

禾川 Q 系列 Modbus TCP 功能简介

Product Function Instruction

 部门：培训与资料开发部

浙江禾川科技股份有限公司

产 品 类 型	PAC	产 品 型 号	HCQ1-1300-D2 (v3.30)	保密等级	<input checked="" type="radio"/> 公开 <input type="radio"/> 内部分享 <input type="radio"/> 保密
修 订	王跃	作 者	沈静	文档编号	
				发布日期	2021/12/10

本文档使用硬件设备和软件工具

- 禾川 HCQ1-1300-D2 (v3.30)
- Q 系列上位编程软件 CODESYS V3.5

适用版本

- 无版本限制

文档更新和发布状态：

发布日期	版本	更新内容	发布状态
2020 年 5 月 12 日	V1.0	Q1 Modbus TCP 功能应用	已发布
2021 年 6 月 1 日	V2.0	v3.30 版本 Q1 Modbus TCP 功能应用	已发布
2021 年 12 月 2 日	V2.1	增加西门子 S7-1500 作为主从站的使用说明	已发布

免责声明：

我们对文档内容都进行了测试与检查，但可能仍有些差错，请您谅解。如果您对本文档有个人的意见或建议，欢迎发送邮件联系作者：400@hcfa.cn。

浙江禾川科技股份有限公司

电话：0570- 7117888

地址：浙江省龙游县工业园阜财路 9 号

地址：杭州市余杭区五常街道文一西路 1001 号 D 幢 4 楼

杭州研发中心

技术支持热线：400 126 969

技术支持邮箱：400@hcfa.cn

目录

1. 软硬件版本	1
1.1 硬件	1
1.2 软件	1
2. 设备连接及使用	1
2.1 设备连接	1
2.2 新建工程	1
2.3 通讯设置	3
2.4 Modbus TCP 主站功能 (Q1 作主站, 客户端)	4
2.4.1 添加主从站	4
2.4.2 配置从站	6
2.4.3 通讯变量配置	8
2.4.4 主站功能调试	8
2.4.5 Q1 做主站 (客户端) 西门子 S7-1500 做从站	10
2.5 Modbus TCP 从站功能 (Q1 作从站, 服务器)	12
2.5.1 添加从站	12
2.5.2 配置从站	12
2.5.3 通讯变量配置	13
2.5.4 从站功能调试	13
2.5.5 Q1 做从站 (服务器) 西门子 S7-1500 做主站	15
附录 1: 描述文件安装	19
附录 2: Modbus TCP 数据报文结构	22

1. 软硬件版本

1.1 硬件

上位控制器：禾川 HCQ1-1300-D2 版本：v3.30（查看当前使用 Q1 版本可参考 2.3 通讯设置步骤）

1.2 软件

PLC 编程软件：CODESYS 版本：V3.5 SP14

描述文件：HCQ1 Pack - Ver0.0.0.6 - (3.30.00.05) .package

描述文件下载地址：<http://class.hcfa.cn/course/view.php?id=66>

2. 设备连接及使用

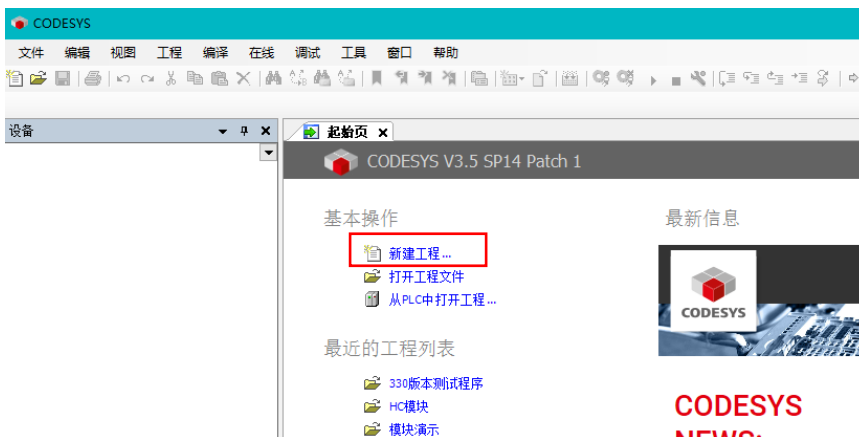
2.1 设备连接

本次实验使用的是 HCQ1-1300-D2 控制器，请按照下图拓扑结构连接测试平台（若使用的是其他 Q 系列产品，连接支持 Modbus TCP 协议的端口即可）。

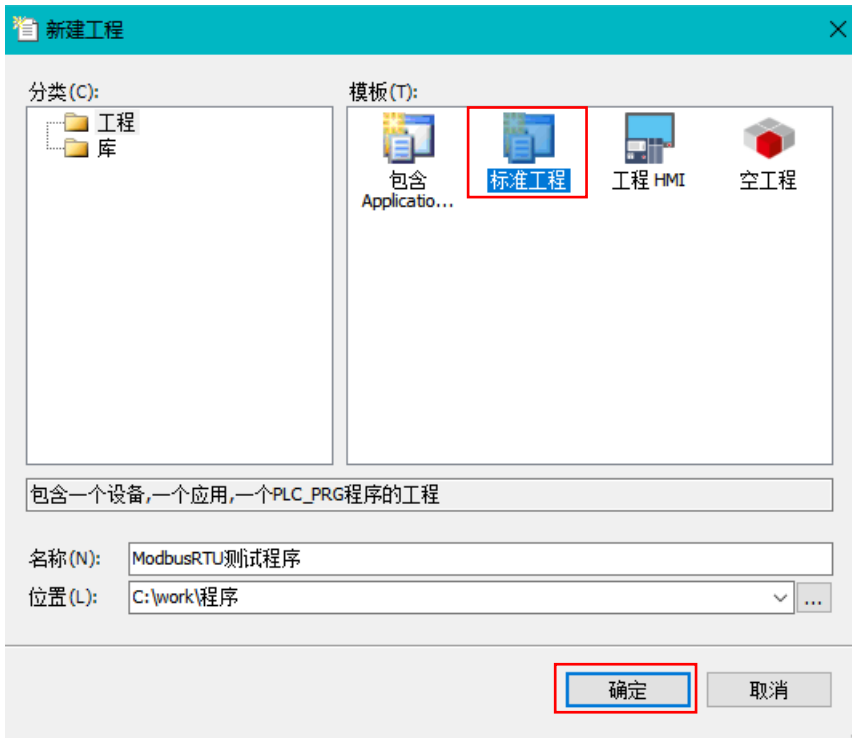


2.2 新建工程

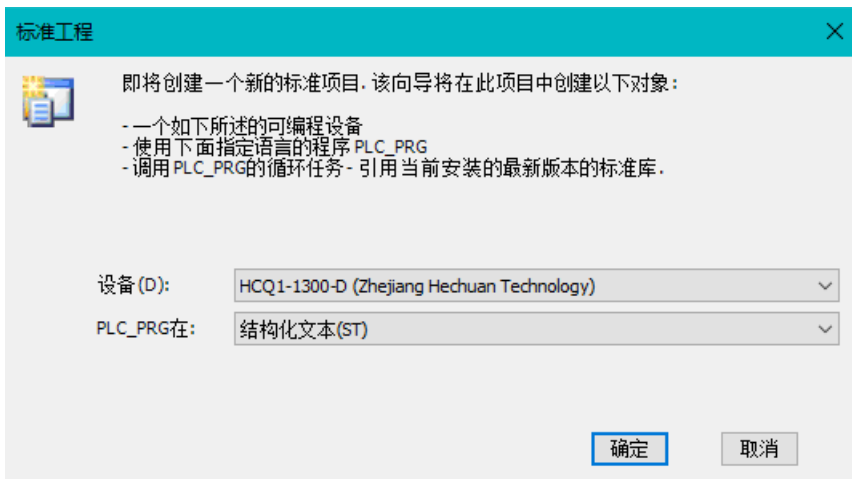
双击打开软件 CODESYS V3.5 SP14，点击【新建工程】。



选择【标准工程】，用户可在此处修改文件名称和设置文件存储地址，完成后点击【确定】。

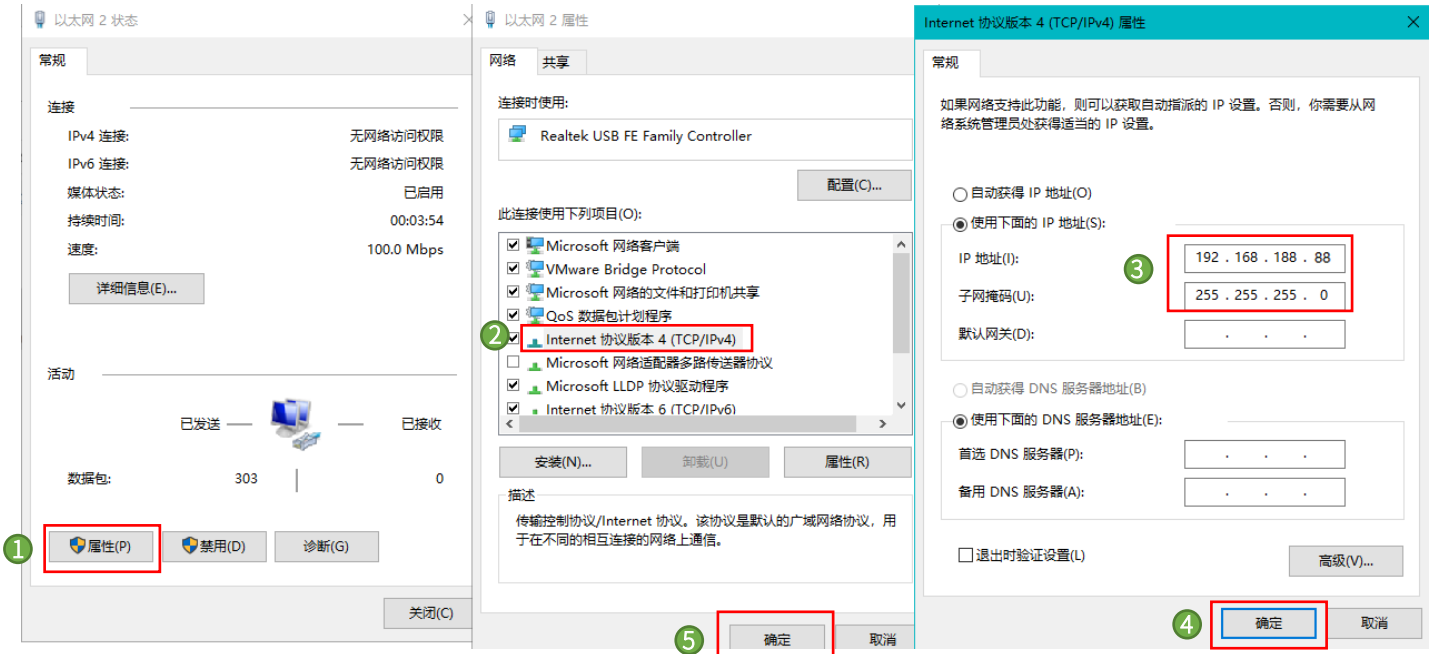


在弹出窗口【设备】栏中下拉选择编程平台为【HCQ1-1300-D】，设置编程语言为【结构化文本（ST）】，点击【确定】，工程新建完成(这一步需要保证 PC 已安装 Q1 描述文件，描述文件的安装方法见 [附录 1](#))。

