S7-1500/1200 系列与 H3u 的 Modbus TCP 通讯

张长兴（18606277674）

说明：在 TIA 软件中，“MB_CLIENT”指令作为 Modbus TCP 客户端通过 PROFINET 连接进行通信。通过“MB_CLIENT”指令，可以在客户端和服务器之间建立连接、发送 Modbus 请求、接收响应并控制 Modbus TCP 客户端的连接终端。

S7-1200 固件版本 V4.0 支持“MB_CLIENT”指令和最高 V3.1 版本的库。S7-1200 固件版本 V4.1 及更高版本和 S7-1500，支持“MB_CLIENT”指令的所有库版本。

可通过 CPU 或 CM/CP 的本地接口建立连接。

1. 硬件连接

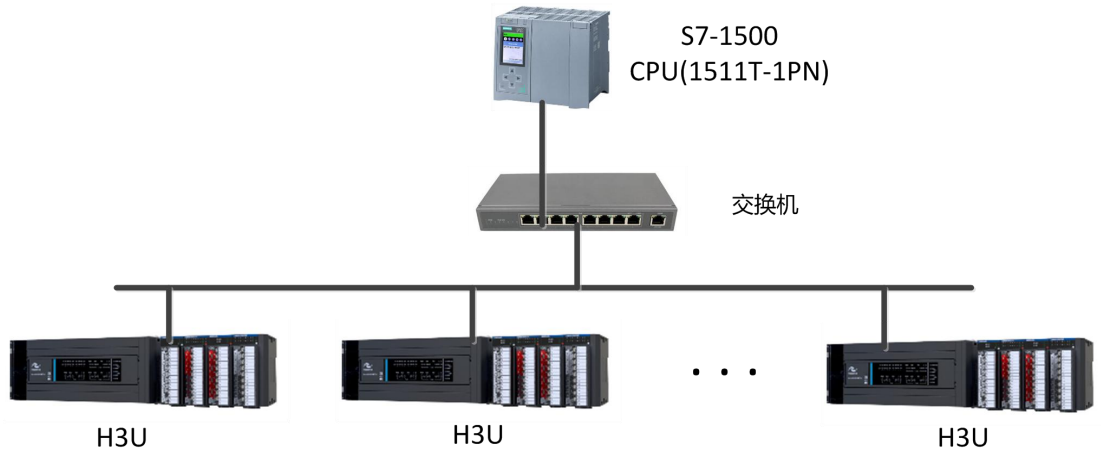


图 2.1.0 TCP 组网接线图

- 网线要求：网线采用标准超 7 类，带屏蔽层，水晶头必须带屏蔽层。
- 交换机要求：工业级交换机（建议使用宇泰工业交换机）。

2. 西门子 TIA 软件设置

