4096 个位变量 (bit) ；

通过索引地址 0.0-0.7、...、511.0-511.7 表示, 客户端通过索引地址访问开关变量包；

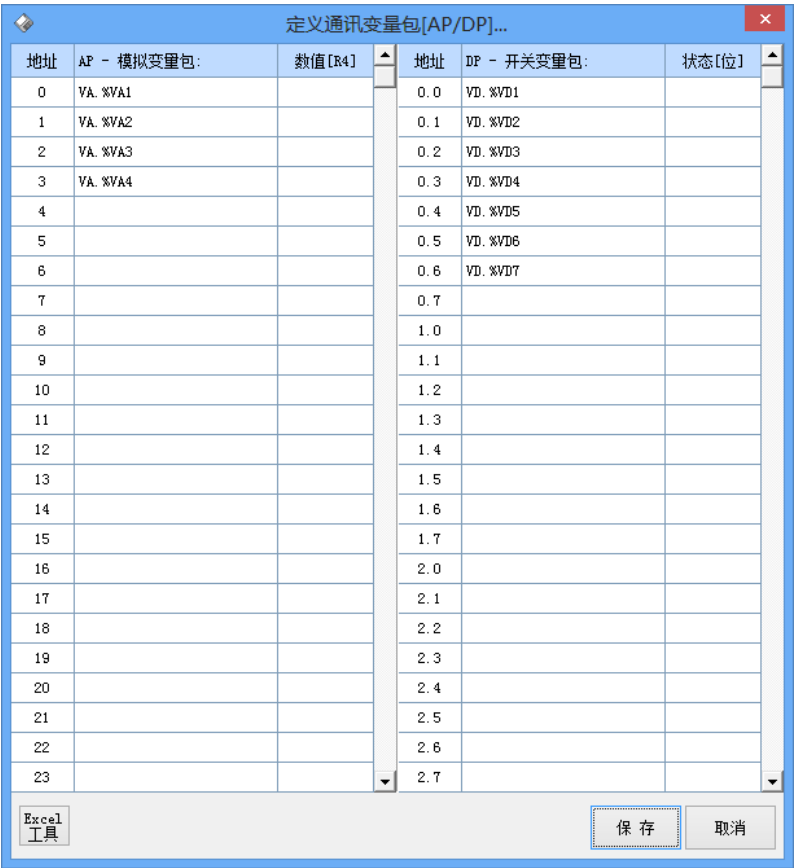
[4]. 变量包中每个索引地址对应运行数据库中某变量；

未对应变量的索引地址, 允许被访问, 但其缺省值/状态总为 0；

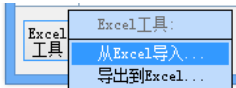
[5]. 鼠标双击变量包索引地址, 从变量列表中连续选择变量直到结束, 按下 Del 键删除某变量；

□ 允许通过 Excel 编辑变量包, 提高组态效率;

[1]. 简单编辑变量包:



[2]. 执行 [Excel 工具] 按钮:



[3]. 执行 [导出到 Excel], 导出变量包到 Excel 文件:

	A	B	C	D	E
1		模拟变量包		开关变量包	
2		VA. %VA1		VD. %VD1	
3		VA. %VA2		VD. %VD2	
4		VA. %VA3		VD. %VD3	
5		VA. %VA4		VD. %VD4	
6				VD. %VD5	
7				VD. %VD6	
8				VD. %VD7	
9					

[4]. 使用 Excel 编辑变量包并保存:

	A	B	C	D	E
1		模拟变量包		开关变量包	
2		VA. %VA1		VD. %VD1	
3		VA. %VA2		VD. %VD2	
4		VA. %VA3		VD. %VD3	
5		VA. %VA4		VD. %VD4	
6		VA. %RAND		VD. %VD5	
7		VA. %X=X+1		VD. %VD6	
8				VD. %VD7	
9				VD. %VD8	