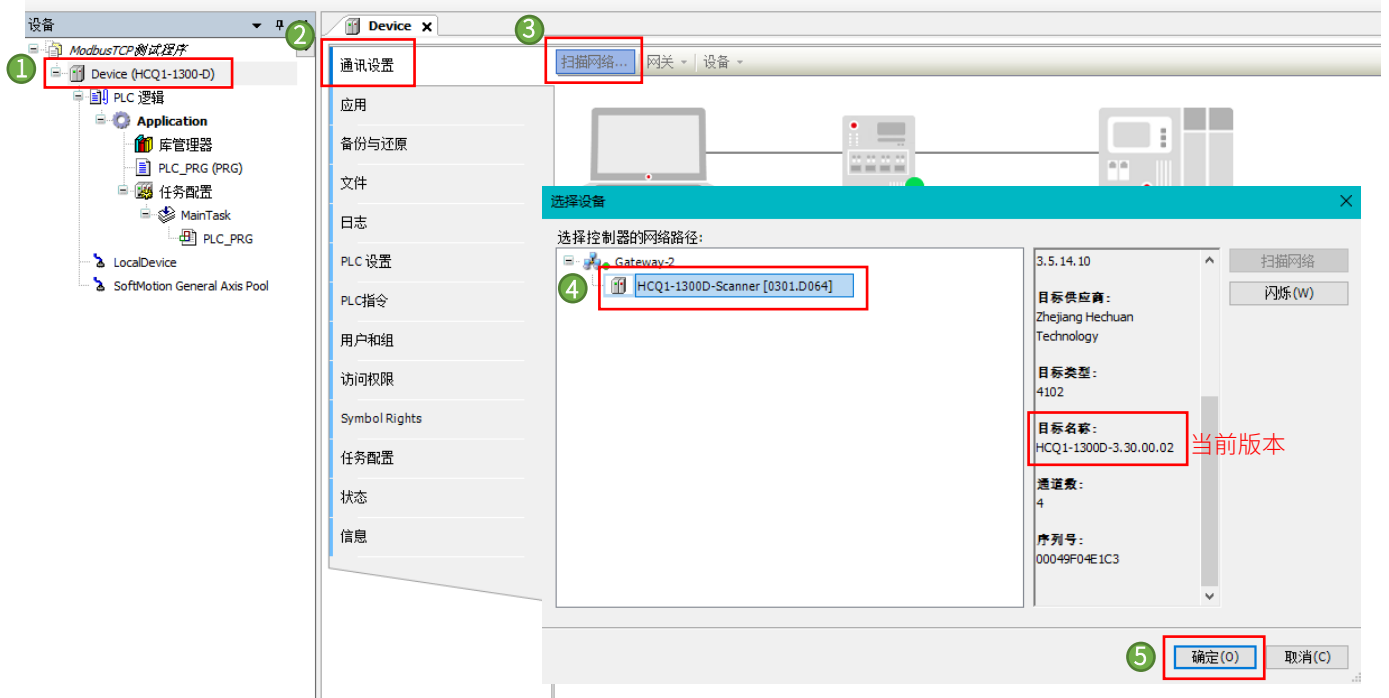


2.3 通讯设置

Q1 的 Port1 默认 IP 地址为 **192.168.188.100**，Port2 的默认 IP 地址为 **192.168.88.100**，本次实验与上位机连接的 Port1 口，需打开以太网设置，点击【属性】→【Internet 协议版本 4 (TCP/IPv4)】→修改上位机 IP 地址，使其与 Q1 Port1 的 IP 地址在同一网段（此处设置的 IP 地址不可与 Q1 Port 口的 IP 地址完全一致），最后点击【确定】。



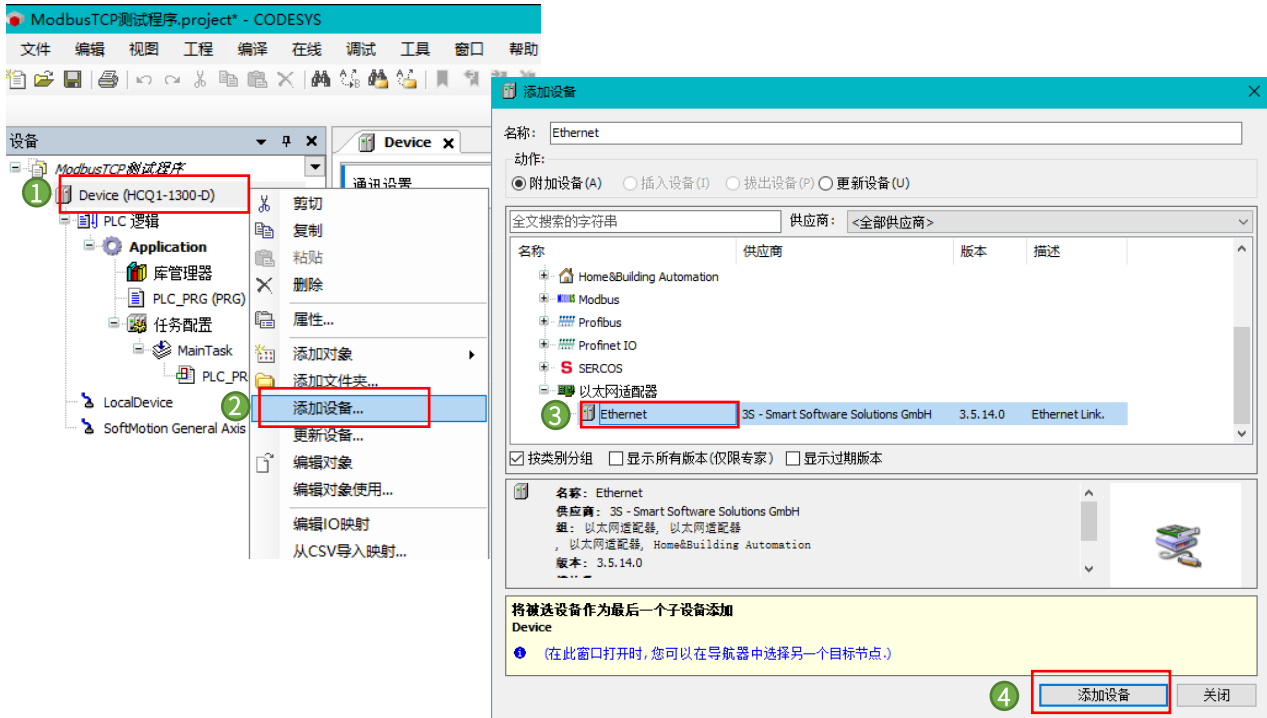
回到软件内，双击左侧树形菜单【Device】，在弹出页面中点击【通讯设置】，点击左上角【扫描网络】，选择扫描出来的 HCQ1-1300-D，下拉可查看当前 Q1 的版本，最后点击【确定】，建立通讯。



2.4 Modbus TCP 主站功能 (Q1 作主站, 客户端)

2.4.1 添加主从站

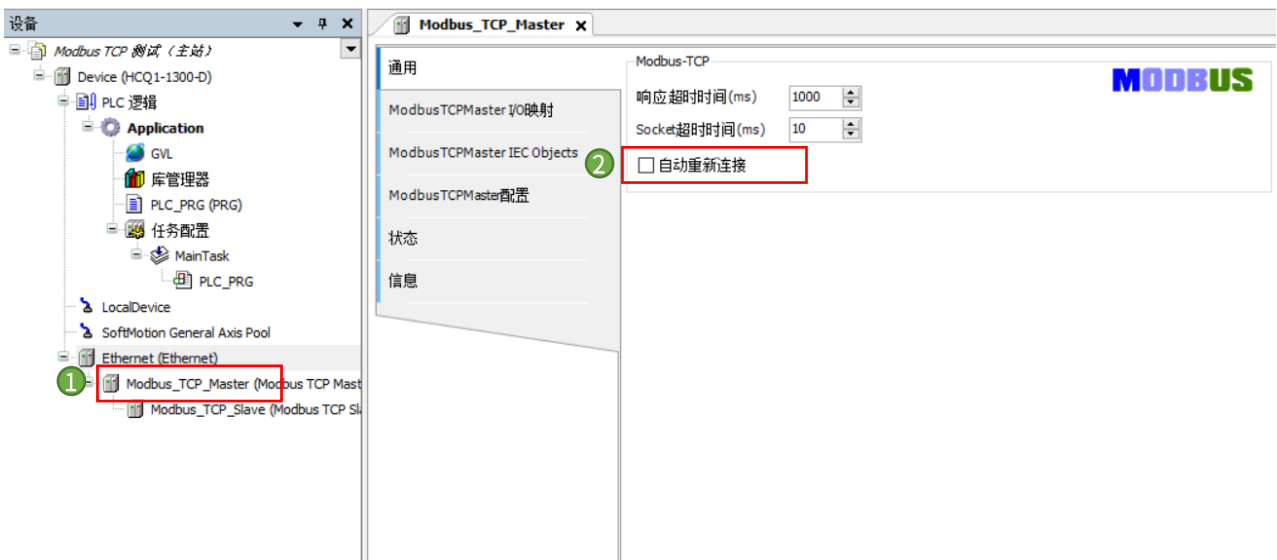
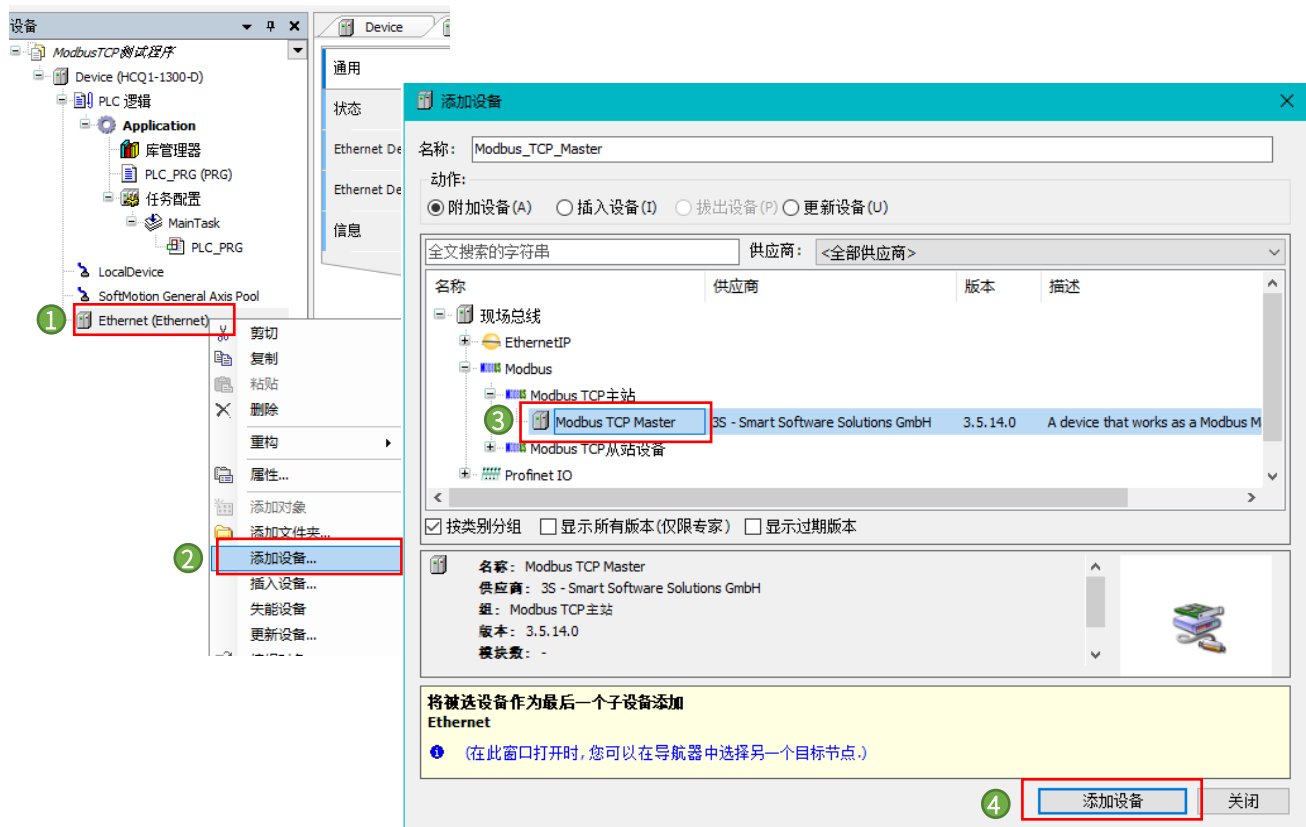
右击左侧树型菜单【Device】→选择【添加设备】，在弹出对话框中下拉选择【以太网适配器】下的【Ethernet】，最后点击【添加设备】。