（1）建立工程，根据实际所连设备添加 CPU 类型，比如 SIMATIC S7-1500 1511T-1 PN ，6ES7 511-1TK01-0AB0。

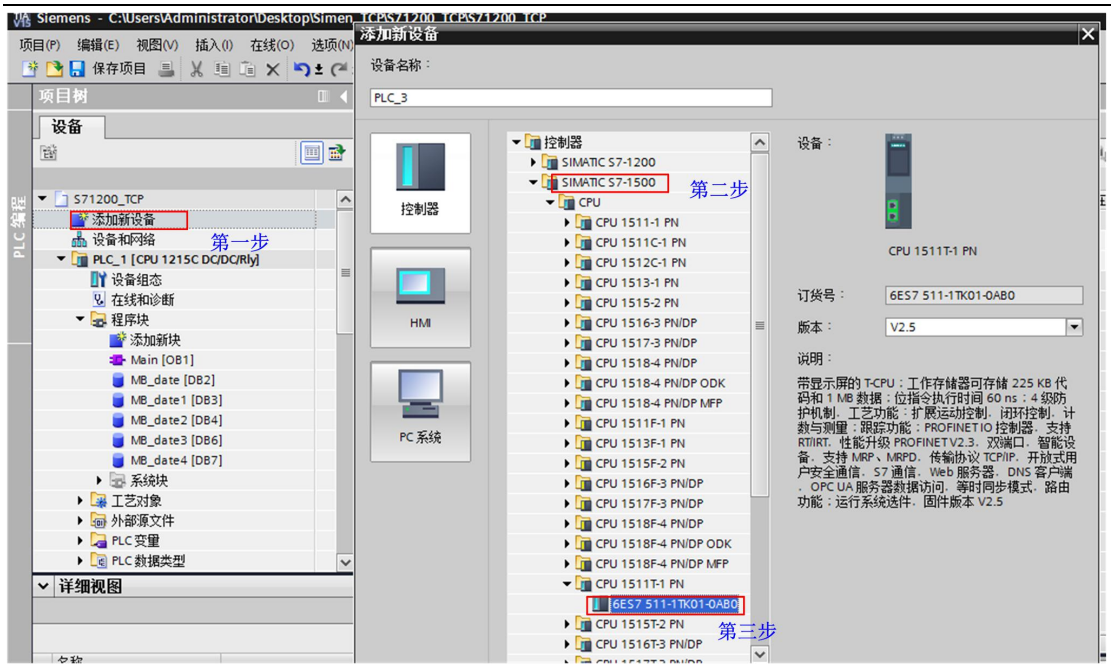


图 2.2.0 TIA 工程建立

（2）添加通讯功能块，“MB_CLIENT”。

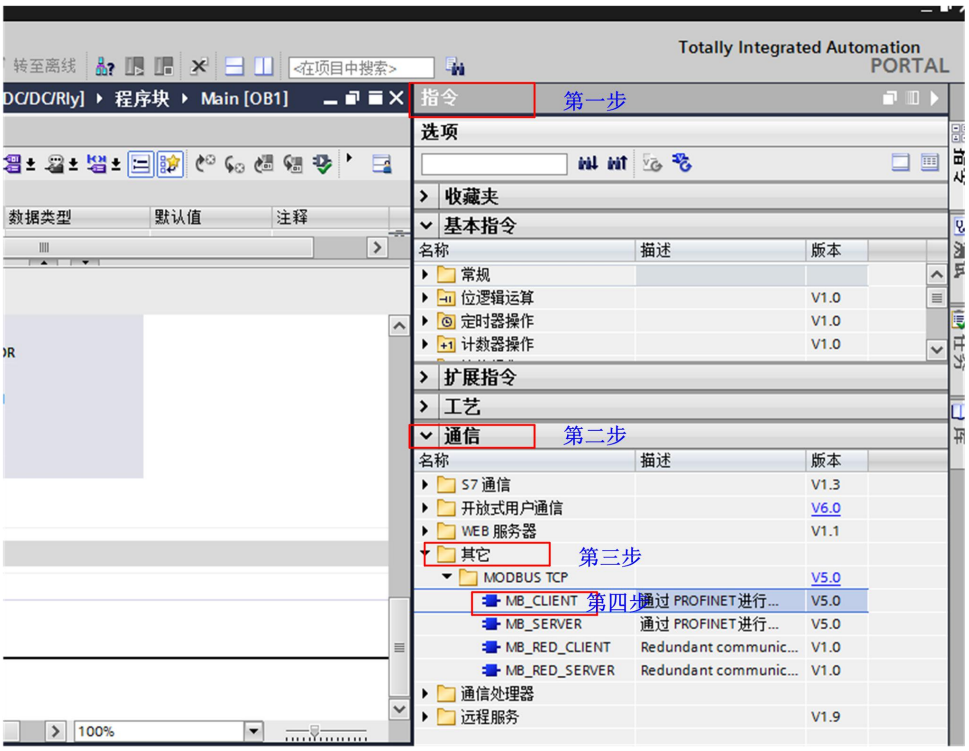


图 2.2.1 MODBUS-TCP 主站功能块添加

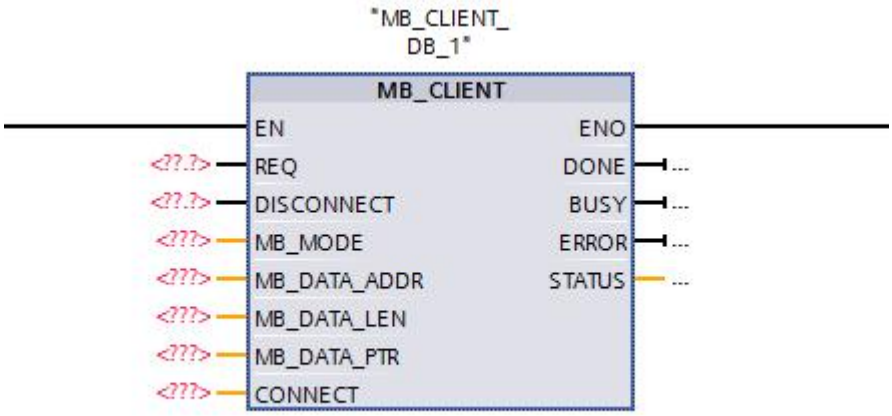