[5]. 执行[从 Excel 导入], 选择导入 Excel 文件名称, 导入变量包内容:

地址	AP - 模拟变量包:	数值[R4]	地址	DP - 开关变量包:	状态[位]
0	VA. %VA1		0.0	VD. %VD1	
1	VA. %VA2		0.1	VD. %VD2	
2	VA. %VA3		0.2	VD. %VD3	
3	VA. %VA4		0.3	VD. %VD4	
4	VA. %RAND		0.4	VD. %VD5	
5	VA. %X=X+1		0.5	VD. %VD6	
6			0.6	VD. %VD7	
7			0.7	VD. %VD8	
8			1.0		
9			1.1		
10			1.2		
11			1.3		
12			1.4		
13			1.5		
14			1.6		
15			1.7		
16			2.0		
17			2.1		
18			2.2		
19			2.3		
20			2.4		
21			2.5		
22			2.6		
23			2.7		

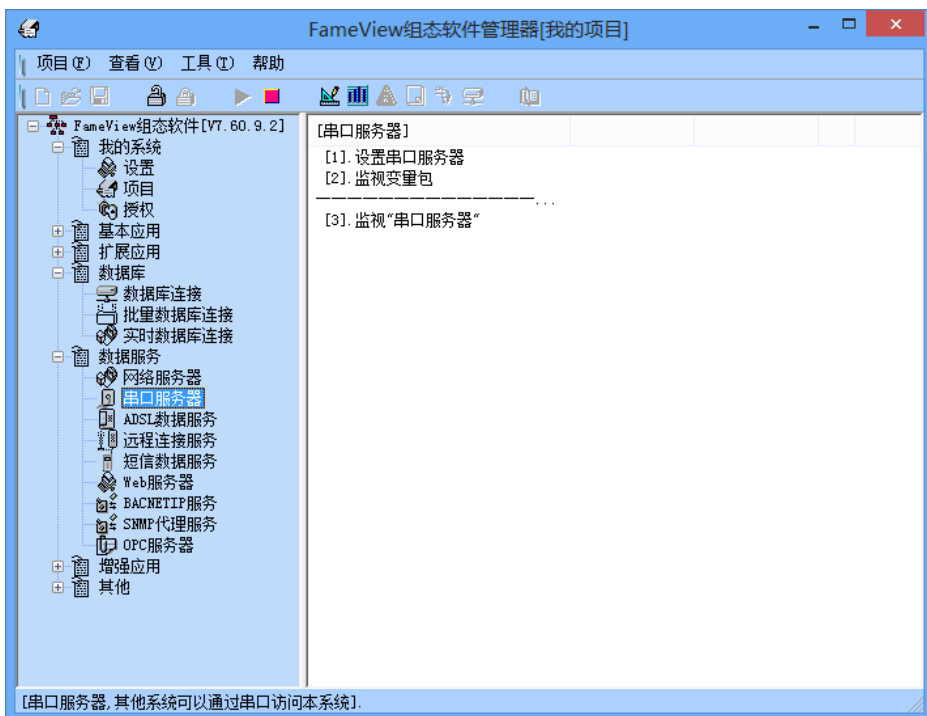
Excel 工具      保存      取消

□ 运行状态打开变量包, 监视索引地址对应的数值和状态;