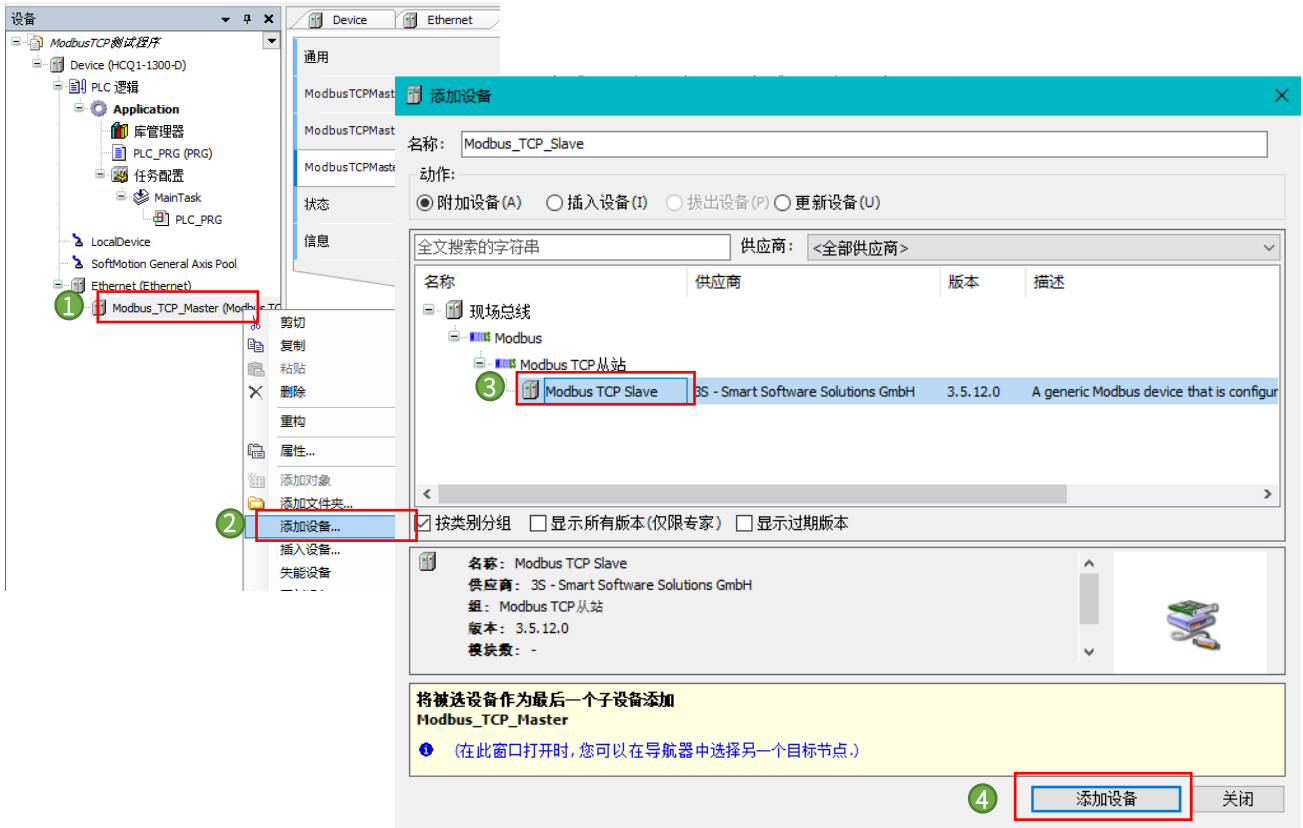
双击添加的【Ethernet】，在右侧通用界面中点击接口右侧按钮，选择eth0（对应Q1的Port1，请根据实际连接的Port口选择），最后点击【确认】。



确定后左侧设备树中会出现【Ethernet】，右击【Ethernet】选择【添加设备】，在弹出对话框中选择【Modbus】→【ModbusTCP 主站】→【ModbusTCPMaster】，最后点击【确定】。双击【Modbus_TCP_Master】，在【通用】选项卡下勾选【自动重新连接】防止断电重启后通讯不连接。

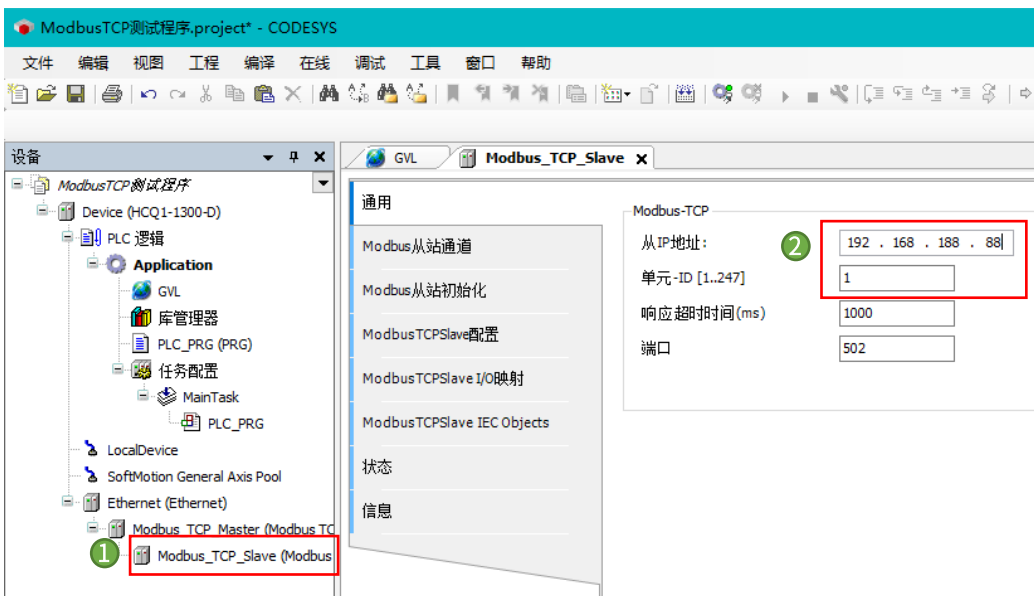


当使用 Q1 作为 ModbusTCP 主站时，同样需要在 CODESYS 的 IDE 界面中配置从站相关信息，如下图示，右击添加的【Modbus_TCP_Master】，选择【添加设备】，在弹出对话框里选择【Modbus TCP Slave】。



2.4.2 配置从站

双击【Modbus_TCP_Slave】，在通用选项卡修改从站 IP 地址为 192.168.188.88（从站设备 IP 地址，确保同一个网段），端口设置为 502。从站地址根据从站站号设置，此处【单元-ID】设置为 1。



选择【Modbus 从站通道】，点击右下角【添加通道】，设置通道名以及访问类型还有长度跟偏移量，如下图示，在本次测试中，设置通道名为 channel0，访问类型为【Read Holding Registers】（访问类型函数代码与 Modbus 报文功能码一致），长度为【5】，偏移量为【0】，点击【确定】建立通道。

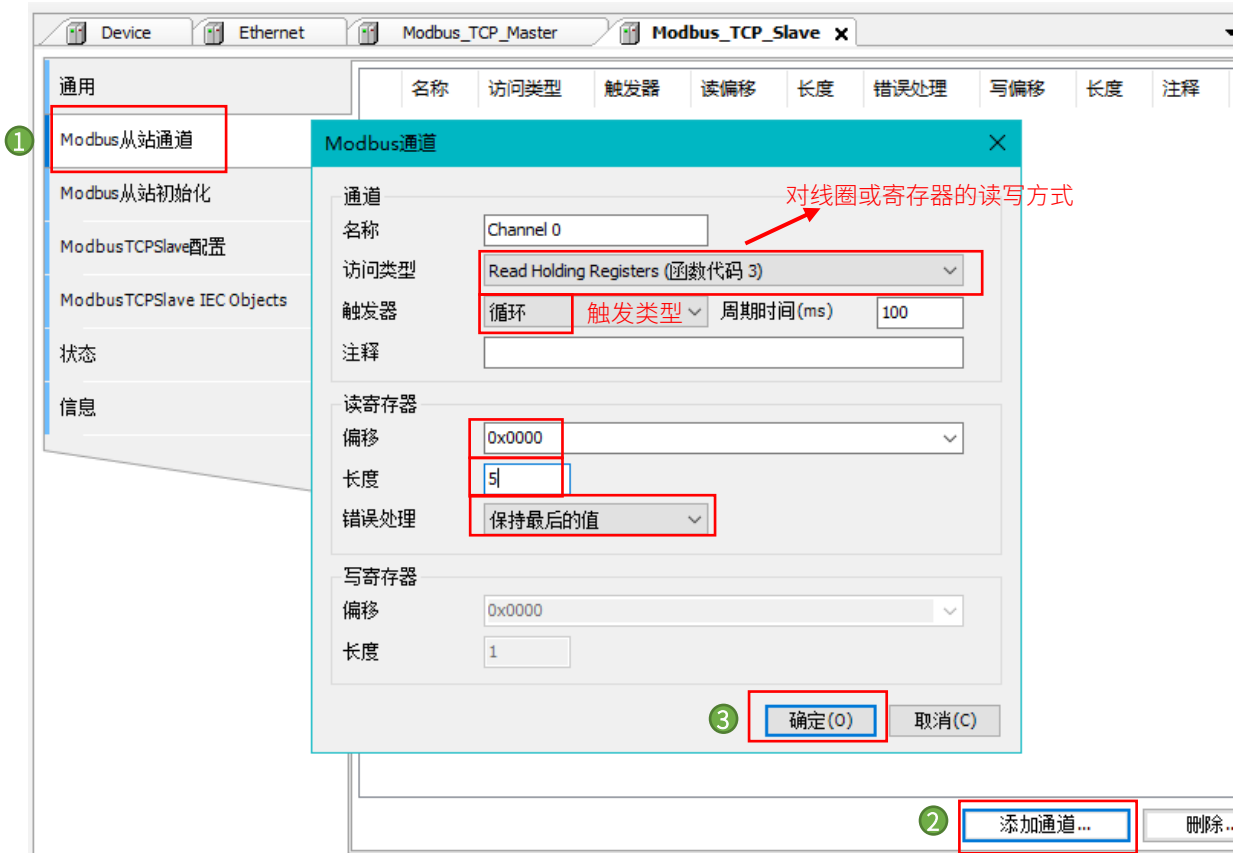


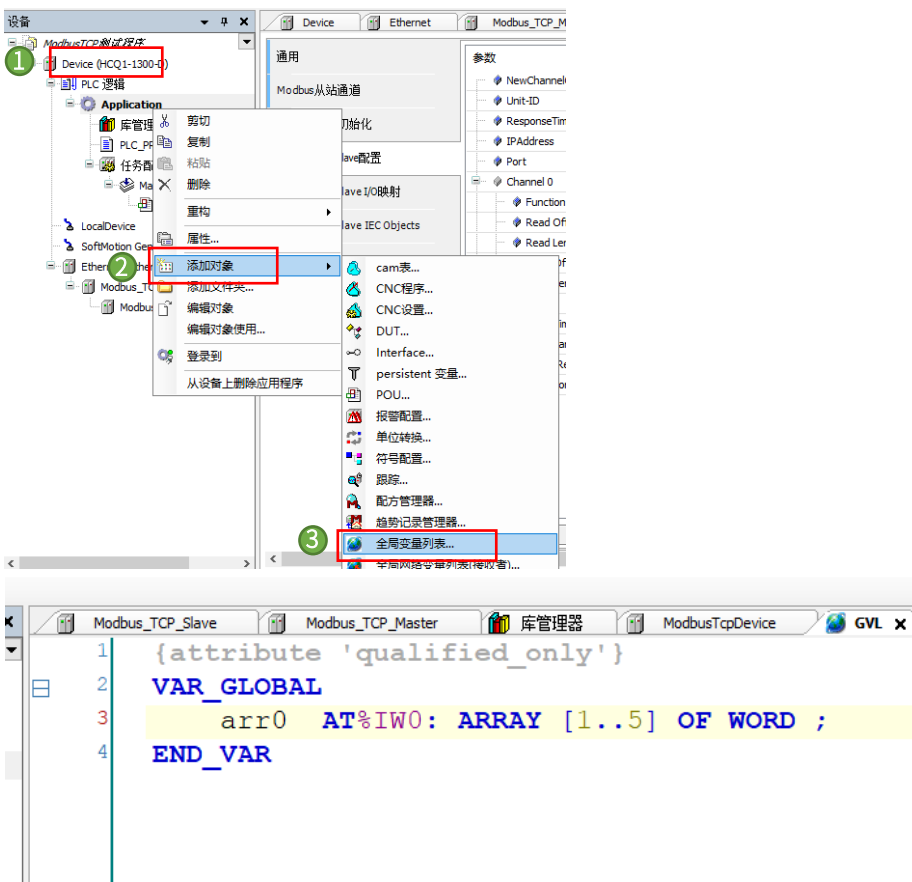
表 1 Modbus TCP 从站通道含义表

项目	类型	说明
访问类型	Read Coils (1)	读线圈
	Read Discrete Inputs (2)	读离散输入
	Read Holding Registers (3)	读保持寄存器
	Read Inputs Registers (4)	读输入寄存器
	Write Single Coil (5)	写单个线圈
	Write Single Register (6)	写单个保持寄存器
	Write Multiple Coils (15)	写多个线圈
	Write Multiple Registers (16)	写多个保持寄存器
	Read or Write Multiple Registers (17)	读/写多个保持寄存器