图 2.2.2 MODBUS-TCP 主站功能块示意

（3）“MB_CLIENT”实例化，引脚配置。

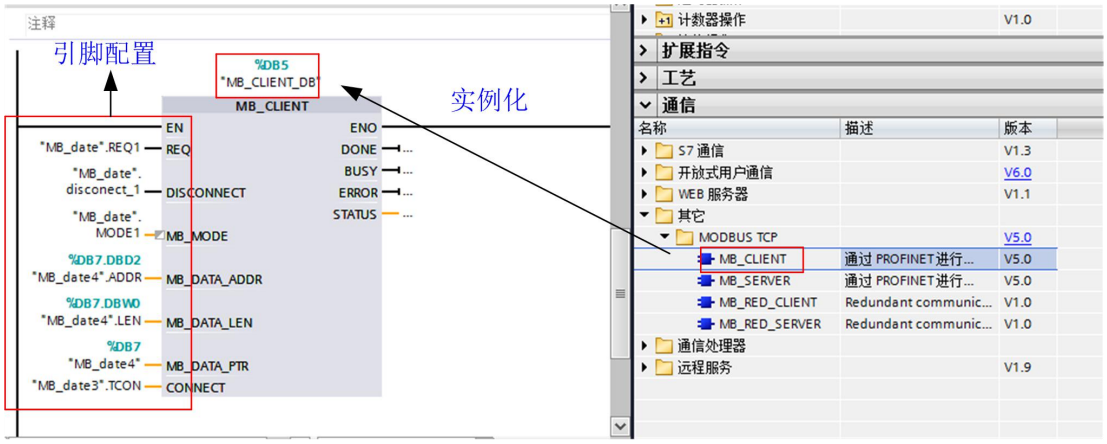


图 2.2.3 MODBUS-TCP 主站功能块设置

注意事项：西门子软件中，需要建立数据块进行变量声明与定义。按照功能块引脚要求，定义准确的变量数据类型。

如下图所示。

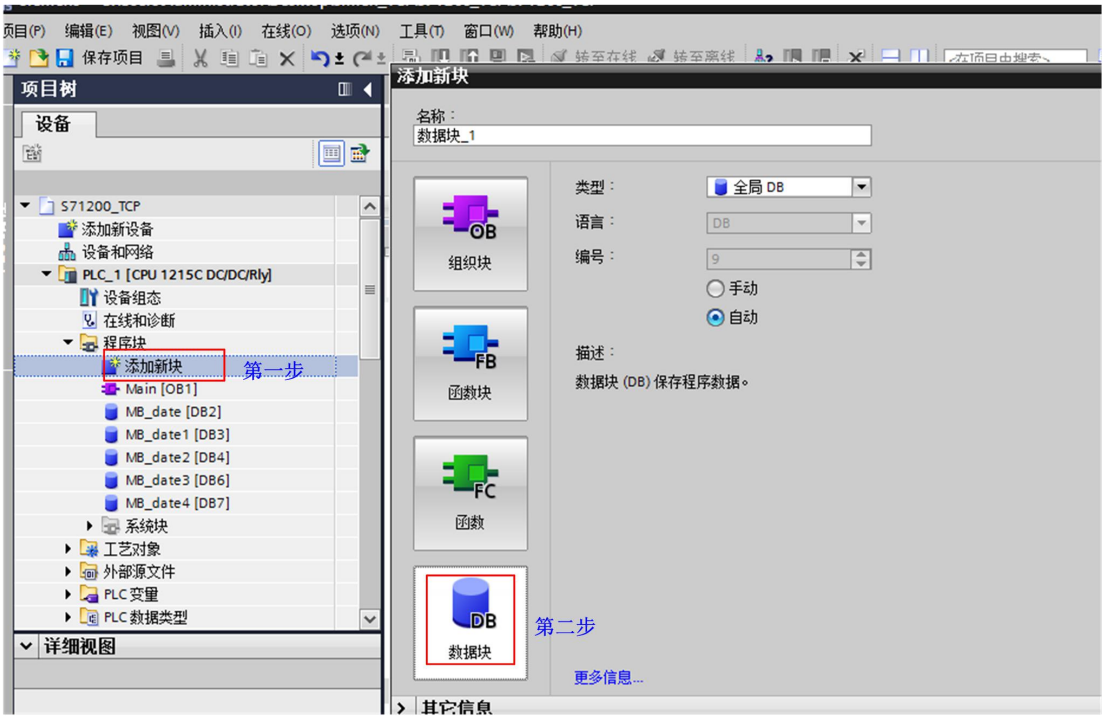


图 2.2.5　添加数据块