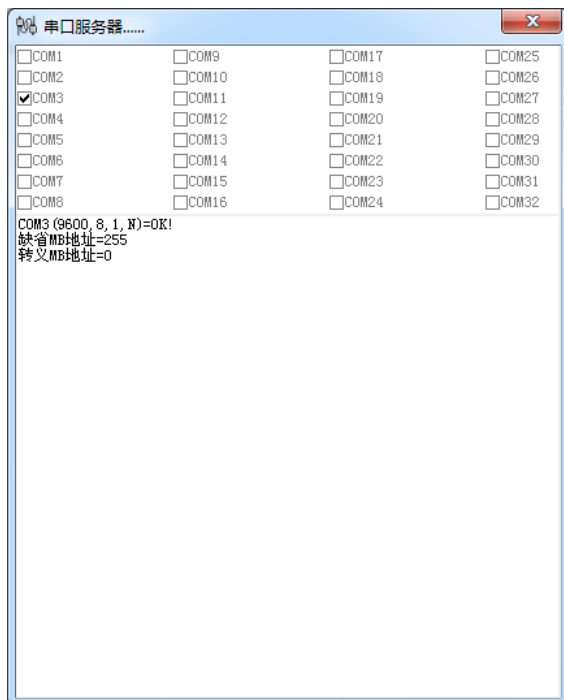
地址	AP - 模拟变量包:	数值[R4]	地址	DP - 开关变量包:	状态[位]
0	VA. %VA1	0	0.0	VD. %VD1	0
1	VA. %VA2	0	0.1	VD. %VD2	1
2	VA. %VA3	0	0.2	VD. %VD3	0
3	VA. %VA4	0	0.3	VD. %VD4	0
4	VA. %RAND	2987.456893	0.4	VD. %VD5	1
5	VA. %X=X+1	284	0.5	VD. %VD6	0
6			0.6	VD. %VD7	0
7			0.7	VD. %VD8	0
8			1.0		
9			1.1		
10			1.2		
11			1.3		
12			1.4		
13			1.5		
14			1.6		
15			1.7		
16			2.0		
17			2.1		
18			2.2		
19			2.3		
20			2.4		
21			2.5		
22			2.6		
23			2.7		

## 29.4 监视串口服务器

- 运行状态, 允许监视服务器工作状态:



- 执行[监视串口服务器]任务:



## 29.5 FCOM 通讯协议

提供简单实用 FCOM 串口协议, 供客户端访问串口服务器数据;

### □ 测试服务器:

客户端发出请求 (16 进制)		
Buffer[0][1]	3E 2A	协议标识
Buffer[2][3]	00 00	功能码: 测试
服务器返回应答 (16 进制)		
Buffer[0][1]	3C	协议标识
Buffer[2][3]	00 00	功能码: 测试

### □ 读取设备号 D1-D1000, 每设备号 1024 字节, 地址表示 0-1023;

客户端发出请求 (16 进制)		
例如: <u>3E 2A 00 01 00 00 00 0A</u> (从设备号 D1 中从字节单元 0 开始, 读 10 个字节)		
Buffer[0][1]	3E 2A	协议标识
Buffer[2][3]	[0001-03E8]	功能码: 读设备号数据 [0001-03E8] 对应 D1-D1000
Buffer[4][5]	开始地址高低字节	0-1023
Buffer[6][7]	字节长度高低字节	1-1024
服务器返回应答 (16 进制)		
例如: <u>3C 2A 00 01 00 0A 00 01 02 03 04 05 06 07 08 09</u>		
Buffer[0][1]	3C 2A	协议标识
Buffer[2][3]	[0001-03E8]	功能码: 读设备号数据 [0001-03E8] 对应 D1-D1000
Buffer[4][5]	字节长度高低字节	1-1024
Buffer[6]...[n]	.....	返回数据

### □ 修改设备号 D1-D1000, 每设备 1024 字节, 地址表示 0-1023;

客户端发出请求 (16 进制)		
例如: <u>3E 2A 03 E9 00 01 00 02 01 02</u> (修改设备号 D1 中, 从字节 1 开始的 2 个字节)		
Buffer[0][1]	3E 2A	协议标识
Buffer[2][3]	[03E9-07D0]	功能码: 修改设备号数据 [03E9-07D0] 对应 D1-1000
Buffer[3][4]	开始地址高低字节	0-1023
Buffer[5][6]	字节长度高低字节	1-1024
Buffer[7]...[n]	.....	修改数据
服务器返回应答 (16 进制)		
例如: <u>3C 2A 03 E9</u>		
Buffer[0][1]	3C 2A	协议标识
Buffer[2][3]	[03E9-07D0]	功能码: 修改设备号数据 [03E9-07D0] 对应 D1-1000