触发器	循环/上升沿/应用程序	触发类型
周期时间		触发器周期
偏移		主从站的起始地址存在偏移，可进行设置
长度		表示所读数据的数据长度
错误处理	保持最后的值/设置为 0	发生错误时寄存器的值

2.4.3 通讯变量配置

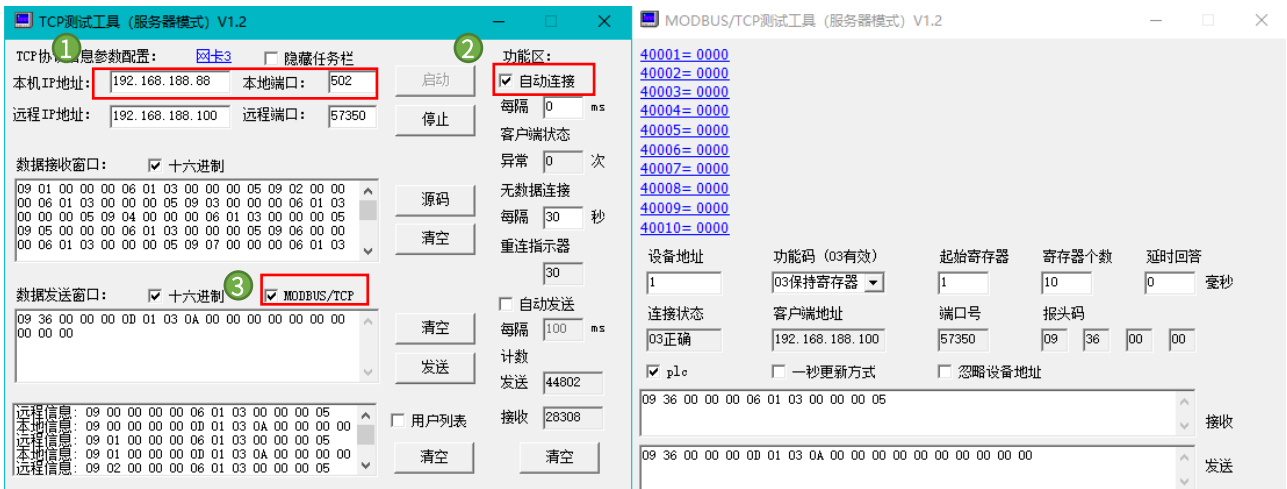
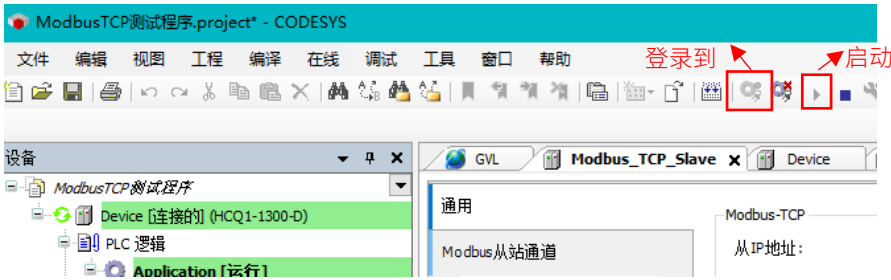
点击左侧树型菜单【Application】→【添加变量】→【全局变量】，如图所示，创建 TCP 通讯变量，此处选择新建数组类型全局变量作为通讯变量。



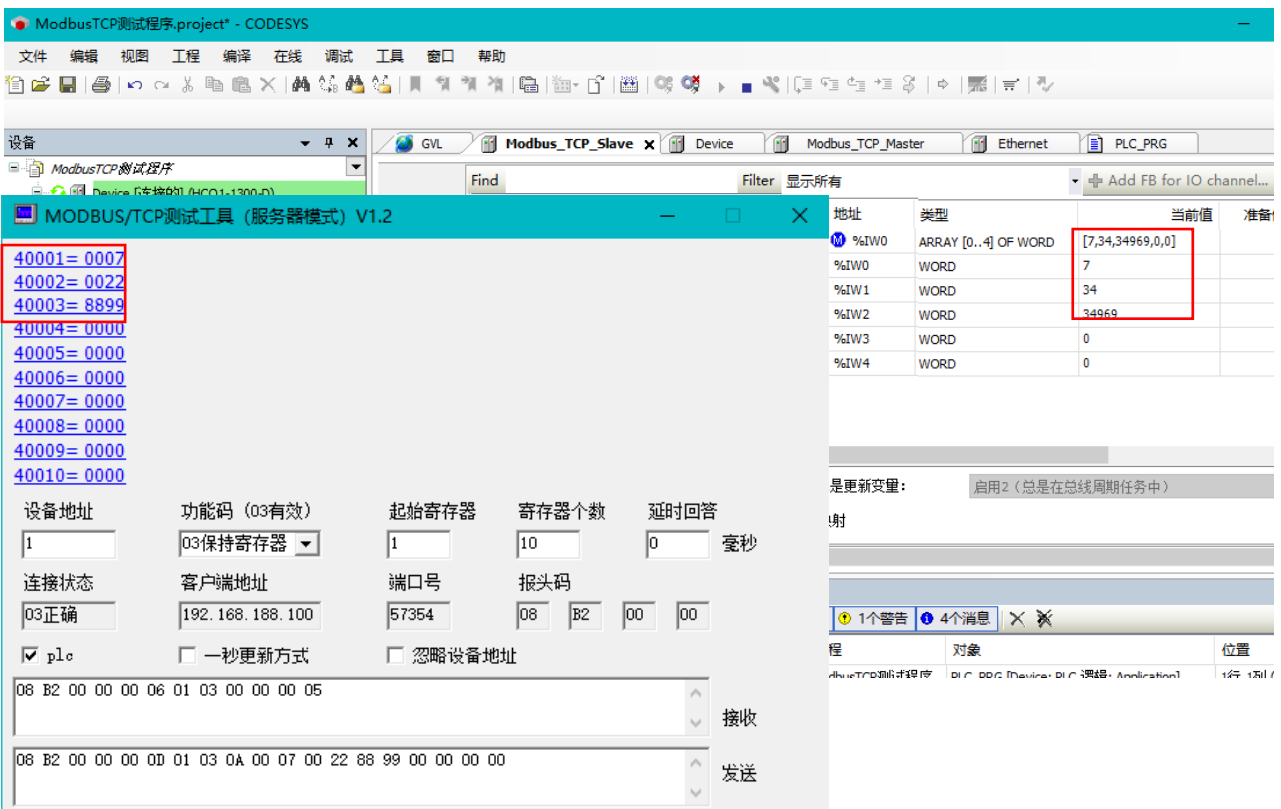
2.4.4 主站功能调试

登录程序到 Q1 中并启动程序，打开 TCP 调试工具，设置从站 IP 为【192.168.188.88】、置端口号为【502】（与上位机中设置的从站 IP 地址、端口号及其他参数配置保持一致）。设置完毕，勾选【自动连接】后，勾选【Modbus/TCP】，可以看到报文头码一直在累加，codesys 中创建的数组变量对应地址区域变量数值也随之改动，代表通讯正常，接收数据报文如下图所示。ModbusTCP 报文数

据结构请参考 (附录 2):

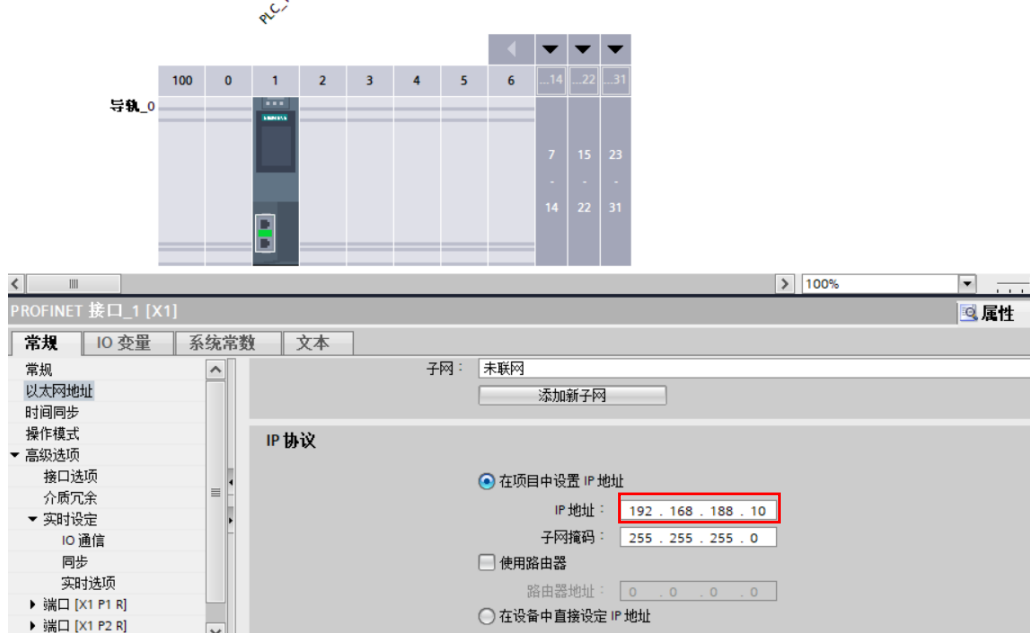


如图更改寄存器 40001, 40002, 40003 的值分别为 0007, 0022, 8899, 运行程序, Modbus TCP 正常通讯的情况下, CODESYS 中对应的寄存器数值也会随之改动, 主站成功读取寄存器

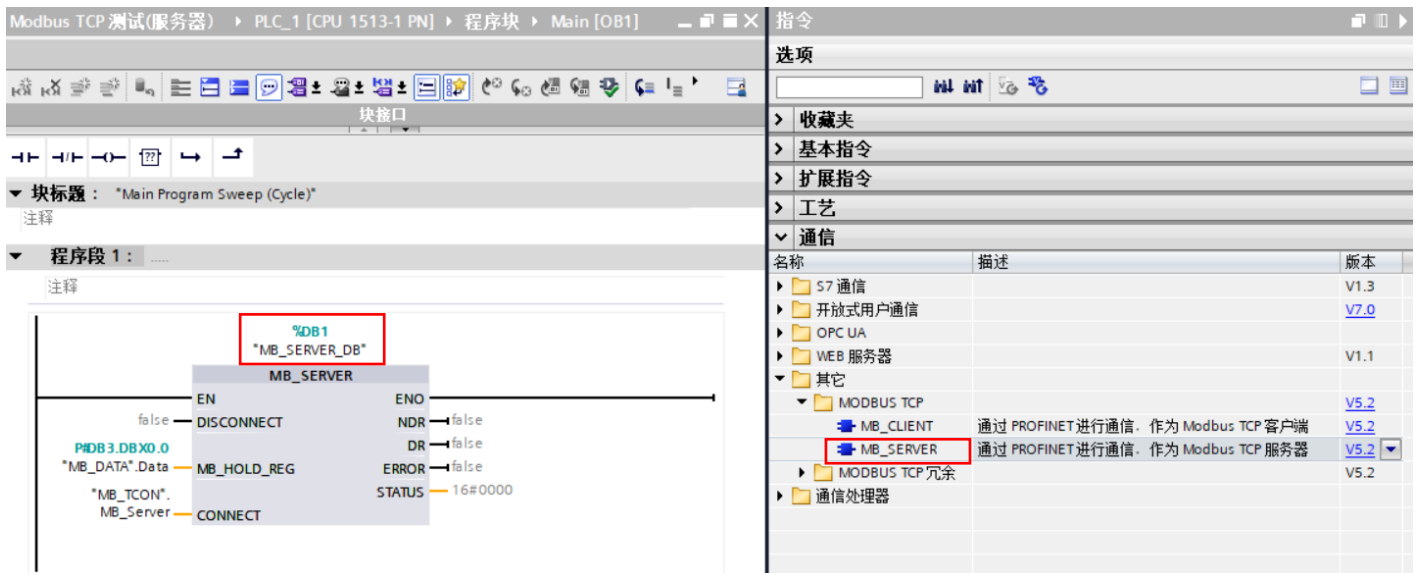


2.4.5 Q1 做主站（客户端） 西门子 S7-1500 做从站

打开 TIA Portal V16 软件，新建一个项目，命名【Modbus TCP 测试（服务器）】，在项目添加 CPU1513-1PN，为集成的 PROFINET 接口新建一个子网并设置 IP 地址，本例中为【192.168.188.10】。