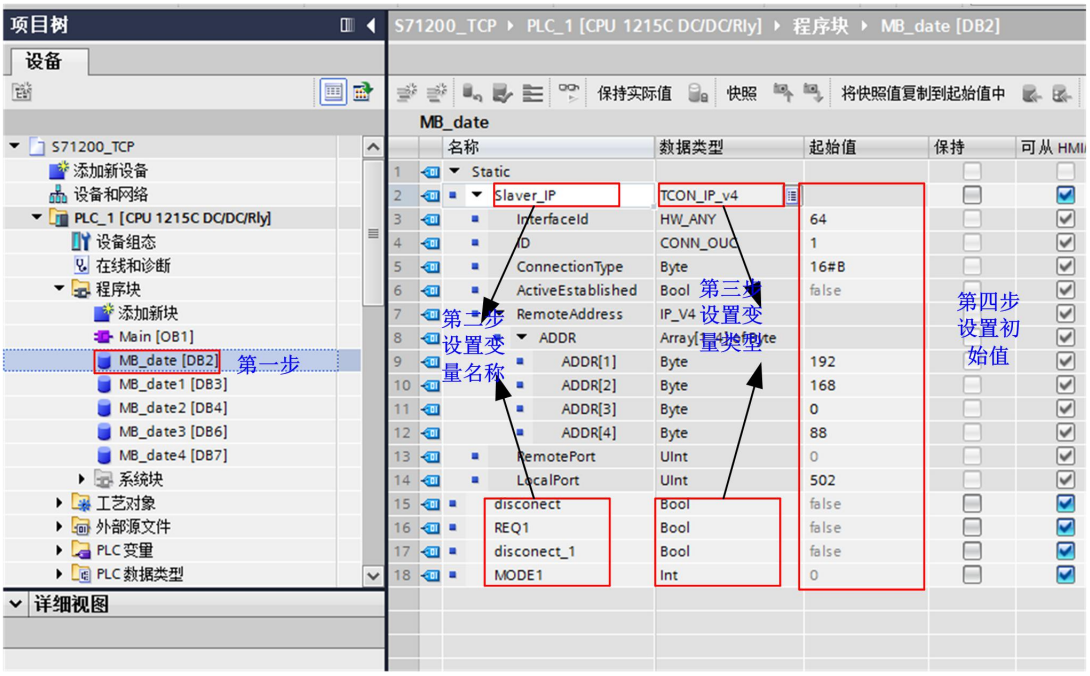


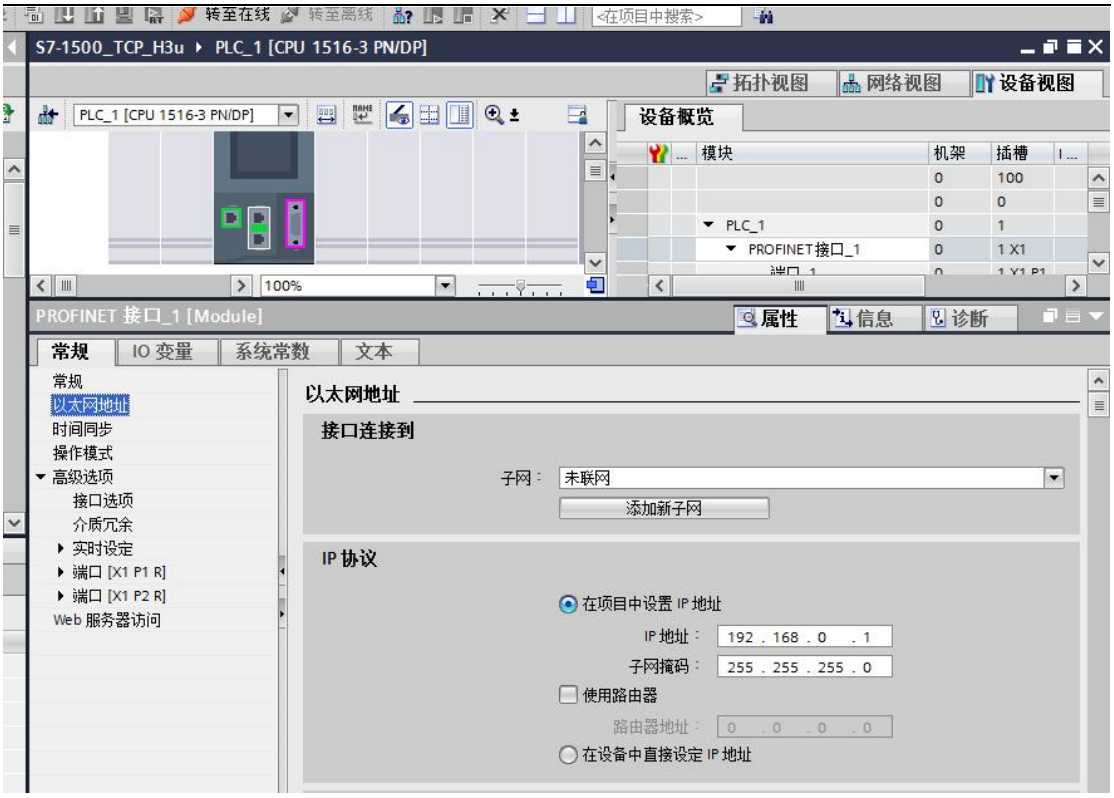
图 2.2.5　数据块中变量定义

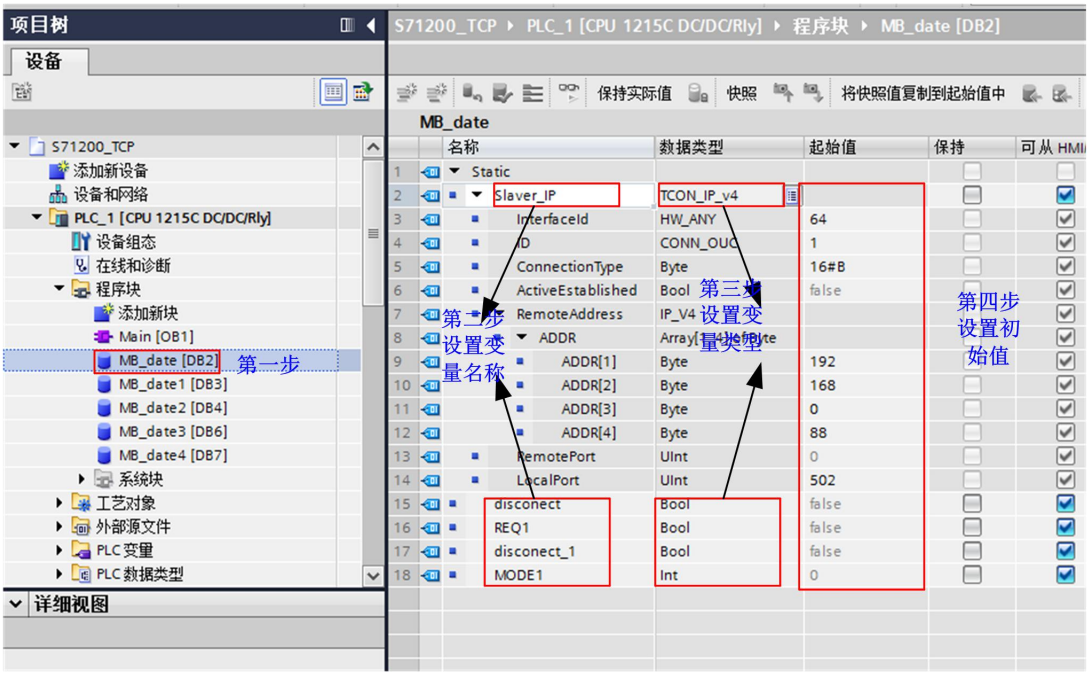
（4）数据传送。

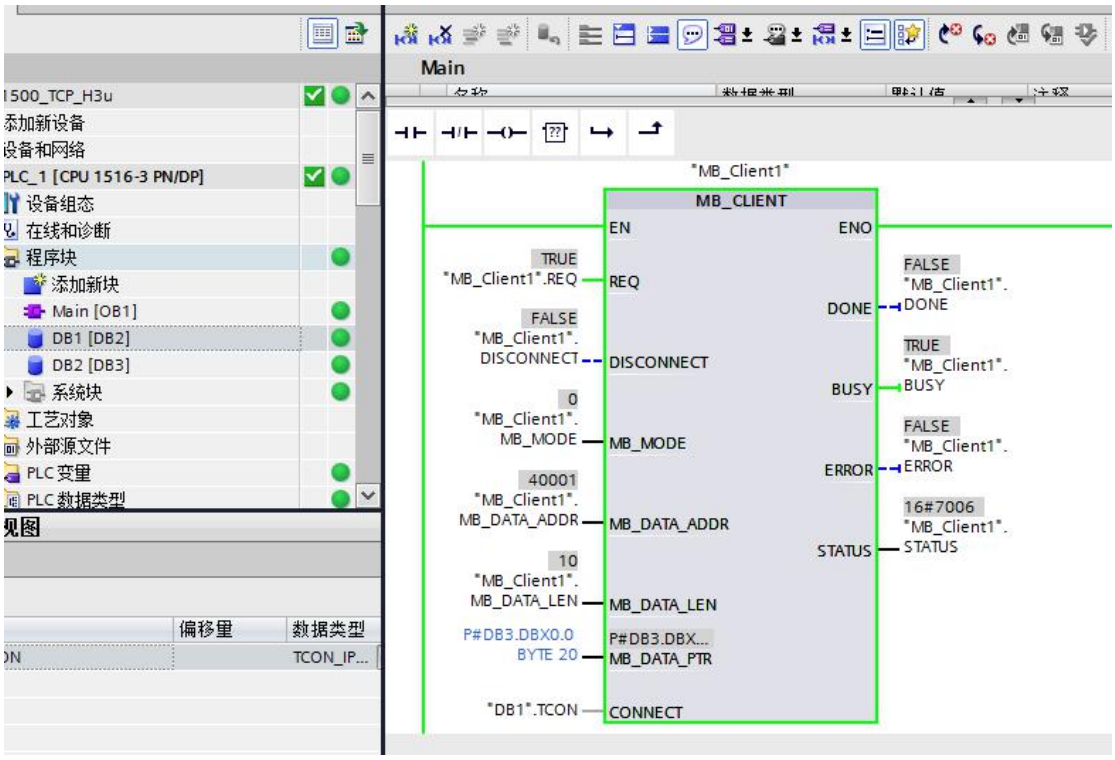
功能块“MB_CLIENT”，引脚 MB_MODE、MB_DATA_ADDR 和 MB_DATA_LEN 参数对应关系及地址说明。