## □ 读取模拟变量包 (AP)

客户端发出请求(16 进制)		
例如: <u>3E 2A 07 D1 00 02 00 02</u>		
(读 2 个模拟变量:AP[2]、AP[3])		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2][3]	2001 (07D1)	功能码=2001 (07D1)
Buffer[4]	开始索引号高字节	0-4095
Buffer[5]	开始索引号低字节	
Buffer[6]	变量数量高字节	1-4096
Buffer[7]	变量数量低字节	
服务器返回应答(16 进制)		
例如: <u>3C 2A 07 D1 00 08 00 00 00 00 00 00 00 00</u>		
Buffer[0]	3C	协议标识
Buffer[1]	2A	
Buffer[2-3]	2001 (07D1)	功能码=2001 (07D1)
Buffer[4]	字节长度高字节	(1-4096)*4
Buffer[5]	字节长度低字节	
Buffer[6]...[n]	返回数据	浮点数格式, 每 4 个字节为 1 个变量

## □ 读取开关变量包 (DP)

客户端发出请求(16 进制)		
例如: <u>3E 2A 07 D2 00 02 00 02</u>		
(读 2 个字节开关变量:DP[2.0..7]、DP[3.0..7])		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2-3]	2002 (07D2)	功能码=2002 (07D2)
Buffer[4]	开始字节高字节	0-511
Buffer[5]	开始字节低字节	
Buffer[6]	字节长度高字节	1-512
Buffer[7]	字节长度低字节	
服务器返回应答(16 进制)		
例如: <u>3C 2A 07 D2 00 02 01 02</u>		
Buffer[0]	3C	协议标识
Buffer[1]	2A	
Buffer[2-3]	2002 (07D2)	功能码=2002 (07D2)
Buffer[4]	字节长度高字节	1-512
Buffer[5]	字节长度低字节	
Buffer[6][n]	返回数据	字节格式

## □ 修改模拟变量包 (AP)

客户端发出请求 (16 进制)		
例如: <u>3E</u> <u>2A</u> <u>07 DB</u> <u>00 08</u> <u>00 08</u> <u>00 00 F6 42</u> <u>00 00 E4 43</u>		
(修改 AP[2]=123、AP[3]=456)		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2][3]	2011 (07DB)	功能码=2011 (07DB)
Buffer[4]	开始字节高字节	[0-4095]*4
Buffer[5]	开始字节低字节	
Buffer[6]	字节长度高字节	(1-4096)*4
Buffer[7]	字节长度低字节	
Buffer[8]...[n]	修改数据	浮点数格式
服务器返回应答 (16 进制)		
例如: <u>3C</u> <u>2A</u> <u>07 DB</u>		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2][3]	2011 (07DB)	功能码=2011 (07DB)

## □ 修改开关变量包 (DP)

客户端发出请求 (16 进制)		
例如: <u>3E</u> <u>2A</u> <u>07 DC</u> <u>00 02</u> <u>00 02</u> <u>02 03</u>		
(修改 DP[2.0..7]=02、DP[3.0..7]=03)		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2][3]	2012 (07DC)	功能码=2012 (07DC)
Buffer[4]	开始字节高字节	0-511
Buffer[5]	开始字节低字节	
Buffer[6]	字节长度高字节	1-512
Buffer[7]	字节长度低字节	
Buffer[8]...[n]	修改数据	字节格式
服务器返回应答 (16 进制)		
例如: <u>3C</u> <u>2A</u> <u>07 DC</u>		
Buffer[0]	3E	协议标识
Buffer[1]	2A	
Buffer[2][3]	2012 (07DC)	功能码=2012 (07DC)