在 CPU1513-1PN 的 OB1 组织块中添加 Modbus TCP Server 功能块【MB_SERVER】，软件将提示会为该 FB 块增加一个背景数据块【DB1 “MB_SERVER_DB”】。



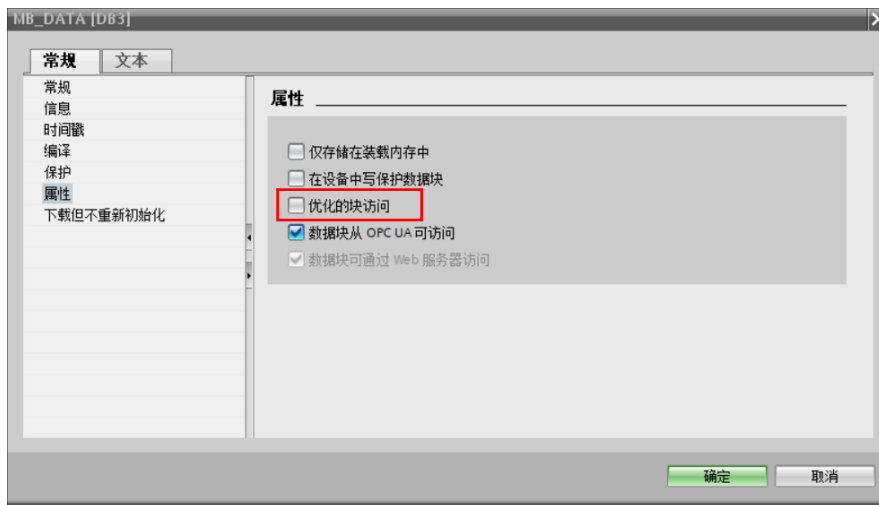
之后在 CPU1513-1PN 中添加一个全局数据块用于匹配功能块【MB_SERVER】的管脚参数【CONNECT】，本例中为数据块【DB2 “MB_TCON”】，打开该数据块，手动输入一个【TCON_IP_v4】数据类型的变量【MB_Server】，并填写参数初始值。

Modbus TCP 测试(服务器) > PLC_1 [CPU 1513-1 PN] > 程序块 > MB_TCON [DB2]

保持实际值 快照 将快照值复制到起始值中 将起始值加载为实际值

MB_TCON		数据类型	起始值	保持	从 HMI/OPC...	从 H...	在 HMI ...	设定值	监控	注释
1	Static			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2	MB_Server	TCON_IP_v4		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	InterfaceId	HW_ANY	64	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HW-identifier of IE-interface submodule
4	ID	CONN_OUC	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	connection reference / identifier
5	ConnectionType	Byte	16#0B	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	type of connection: 11=TCP/IP, 19=UDP (17=TCP)
6	ActiveEstablished	Bool	false	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	active/passive connection establishment
7	RemoteAddress	IP_V4		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	remote IP address (IPv4)
8	ADDR	Array[1..4] of Byte		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 address
9	ADDR[1]	Byte	192	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 address
10	ADDR[2]	Byte	168	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 address
11	ADDR[3]	Byte	188	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 address
12	ADDR[4]	Byte	100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 address
13	RemotePort	UInt	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	remote UDP/TCP port number
14	LocalPort	UInt	502	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	local UDP/TCP port number

创建一个全局数据块用于匹配功能块【MB_SERVER】的管脚参数【MB_HOLD_REG】，本例中为【DB3 “MB_DATA”】，用于存储保持性寄存器的通信数据，需要注意的是该数据块必须为非优化数据块（支持绝对寻址），在该数据块的属性中不勾选【优化的块访问】选项。在数据块中建一个数组【Array[0..255] of Word】（长度、类型随意）。

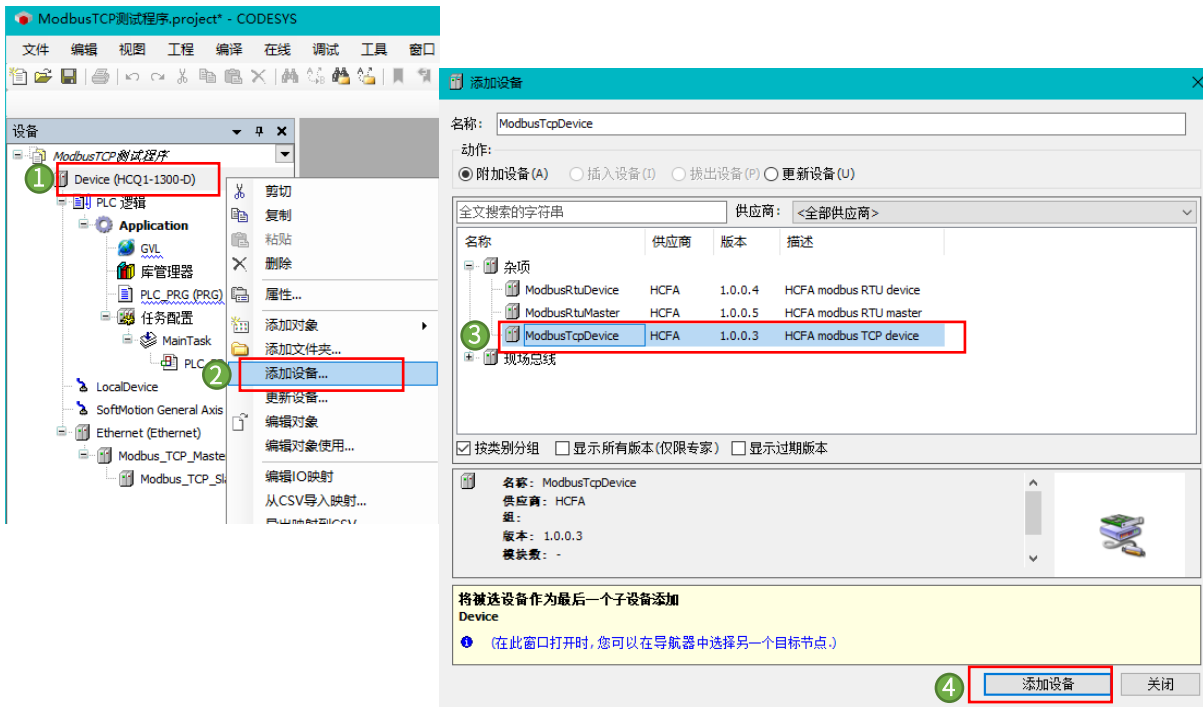


完成上述各管脚参数后，下载项目到 CPU1513-1PN 中，在线监控【DB3 “MB_DATA”】中数组内数据和 Q1 变量表内数据，Modbus TCP 正常通讯的情况下，CODESYS 中对应的寄存器数值也会随之改动，主站成功读取寄存器。

2.5 Modbus TCP 从站功能 (Q1 作从站, 服务器)

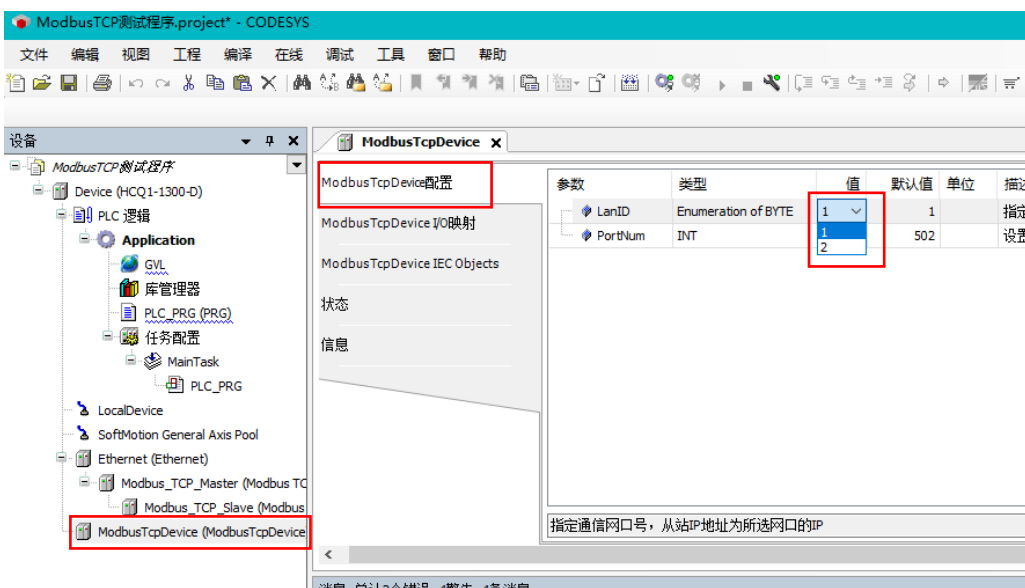
2.5.1 添加从站

右击左侧树型菜单【Device】→选择【添加设备】，在弹出对话框中打开【杂项】，选中【ModbusTcpDevice】，最后点击【添加设备】。



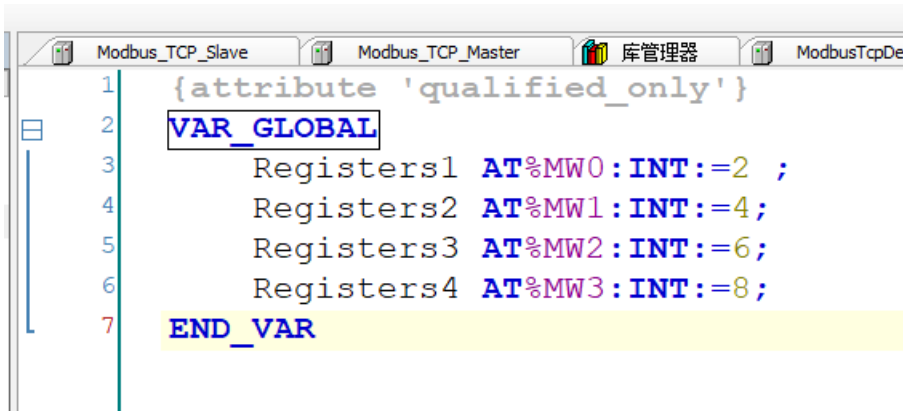
2.5.2 配置从站

打开【ModbusTcpDevice】→【ModbusTcpDevice 配置】，根据上位机与 Q1 所连的 Port 口来选择【LanID】(1 为 Port1 口；2 为 Port2 口)，本次实验连接的是 Port1 口，故此处【LanID】选择【1】；端口号【PortNum】默认为 502。



