

测试人：李朋

测试时间：2017 年 8 月 22 日星期二

硬件配置：

1. Beckhoff 控制器 CX5010—0112 winCE 系统；
2. 以 ModScan32 模拟触摸屏发送和接收数据。
3. TC2 软件（注意 TC2 与 TC3 操作有很大区别）

准备：

1. 安装 TwinCAT_Modbus_Server_CE 插件。
2. 安装完成后，在路径：C:\TwinCAT\CE\TCModbusTCP\Install 下复制 TcModbusTcpSvrCe.I586 到倍福控制器的 CF 卡中。
3. 将控制器连接显示屏或者远程接管控制器（CERhost），双击 TcModbusTcpSvrCe.I586 文件，自动安装。
4. 在 TC2 PLC 中定义如下变量：

`mb0_10 AT %MB0 :ARRAY[1..1000] OF WORD;`

`Ib0_10 AT %IB0 :ARRAY[1..1000] OF WORD;`

`Qb0_10 AT %QB0 :ARRAY[1..1000] OF WORD;`

`mb_Input_Coils : ARRAY [0..255] OF BOOL;`

`mb_Output_Coils : ARRAY [0..255] OF BOOL;`

`mb_Input_Registers : ARRAY [0..255] OF WORD;`

`mb_Output_Registers : ARRAY [0..255] OF WORD;`

两种颜色变量分别代表不同的地址，但都可以实现 Modbus TCP 通信。
编译，下载，运行。

- 5 打开 ModScan32 软件，设定 IP 地址为控制器的 IP 地址，连接成功后监测。

数据测试：

Mapping between Modbus and ADS

In Modbus, the following four addressing areas are defined:

Modbus areas	Data type	Access
Digital inputs (discrete inputs)	1 bit	read only
Digital outputs (coils)	1 bit	read and write
Input register	16 bit	read only
Output register	16 bit	read and write

The individual **areas** can be addressed with 0 - 0xFFFF. The **ADS** server maps these addresses to the individual **ADS areas**. The standard settings are shown in the following table:

Modbus areas	Modbus address	ADS area	
Digital inputs	0x0000 - 0x7FFF	Index group	Index offset
		0xF021 - process image of the physical inputs (bit access)	0x0
	0x8000 - 0x80FF	Name of the variables in the PLC program	Data type
		.mb_Input_Coils	ARRAY [0..255] OF BOOL
Digital outputs (coils)	0x0000 - 0x7FFF	Index group	Index offset
		0xF031 - process image of the physical outputs (bit access)	0x0
	0x8000 - 0x80FF	Name of the variables in the PLC program	Data type
		.mb_Output_Coils	ARRAY [0..255] OF BOOL
Input registers	0x0000 - 0x7FFF	Index group	Index offset
		0xF020 - process image of the physical inputs	0x0
	0x8000 - 0x80FF	Name of the variables in the PLC program	Data type
		.mb_Input_Registers	ARRAY [0..255] OF WORD
Output registers	0x0000 - 0x2FFF	Index group	Index offset
		0xF030 - process image of the physical outputs	0x0
	0x3000 - 0x5FFF	0x4020 - PLC memory area	0x0
	0x6000 - 0x7FFF	0x4040 - PLC data area	0x0
	0x8000 - 0x80FF	Name of the variables in the PLC program	Data type
		.mb_Output_Registers	ARRAY [0..255] OF WORD

首先测试自定义变量的数据:

```
mb_Input_Coils      : ARRAY [0..255] OF BOOL;
mb_Output_Coils    : ARRAY [0..255] OF BOOL;
mb_Input_Registers : ARRAY [0..255] OF WORD;
mb_Output_Registers : ARRAY [0..255] OF WORD;
```

由上面表格可知，自定义变量的数据地址自动偏移 0x8000 (32768) +1

BOOL 量输入 (只读)

ModSca2 configuration for digital inputs:

- Address: 32769
- Device Id: 1
- MODBUS Point Type: 02: INPUT STATUS
- Length: 100

Address list (Address <Value>):

- 132769: <1>
- 132770: <0>
- 132771: <0>
- 132772: <0>
- 132773: <0>
- 132774: <0>
- 132775: <0>
- 132776: <0>
- 132777: <0>
- 132778: <0>
- 132779: <0>
- 132780: <0>
- 132781: <0>
- 132782: <0>
- 132783: <0>
- 132784: <0>
- 132785: <0>
- 132786: <0>
- 132787: <0>
- 132788: <0>
- 132789: <0>
- 132790: <0>
- 132791: <0>
- 132792: <0>
- 132793: <0>
- 132794: <0>
- 132795: <0>
- 132796: <0>
- 132797: <0>
- 132798: <0>
- 132799: <0>

BOOL 量输出 (读/写)

ModSca2 configuration for digital outputs:

- Address: 32769
- Device Id: 1
- MODBUS Point Type: 01: COIL STATUS
- Length: 100

Address list (Address <Value>):

- 032769: <1> 03
- 032770: <0> 03
- 032771: <1> 03
- 032772: <0> 03
- 032773: <0> 03
- 032774: <0> 03
- 032775: <0> 03

Write Coil dialog box details:

- Node: 1
- Address: 32772
- Value: OFF

实数输入（只读）

Left pane (mb_Input_Regist...):

- mb_Input_Re... = 37
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 46
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb_Input_Re... = 0
- mb Input Re... = 0

Right pane (ModSca2):

Address: 32769 Device Id: 1

Length: 100 MODBUS Point Type: 04: INPUT REGISTER

Data Table:

332769:	<00037>	332776:	<00000>	332783:	<00000>
332770:	<00000>	332777:	<00000>	332784:	<00000>
332771:	<00000>	332778:	<00000>	332785:	<00000>
332772:	<00046>	332779:	<00000>	332786:	<00000>

实数输出（读/写）

Left pane (mb_Output_Regi...):

- mb_Output_R... = 17
- mb_Output_R... = 69
- mb_Output_R... = 0
- mb_Output_R... = 22
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0
- mb_Output_R... = 0

Right pane (ModSca2):

Address: 32769 Device Id: 1

Length: 100 MODBUS Point Type: 03: HOLDING REGISTER

Write Register Dialog:

Node: 1

Address: 32770

Value: 69

Buttons: Update, Cancel

再测试定义变量地址:

Ib0_10 AT %IB0 :ARRAY[1..9] OF BOOL;

Ib0_11 AT %IB10 :ARRAY[1..100] OF WORD;

Qb0_10 AT %QB0 :ARRAY[1..9] OF BOOL;

Qb0_11 AT %QB10 :ARRAY[1..100] OF WORD;

请注意倍福 PLC 中是用 1 个 Byte 来处理 bool 变量的。SO:

Bool 量输入（只读）:

Left pane (mb0_10 (%MB0), Ib0_10 (%IB0)):

- Ib0_10[1] = TRUE
- Ib0_10[2] = TRUE
- Ib0_10[3] = FALSE
- Ib0_10[4] = FALSE
- Ib0_10[5] = FALSE
- Ib0_10[6] = FALSE
- Ib0_10[7] = FALSE
- Ib0_10[8] = FALSE
- Ib0_10[9] = FALSE

Right pane (ModSca3):

Address: 0001 Device Id: 1

Length: 100 MODBUS Point Type: 02: INPUT STATUS

Data Table:

10001:	<1>	10010:	<0>	10019:	<0>	10028:	<0>
10002:	<0>	10011:	<0>	10020:	<0>	10029:	<0>
10003:	<0>	10012:	<0>	10021:	<0>	10030:	<0>
10004:	<0>	10013:	<0>	10022:	<0>	10031:	<0>
10005:	<0>	10014:	<0>	10023:	<0>	10032:	<0>
10006:	<0>	10015:	<0>	10024:	<0>	10033:	<0>
10007:	<0>	10016:	<0>	10025:	<0>	10034:	<0>
10008:	<0>	10017:	<0>	10026:	<0>	10035:	<0>
10009:	<1>	10018:	<0>	10027:	<0>	10036:	<0>

BOOL 量输出 (读/写):

ModSca3 configuration window showing:

- Address: 0001, Device Id: 1, MODBUS Point Type: 01: COIL STATUS
- Length: 100

Boolean Output List:

- Ib0_10[1] = TRUE
- Ib0_10[2] = TRUE
- Ib0_10[3] = FALSE
- Ib0_10[4] = FALSE
- Ib0_10[5] = FALSE
- Ib0_10[6] = FALSE
- Ib0_10[7] = FALSE
- Ib0_10[8] = FALSE
- Ib0_10[9] = FALSE
- Qb0_10[1] = TRUE
- Qb0_10[2] = TRUE
- Qb0_10[3] = TRUE
- Qb0_10[4] = FALSE
- Qb0_10[5] = FALSE
- Qb0_10[6] = FALSE
- Qb0_10[7] = FALSE
- Qb0_10[8] = FALSE
- Qb0_10[9] = FALSE

Write Coil Dialog Box:

- Node: 1
- Address: 17
- Value: Off On

实数输入 (只读):

ModSca3 configuration window showing:

- Address: 0001, Device Id: 1, MODBUS Point Type: 04: INPUT REGISTER
- Length: 100

Real Number Input List:

- Ib0_10[1] = TRUE
- Ib0_10[2] = TRUE
- Ib0_10[3] = FALSE
- Ib0_10[4] = FALSE
- Ib0_10[5] = FALSE
- Ib0_10[6] = FALSE
- Ib0_10[7] = FALSE
- Ib0_10[8] = FALSE
- Ib0_10[9] = FALSE
- Qb0_11[1] = 37
- Qb0_11[2] = 0
- Qb0_11[3] = 0
- Qb0_11[4] = 0
- Qb0_11[5] = 0
- Qb0_11[6] = 0
- Qb0_11[7] = 0
- Qb0_11[8] = 0
- Qb0_11[9] = 0

Main Configuration Window Data Table:

30001: <00257>	30010: <00000>	30019: <00000>	30028: <00000>
30002: <00000>	30011: <00000>	30020: <00000>	30029: <00000>
30003: <00000>	30012: <00000>	30021: <00000>	30030: <00000>
30004: <00000>	30013: <00000>	30022: <00000>	30031: <00000>
30005: <00000>	30014: <00000>	30023: <00000>	30032: <00000>
30006: <00037>	30015: <00000>	30024: <00000>	30033: <00000>

注意: 30001-30005 倍前面定义的 Bool 输入空间占用。

实数输入 (读/写)

ModSca3 configuration window showing:

- Address: 0001, Device Id: 1, MODBUS Point Type: 03: HOLDING REGISTER
- Length: 100

Real Number Input List:

- Qb0_11[1] = 35
- Qb0_11[2] = 29
- Qb0_11[3] = 0
- Qb0_11[4] = 0
- Qb0_11[5] = 0
- Qb0_11[6] = 0
- Qb0_11[7] = 0
- Qb0_11[8] = 0
- Qb0_11[9] = 0
- Qb0_11[10] = 0
- Qb0_11[11] = 0

Write Register Dialog Box:

- Node: 1
- Address: 7
- Value: 29