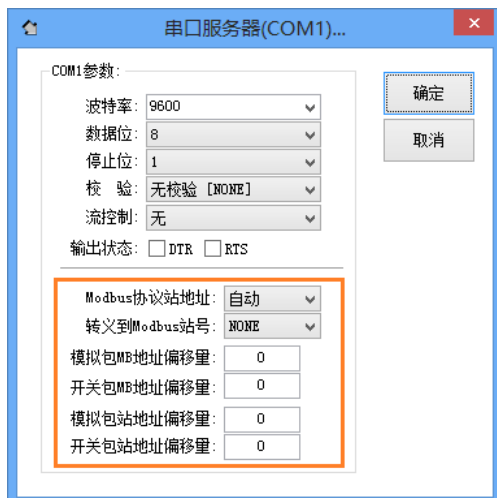
## 29.6 MODBUS (RTU) 协议

- 客户端程序通过 MODBUS RTU 协议, 访问串口服务器数据;
  - [1]. 读写串口服务器中模拟变量包 (AP) 和开关变量包 (DP);
  - [2]. 根据站地址区分数据类型及处理方式;
- MODBUS 与串口服务器数据对应关系:

MODBUS 协议			串口服务器			
站地址	功能码	数据地址	数据类型	地址	数据单位	
寄存器或模拟输入, 访问模拟包 (AP), 以字为单位反高低字节处理, R4 (2, 1, 4, 3)						
201[C9] 1-10	03/04/10	400001-408192 300001-308192	模拟变量包 (AP)	0-4095	浮点 (R4)	
寄存器或模拟输入, 访问模拟包 (AP), 无处理, R4 (1, 2, 3, 4)						
211[D3] 11-20	03/04/10	400001-408192 300001-308192	模拟变量包 (AP)	0-4095	浮点 (R4)	
寄存器或模拟输入, 访问模拟包 (AP), 以双字为单位反高低字节处理, R4 (4, 3, 2, 1)						
221[DD] 101-110	03/04/10	400001-408192 300001-308192	模拟变量包 (AP)	0-4095	浮点 (R4)	
继电器或开关输入, 访问开关包 (DP), 开始地址须 $m*8+1$ , 长度须 $n*8$						
1-255	01/02/05/0F	000001-004096 100001-104096	开关变量包 (DP)	0-511	字节	
寄存器或模拟输入, 访问模拟包 (AP), 反高低字节处理, I2 (h, 1)						
203[CB] 21-30	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*1
204[CC] 41-50	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*10
205[CD] 61-70	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*100
206[CE] 81-90	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*1000
通过寄存器或模拟输入, 访问模拟包 (AP), 无处理, I2 (1, h)						
213[D5] 31-40	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*1
214[D6] 51-60	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*10
215[D7] 71-80	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*100
216[D8] 91-100	03/04/10/06	400001-404096 300001-304096	模拟变量包 (AP)	0-4095	字	*1000