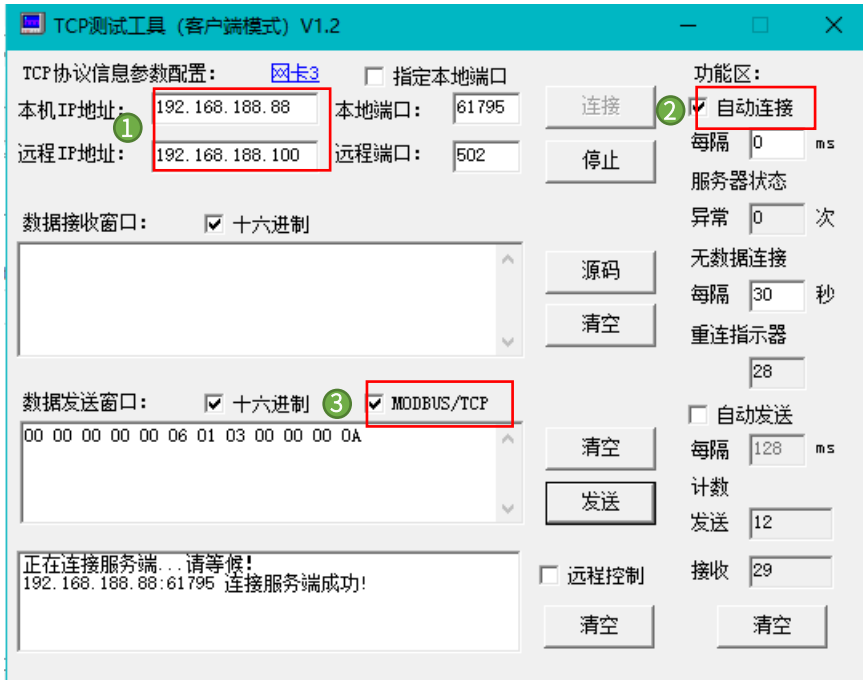
2.5.3 通讯变量配置

如图所示，在全局变量列表里新建 4 个变量【Registers1】【Registers2】【Registers3】【Registers4】并映射地址和赋值。

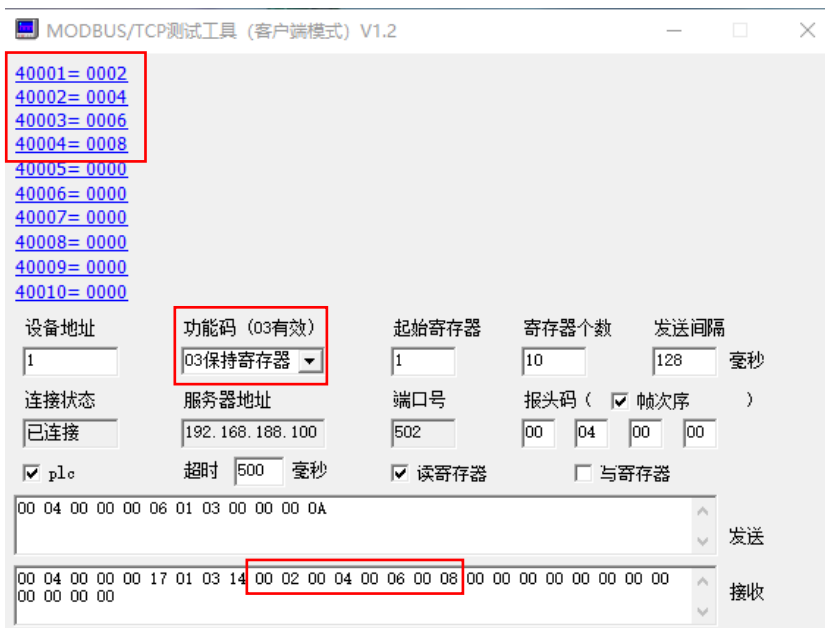
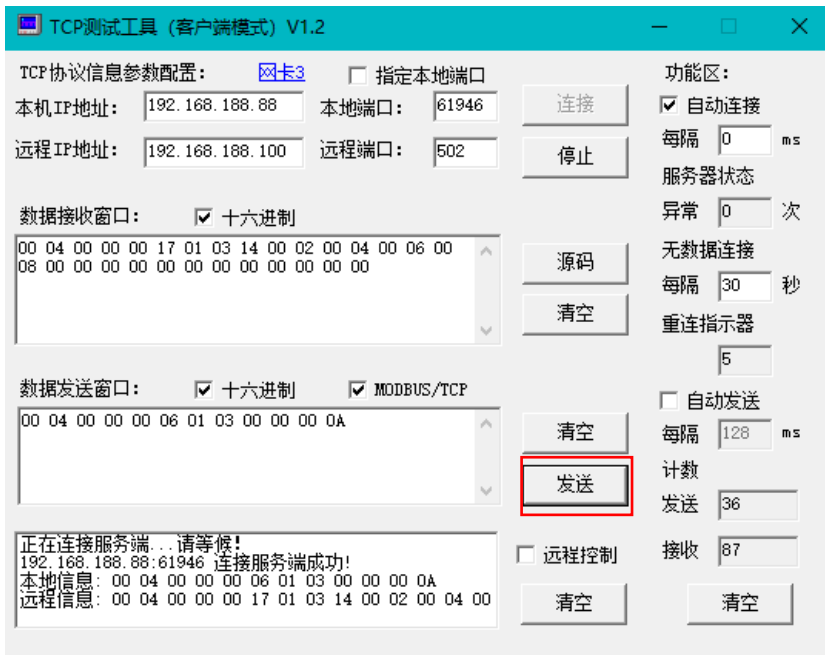


2.5.4 从站功能调试

登录程序到 Q1 中并启动程序，打开 TCP 测试工具（客户端模式）。设置本机 IP 为【192.168.188.88】（与上位机中设置的从站 IP 地址、端口号及其他参数配置保持一致）。远程 IP 地址为【192.168.188.100】（与 Q1 Port1 口 IP 地址一致），远程端口号默认为【502】，设置完毕，勾选【自动连接】后，勾选【Modbus/TCP】，此时显示连接成功，表示通讯无误。

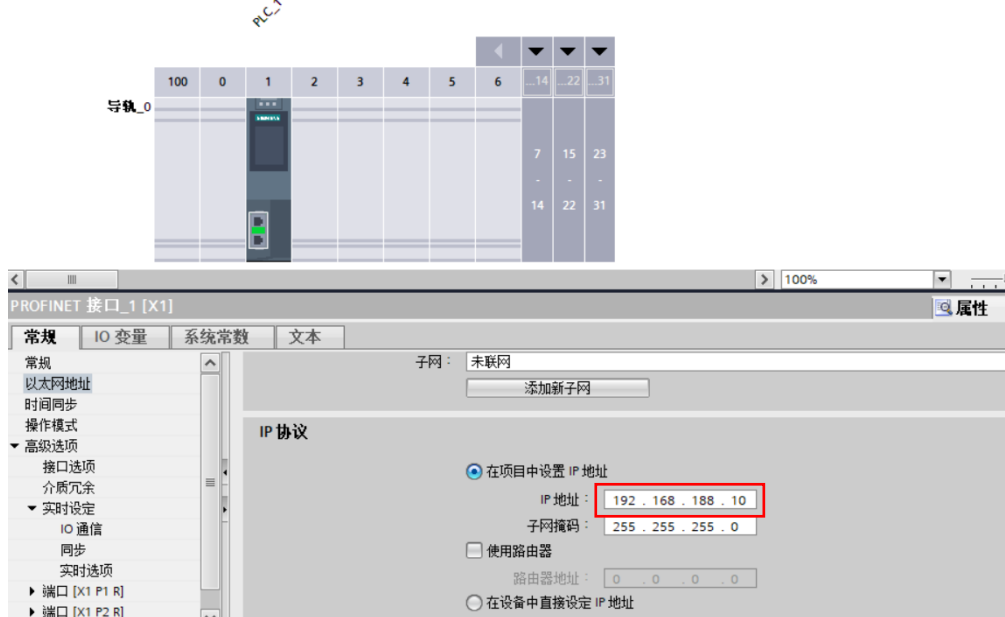


点击【发送】报文后，寄存器读取到从站中的数据，寄存器 0~3 分别为 16 进制的 2、4、6、8，与程序中写入的变量值一致，主站成功读取到从站相应寄存器的数值。

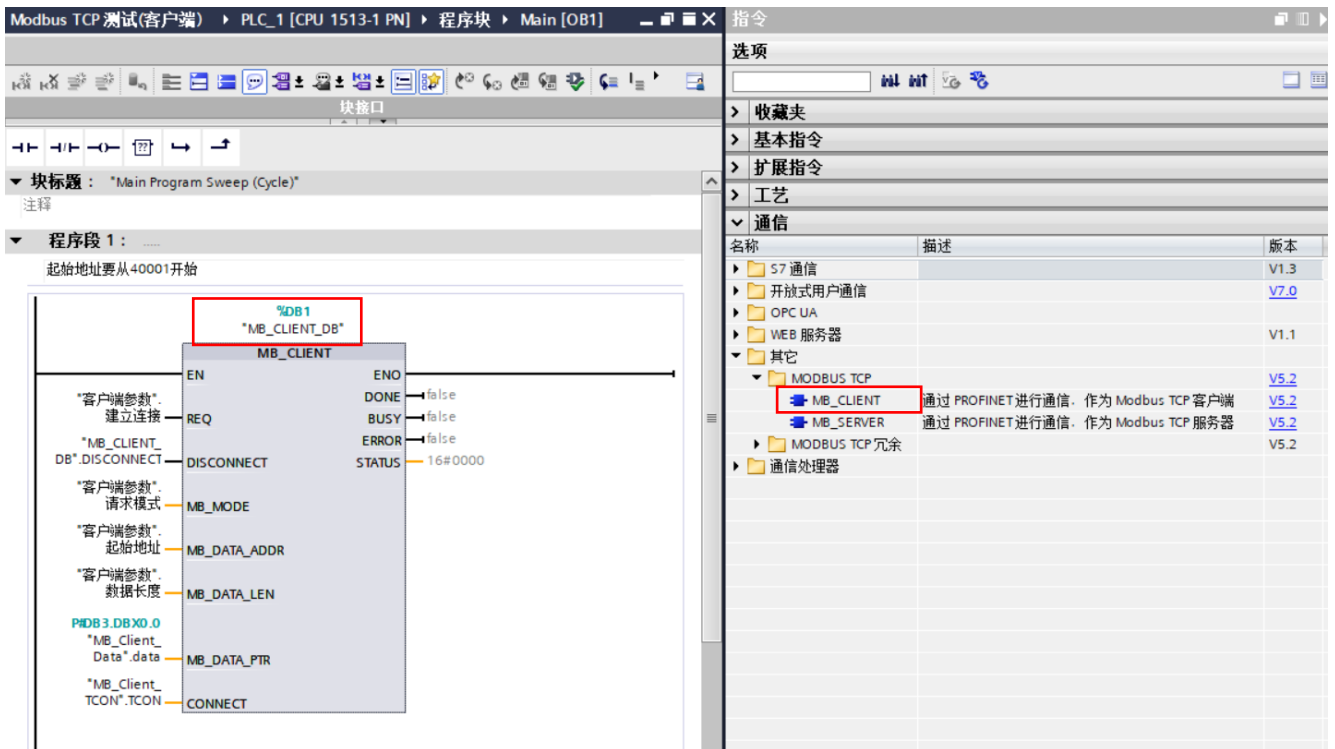


2.5.5 Q1 做从站 (服务器) 西门子 S7-1500 做主站

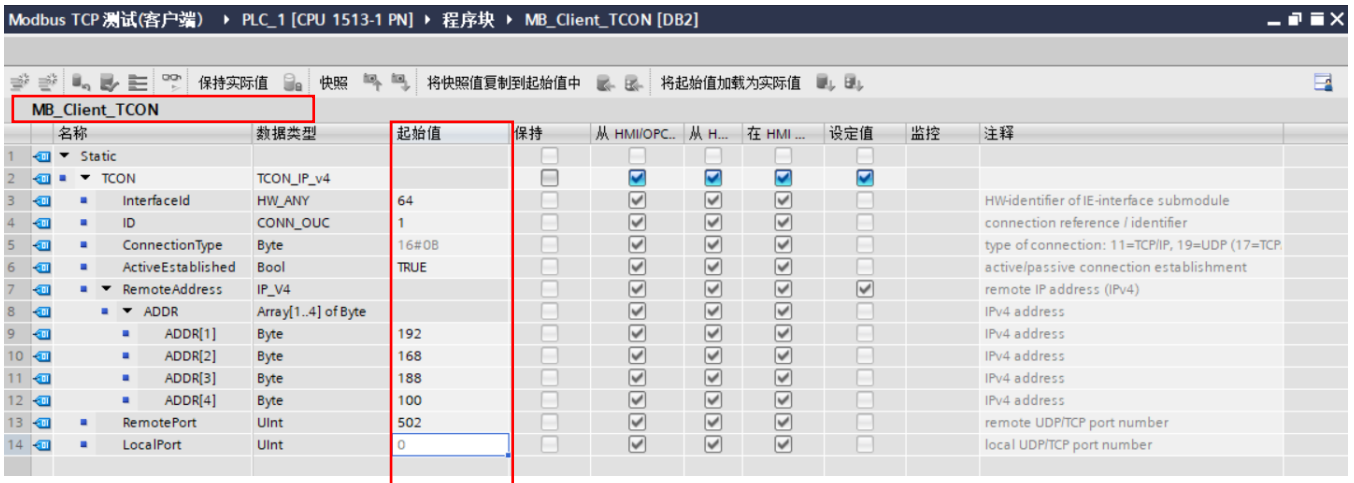
打开 TIA Portal V16 软件, 新建一个项目, 命名【Modbus TCP 测试 (服务器)】, 在项目添加 CPU1513-1PN, 为集成的 PROFINET 接口新建一个子网并设置 IP 地址, 本例中为【192.168.188.10】。