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	• 40001 到 49999 • 400001 到 465535	1 到 125	03	• 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	• 40001 到 49999 • 400001 到 465535	1	06	• 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	• 40001 到 49999 • 400001 到 465535	2 到 123	16	• 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	• 40001 到 49999 • 400001 到 465535	1 到 123	16	• 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
11	在该指令的执行过程中，不会评估 MB_DATA_ADDR 和 MB_DATA_LEN 参数的值。		11	读取服务器的状态字和事件计数器： • 状态字反映了处理的状态（0 - 未处理，0xFFFF - 正在处理） • Modbus 请求成功执行时，事件计数器将递增。如果执行 Modbus 功能时出错，则服务器将发送消息，但不会递增事件计数器。
80	-	1	08	通过诊断代码 0x0000 检查服务器状态（返回循环测试 - 服务器发回请求）： • 每次调用 1 个 WORD
81	-	1	08	通过诊断代码 0x000A 复位服务器的事件计数器： • 每次调用 1 个 WORD
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

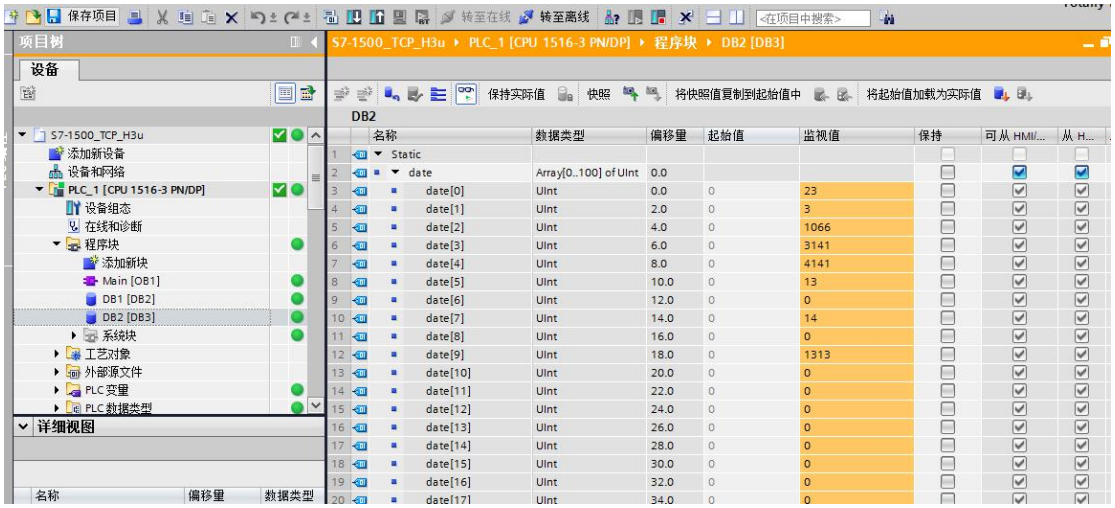
（5）根据功能块说明，MODBUS-TCP 从站，建立 IP 地址关联，按照（4）中地址对应关系，实现数据交互。