寄存器(4xxxxx), 按字访问设备设备数据表 D1-2000, 不反高低字节, I2(x1, x2) 不支持跨设备号访问, m=设备号, n=字单元号;				
231[E7]	03, 06, 10	400001-451200	D1-100	$(m-1)*512+n+1$
232[E8]	03, 06, 10	400001-451200	D101-200	$(m-101)*512+n+1$
233[E9]	03, 06, 10	400001-451200	D201-300	$(m-201)*512+n+1$
234[EA]	03, 06, 10	400001-451200	D301-400	$(m-301)*512+n+1$
235[EB]	03, 06, 10	400001-451200	D401-500	$(m-401)*512+n+1$
236[EC]	03, 06, 10	400001-451200	D501-600	$(m-501)*512+n+1$
237[ED]	03, 06, 10	400001-451200	D601-700	$(m-601)*512+n+1$
238[EE]	03, 06, 10	400001-451200	D701-800	$(m-701)*512+n+1$
239[EF]	03, 06, 10	400001-451200	D801-900	$(m-801)*512+n+1$
240[F0]	03, 06, 10	400001-451200	D901-1000	$(m-901)*512+n+1$
241[F1]	03, 06, 10	400001-451200	D1001-1100	$(m-1001)*512+n+1$
242[F2]	03, 06, 10	400001-451200	D1101-1200	$(m-1101)*512+n+1$
243[F3]	03, 06, 10	400001-451200	D1201-1300	$(m-1201)*512+n+1$
244[F4]	03, 06, 10	400001-451200	D1301-1400	$(m-1301)*512+n+1$
245[F5]	03, 06, 10	400001-451200	D1401-1500	$(m-1401)*512+n+1$
246[F6]	03, 06, 10	400001-451200	D1501-1600	$(m-1501)*512+n+1$
247[F7]	03, 06, 10	400001-451200	D1601-1700	$(m-1601)*512+n+1$
248[F8]	03, 06, 10	400001-451200	D1701-1800	$(m-1701)*512+n+1$
249[F9]	03, 06, 10	400001-451200	D1801-1900	$(m-1801)*512+n+1$
250[FA]	03, 06, 10	400001-451200	D1901-2000	$(m-1901)*512+n+1$

- 允许自定义 Modbus 参数, 转义站地址:



[1]. Modbus 协议站地址 (stnAddr)

stnAddr=自动, 默认方式, 客户端以任意地址访问服务器;

stnAddr=1..254, 客户端只能以某固定地址访问服务器, 否则服务器不予应答;

[2]. 转义到 Modbus 站号 (actAddr)

actAddr=None, 默认方式, 解析 stnAddr 访问其对应数据类型;

actAddr=1..250, 忽略 stnAddr, 解析 actAddr 访问其对应数据类型;

[3]. 模拟包 MB 地址偏移量 (m1)

客户端请求寄存器或模拟包起始地址 startAddr1

$startAddr1 = startAddr1 + m1$

[4]. 开关包 MB 地址偏移量 (m2)

客户端请求继电器或开关起始地址 startAddr2

$startAddr2 = startAddr2 + m2$

[5]. 模拟包站地址偏移量 (n1)

$startAddr1 = startAddr1 + (stnAddr - 1) * n1$

[6]. 开关包站地址偏移量 (n2)

$startAddr2 = startAddr2 + (stnAddr - 1) * n2$

例 1 (站地址转义): 客户端通过站地址 30, 访问服务器中站地址 201 对应数据;

Modbus 协议站地址:	30
转义到 Modbus 站号:	201

例 2: 客户端通过寄存器 400101, 访问服务器变量包 AP[0];

AP[0] 缺省 Modbus 寄存器地址为 400001, 模拟包 Modbus 地址须偏移 (n-100);

模拟包 MB 地址偏移量: -100

例 3: 客户端通过寄存器 400001, 访问服务器变量包 AP[100];

AP[100] 缺省 Modbus 寄存器地址为 400201, 模拟包 Modbus 地址须偏移 (n+200);

模拟包 MB 地址偏移量: 200

例 4：客户端根据站地址分区访问变量包；

站地址	Modbus开始地址	模拟变量包 (AP)	开关变量包 (DP)
1	400001	100001	0, 1, ..., 9
2	400001	100001	10, 11, ..., 19
...	...	...	...
N	400001	100001	(N-1)*A, ..., N*A-1

N=站地址, A=模拟包站地址偏移量, B=开关包站地址偏移量

Modbus协议站地址

自动

转义到Modbus站号

201

模拟包MB地址偏移量:

0

开关包MB地址偏移量:

0

模拟包站地址偏移量:

20

开关包站地址偏移量:

16

- 测试串口服务器MODBUS-RTU协议：
- 读取第 1 个模拟变量包数据, 站号 201 (C9), 功能码 03;
- C9 03 00 00 00 02 D4 43
- 返回数据格式:
- C9 03 04 xx xx xx xx yy yy