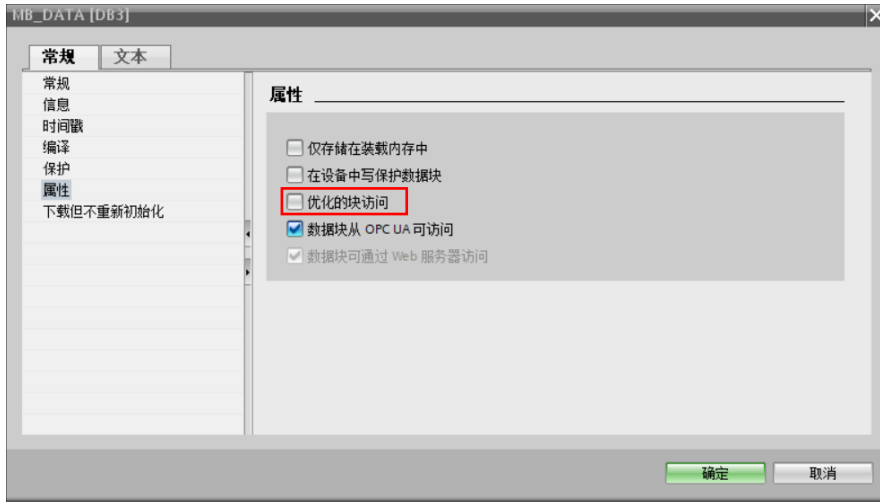
在 CPU1513-1PN 的 OB1 组织块中添加 Modbus TCP Client 功能块【MB_CLIENT】, 软件将提示会为该 FB 块增加一个背景数据块【DB1 “MB_CLIENT_DB”】。



同样在 CPU1513-1PN 中添加一个全局数据块用于匹配功能块【MB_CLIENT】的管脚参数【CONNECT】，本例中为数据块【DB2 “MB_Client_TCON”】，打开该数据块，手动输入一个【TCON_IP_v4】数据类型为的变量【TCON】，并填写参数初始值。



创建一个全局数据块用于匹配功能块【MB_CLIENT】的管脚参数【MB_DATA_PTR】，本例中为【DB3 “MB_Client_Data”】，用于存储保持性寄存器的通信数据，需要注意的是该数据块必须为非优化数据块（支持绝对寻址），在该数据块的属性中不勾选【优化的块访问】选项。在数据块中建一个数组【Array[0..255] of Word】（长度、类型随意）。



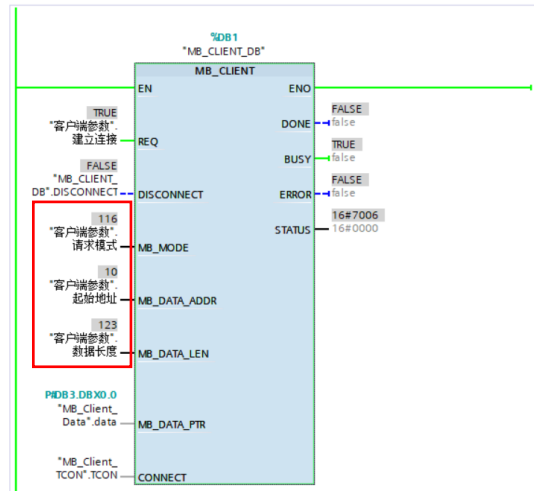
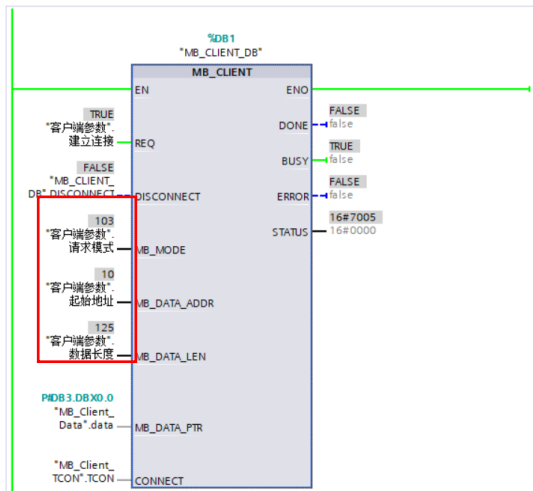
对于功能块【MB_CLIENT】的其它管脚参数如下表：

“MB_CLIENT”的管脚参数	管脚类型声明	数据类型	含义
REQ	输入	BOOL	与 Modbus TCP 服务器之间的通信请求，常 1 有效
DISCONNECT	输入	BOOL	0：与通过 CONNECT 参数组态的连接伙伴建立通信连接。 1：断开通信连接

MB_MODE	输入	USINT	选择 Modbus 请求模式 (0=读取、1=写入 或诊断)
MB_DATA_ADDR	输入	UDINT	由“MB_CLIENT”指令所访问数据的起始地址
MB_DATA_LEN	输入	UINT	数据长度：数据访问的位数或字数
DONE	输出	BOOL	只要最后一个作业成功完成，立即将输出参数 DONE 的位置位为“1”
BUSY	输出	BOOL	0: 无 Modbus 请求在进行中 1: 正在处理 Modbus 请求
ERROR	输出	BOOL	0: 无错误 1: 出错。出错原因由参数 STATUS 指示
STATUS	输出	WORD	指令的详细状态信息

对于【MB_MODE】、【MB_DATA_ADDR】和【MB_DATA_LEN】参数，其对应关系如下：（很重要，建议采用红框内的参数设置）

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus 功能	功能和数据类型
0	1 到 9999	1 到 2000	01	在远程地址 0 到 9998 处，读取 1 到 2000 个输出位
0	10001 到 19999	1 到 2000	02	在远程地址 0 到 9998 处，读取 1 到 2000 个输入位
0	<ul style="list-style-type: none"> 40001 到 49999 400001 到 465535 	1 到 125	03	<ul style="list-style-type: none"> 在远程地址 0 到 9998 处，读取 1 到 125 个保持性寄存器 在远程地址 0 到 65534 处，读取 1 到 125 个保持性寄存器
0	30001 到 39999	1 到 125	04	在远程地址 0 到 9998 处，读取 1 到 125 个输入字
1	1 到 9999	1	05	在远程地址 0 到 9998 处，写入 1 个输出位
1	<ul style="list-style-type: none"> 40001 到 49999 400001 到 465535 	1	06	<ul style="list-style-type: none"> 在远程地址 0 到 9998 处，写入 1 个保持性寄存器 在远程地址 0 到 65534 处，写入 1 个保持性寄存器
1	1 到 9999	2 到 1968	15	在远程地址 0 到 9998 处，写入 2 到 1968 个输出位
1	<ul style="list-style-type: none"> 40001 到 49999 400001 到 465535 	2 到 123	16	<ul style="list-style-type: none"> 在远程地址 0 到 9998 处，写入 2 到 123 个保持性寄存器 在远程地址 0 到 65534 处，写入 2 到 123 个保持性寄存器
2	1 到 9999	1 到 1968	15	在远程地址 0 到 9998 处，写入 1 到 1968 个输出位
2	<ul style="list-style-type: none"> 40001 到 49999 400001 到 465535 	1 到 123	16	<ul style="list-style-type: none"> 在远程地址 0 到 9998 处，写入 1 到 123 个保持性寄存器 在远程地址 0 到 65534 处，写入 1 到 123 个保持性寄存器
101	0 到 65535	1 到 2000	01	在远程地址 0 到 65535 处，读取 1 到 2000 个输出位
102	0 到 65535	1 到 2000	02	在远程地址 0 到 65535 处，读取 1 到 2000 个输入位
103	0 到 65535	1 到 125	03	在远程地址 0 到 65535 处，读取 1 到 125 个保持性寄存器
104	0 到 65535	1 到 125	04	在远程地址 0 到 65535 处，读取 1 到 125 个输入字
105	0 到 65535	1	05	在远程地址 0 到 65535 处，写入 1 个输出位
106	0 到 65535	1	06	在远程地址 0 到 65535 处，写入 1 个保持性寄存器
115	0 到 65535	1 到 1968	15	在远程地址 0 到 65535 处，写入 1 到 1968 个输出位
116	0 到 65535	1 到 123	16	在远程地址 0 到 65535 处，写入 1 到 123 个保持性寄存器

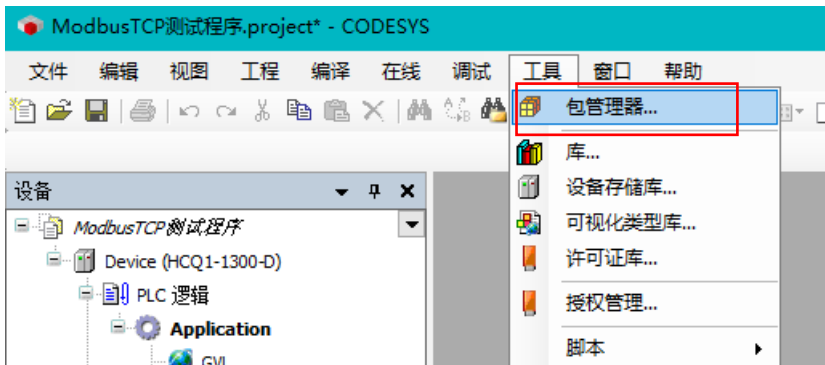


完成上述各管脚参数后，下载项目到 CPU1513-1PN 中，在线监控【DB3 “MB_Client_Data”】中数组内数据和 Q1 变量表内数据，Modbus TCP 正常通讯的情况下，CODESYS 中对应的寄存器数值也会随之改动，主站成功读取寄存器。