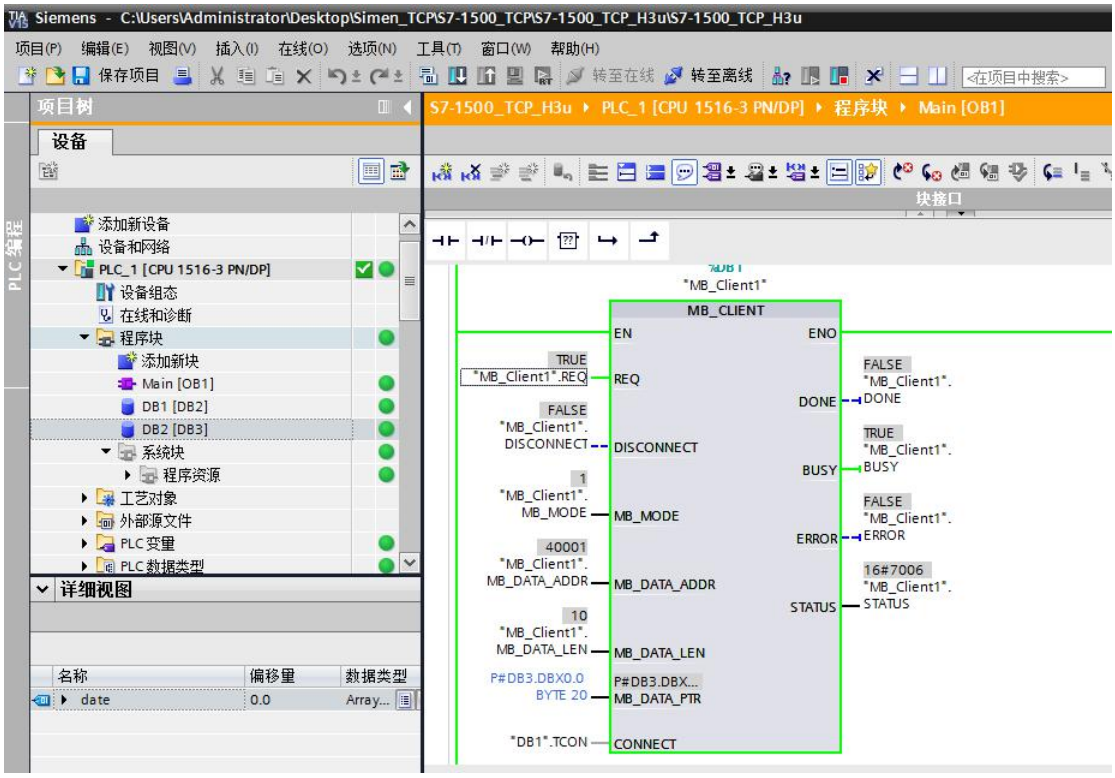

S7-1500_TCP_H3u ▸ PLC_1 [CPU 1516-3 PN/DP]
拓扑视图
网络视图
设备视图
设备概览
模块
机架
插槽
PLC_1
PROFINET接口_1
PROFINET 接口_1 [Module]
属性
信息
诊断
常规
IO 变量
系统常数
文本
以太网地址
接口连接到
子网：
未联网
添加新子网
IP 协议
在项目中设置 IP 地址
IP 地址：
192 . 168 . 0 . 1
子网掩码：
255 . 255 . 255 . 0
使用路由器
路由器地址：
在设备中直接设定 IP 地址

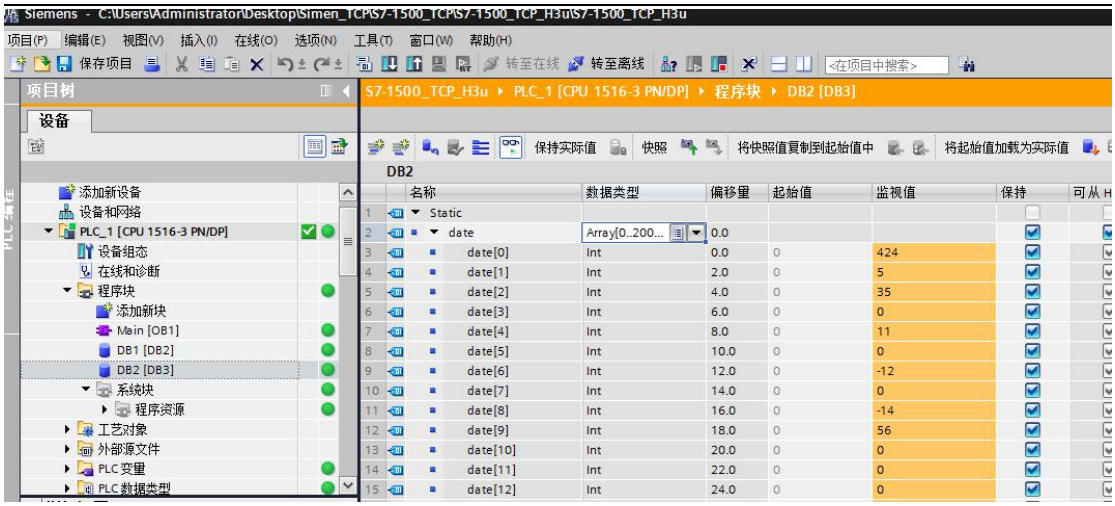

项目树
设备
S71200_TCP ▸ PLC_1 [CPU 1215C DC/DC/Rly] ▸ 程序块 ▸ MB_date [DB2]
保持实际值
快照
将快照值复制到起始值中
MB_date
名称
数据类型
起始值
保持
Static
Slaver_IP
TCON_IP_v4
InterfaceId
HW_ANY
64
ID
CONN_OUC
1
ConnectionType
Byte
16#B
ActiveEstablished
Bool
false
RemoteAddress
IP_V4
ADDR
Array[1..4] of Byte
ADDR[1]
192
ADDR[2]
168
ADDR[3]
0
ADDR[4]
88
RemotePort
UInt
0
LocalPort
UInt
502
disconect
Bool
false
REQ1
Bool
false
disconect_1
Bool
false
MODE1
Int
0
第一步
第二步
设置变量名称
第三步
设置变量类型
第四步
设置初始值
详细视图