附录 1：描述文件安装

目前，Q1 常用描述文件已打包成软件包，用户只需安装一个 package 即可安装大部分描述文件（包括 Q1 描述文件，Modbus TCP 描述文件等等）。

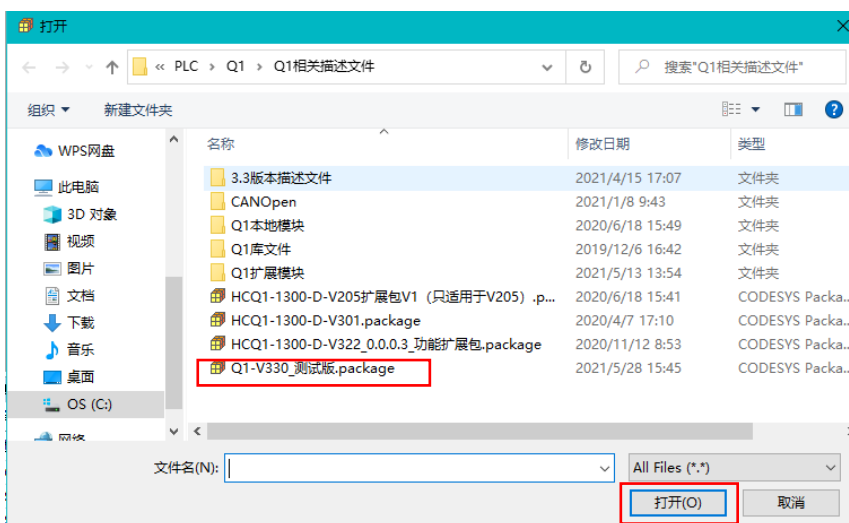
1. 在菜单栏中点击【工具】→【包管理器】



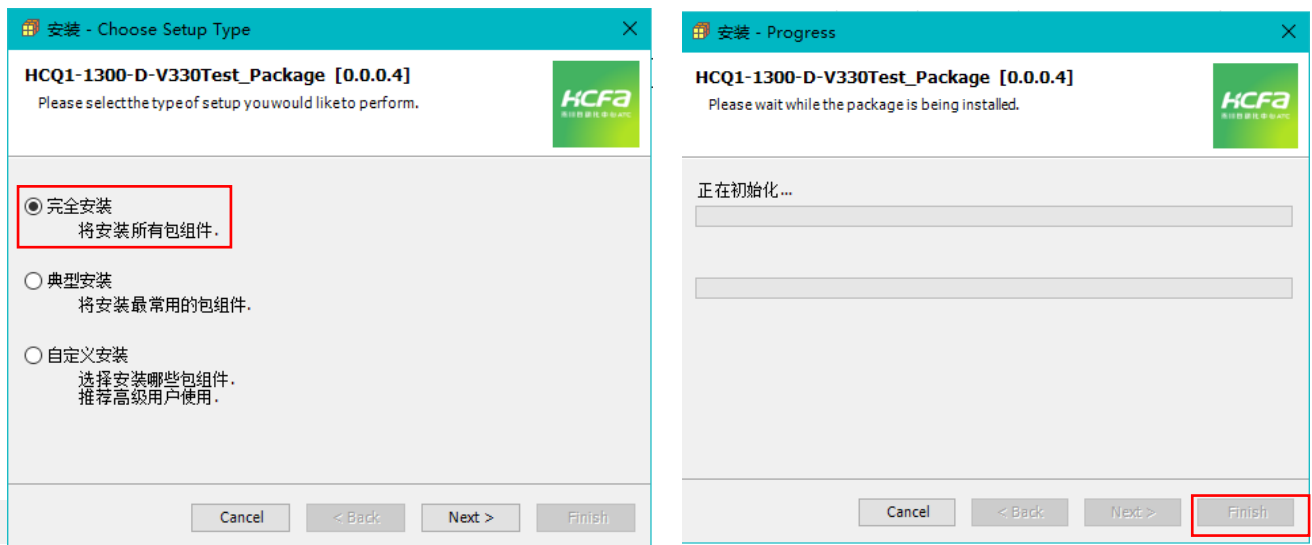
2. 在弹出窗口中点击右侧【安装】



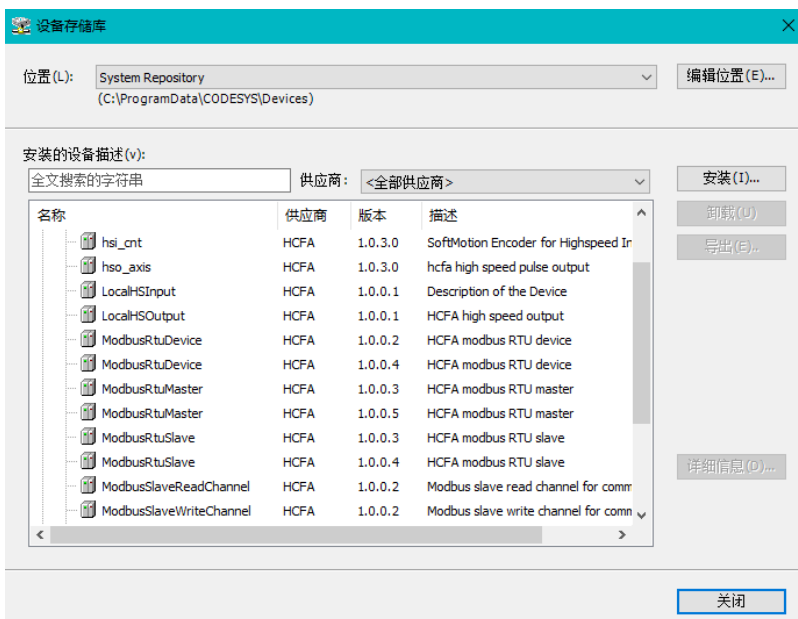
3. 找到下载的 package 文件，点击【打开】



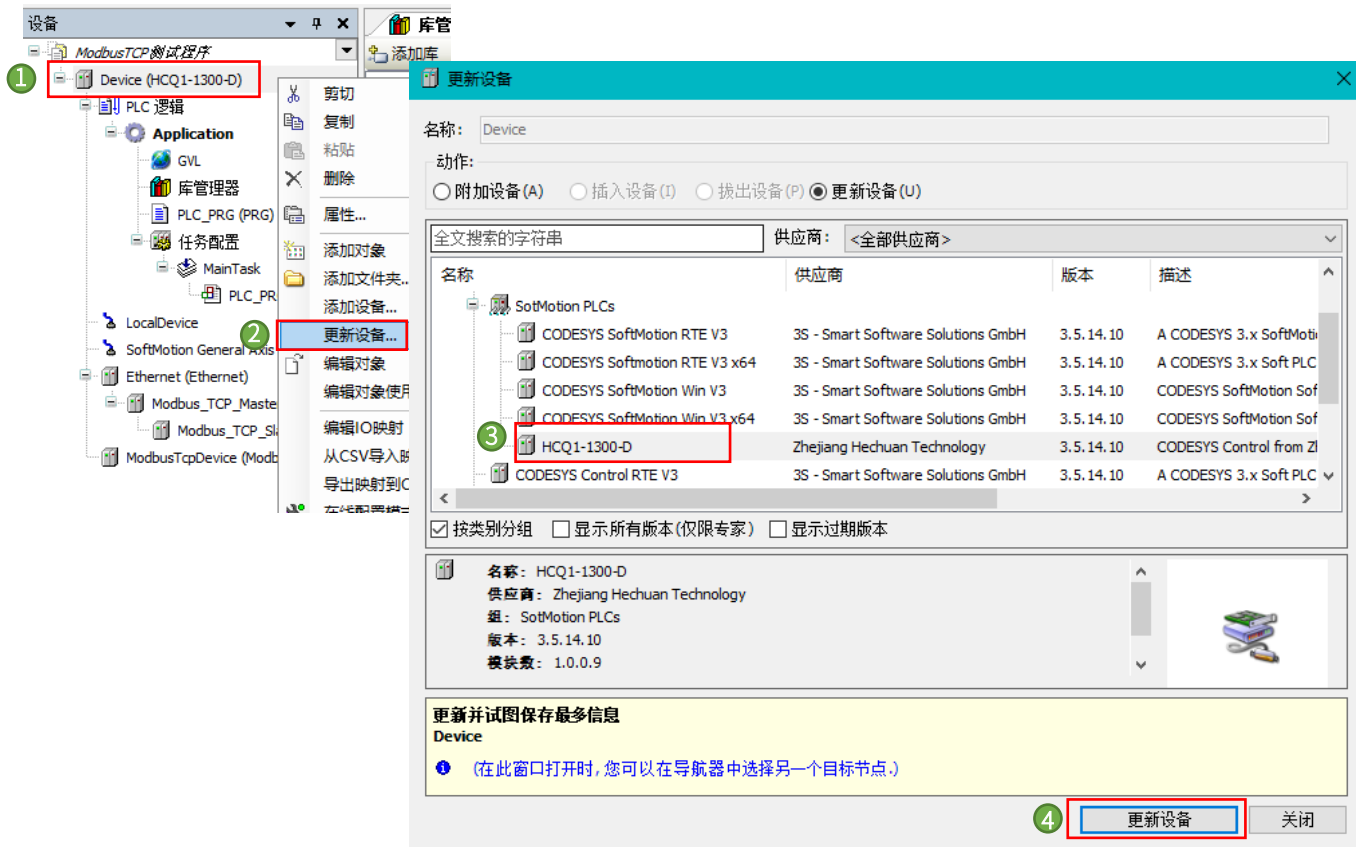
4. 在弹出窗口中选择【完全安装】，进入安装流程，结束后点击【Finish】



5. 成功安装后在包管理器的当前软件安装包界面中可以看到成功安装的描述文件包，在描述文件列表中也可以查看到新安装好的描述文件。



6. 若用户已创建的项目不在 HCQ1-1300-D 平台下，此时需要 PLC 程序更改运行平台。右击【Device】→【更新设备】，即可进行切换平台。



附录 2: Modbus TCP 数据报文结构

Modbus 是一个请求/应答协议，并且提供功能码规定的服务，下面介绍 Modbus TCP 的报文结构。

以下列请求及应答报文为例：

请求：97 76 00 00 00 06 04 04 00 00 00 01

应答：97 76 00 00 00 05 04 04 02 12 34

请求报文：

97 76 00 00 00 06 04 04 00 00 00 01				
	示例	长度	说明	备注
Map 报文头	0x97	1	事务处理标识符 Hi	客户机发起，服务器复制，用于事务处理配对
	0x76	1	事务处理标识符 Lo	
	0x0000	2	协议标识符号	客户机发起，服务器复制 Modbus 协议= 0.
	0x0006	2	长度	从本字节下一个到最后
	0x04	1	单元标识符	客户机发起，服务器复制 串口链路或其他总线上远程终端标识
功能码	0x04	1	功能码，读寄存器	参考标准 modbus 协议
数据	0x0000	2	起始地址	
	0x 0001	2	寄存器数量	
校验				

应答报文：

97 76 00 00 00 05 04 04 02 12 34				
	示例	长度	说明	备注
Map 报文头	0x97	1	事务处理标识符 Hi	客户机发起，服务器复制，用于事务处理配对
	0x76	1	事务处理标识符 Lo	
	0x0000	2	协议标识符号	客户机发起，服务器复制 Modbus 协议= 0.
	0x0005	2	长度	从本字节下一个到最后
	0x04	1	单元标识符	客户机发起，服务器复制 串口链路或其他总线上远程终端标识
功能码	0x04	1	功能码，读寄存器	参考标准 modbus 协议
数据	0x02	1	字节个数	
	0x ----		数据	此报文中数据为 12 34
校验				

部分功能码定义如下表：

功能码	描述	访问类型	Q1 从站地址	数据类型	操作数量
0x01	线圈	读	%QX0.0 - %QX8191.7	位	单/多
0x02	离散输入	读	%IX0.0 - %IX8191.7	位	单/多
0x03	保持寄存器	读	%MW0 - %MW65535	字	单/多
0x04	输入寄存器	读	%MW0 - %MW65535	字	单/多
0x05	单个线圈	写	%QX0.0 - %QX8191.7	位	单
0x06	单个保持寄存器	写	%MW0 - %MW65535	字	单
0x0F	多个线圈	写	%QX0.0 - %QX8191.7	位	多
0x10	多个保持寄存器	写	%MW0 - %MW65535	字	多

Modbus 寄存器地址分配如下表：

Q1 从站地址	适用功能	寄存器种类	读写状态
%QX0.0 - %QX8191.7	01H	线圈	可读
	05H 0FH		可写
%IX0.0 - %IX8191.7	02H	离散输入	可读
%MW0 - %MW65535	04H	输入寄存器	可读
%MW0 - %MW65535	03H 06H 10H 17H	保存寄存器	可读可写

寄存器种类说明如下表：

寄存器种类	说明	PLC 类比	举例说明
线圈	输出端口，可设定端口的输出状态，也可以读取该位的输出状态。可分为两种不同的执行状态，例如保持型和边沿触发型。	DO 数字量输出	电磁阀输出、MOSFET 输出、LED 显示等。
离散输入	输入端口，通过外部设定该案输入状态，可读但不可写。	DI 数字量输入	拨码开关、接近开关等。
输入寄存器	输入参数，控制器运行时从外部设备获得的参数，可读但不可写。	AD 模拟量输入	模拟量输入
保存寄存器	输出参数或保存参数，控制器运行时被设定的某些参数，可读可写。	DA 模拟量输出	模拟量输出设定值，PID 运行参数，变量阀输出大小，传感器报警上限下限。