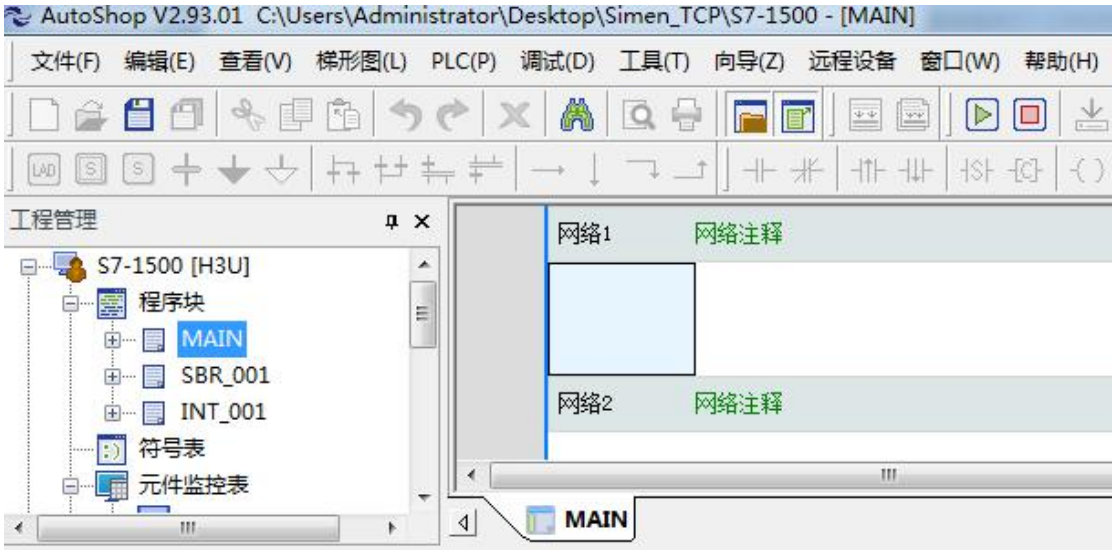


	元件名称	数据类型	显示格式	当前值	注释
	D0	16位整数	十进制	23	
	D1	16位整数	十进制	3	
	D2	16位整数	十进制	1066	
	D3	16位整数	十进制	3141	
	D4	16位整数	十进制	4141	
	D5	16位整数	十进制	13	
	D6	16位整数	十进制	0	
	D7	16位整数	十进制	14	
	D8	16位整数	十进制	0	
0	D9	16位整数	十进制	1313	
1	D10	16位整数	十进制	0	
2	D11	16位整数	十进制	0	
3	D12	16位整数	十进制	0	
4	D13	16位整数	十进制	0	
5	D14	16位整数	十进制	0	
6	D15	16位整数	十进制	0	


项目树
设备
S7-1500_TCP_H3u ▸ PLC_1 [CPU 1516-3 PN/DP] ▸ 程序块 ▸ DB2 [DB3]
DB2
S7-1500_TCP_H3u
添加新设备
设备和网络
PLC_1 [CPU 1516-3 PN/DP]
设备组态
在线和诊断
程序块
添加新块
Main [OB1]
DB1 [DB2]
DB2 [DB3]
系统块
工艺对象
外部源文件
PLC 变量
PLC 数据类型
详细视图
名称 数据类型 偏移量 起始值 监视值 保持 可从 HMI/... 从 H...
Static
date Array[0..100] of UInt 0.0
date[0] UInt 0.0 0 23
date[1] UInt 2.0 0 3
date[2] UInt 4.0 0 1066
date[3] UInt 6.0 0 3141
date[4] UInt 8.0 0 4141
date[5] UInt 10.0 0 13
date[6] UInt 12.0 0 0
date[7] UInt 14.0 0 14
date[8] UInt 16.0 0 0
date[9] UInt 18.0 0 1313
date[10] UInt 20.0 0 0
date[11] UInt 22.0 0 0
date[12] UInt 24.0 0 0
date[13] UInt 26.0 0 0
date[14] UInt 28.0 0 0
date[15] UInt 30.0 0 0
date[16] UInt 32.0 0 0
date[17] UInt 34.0 0 0


Siemens - C:\Users\Administrator\Desktop\Simen_TCP\S7-1500_TCP\S7-1500_TCP_H3u\S7-1500_TCP_H3u
项目(P) 编辑(E) 视图(V) 插入(I) 在线(O) 选项(N) 工具(T) 窗口(W) 帮助(H)
项目树
设备
S7-1500_TCP_H3u ▸ PLC_1 [CPU 1516-3 PN/DP] ▸ 程序块 ▸ Main [OB1]
块接口
PLC 编程
添加新设备
设备和网络
PLC_1 [CPU 1516-3 PN/DP]
设备组态
在线和诊断
程序块
添加新块
Main [OB1]
DB1 [DB2]
DB2 [DB3]
系统块
程序资源
工艺对象
外部源文件
PLC 变量
PLC 数据类型
详细视图
名称 偏移量 数据类型
date 0.0 Array...
"MB_Client1"
MB_CLIENT
EN ENO
TRUE "MB_Client1".REQ REQ
FALSE "MB_Client1".DISCONNECT DISCONNECT
1 "MB_Client1".MB_MODE MB_MODE
40001 "MB_Client1".MB_DATA_ADDR MB_DATA_ADDR
10 "MB_Client1".MB_DATA_LEN MB_DATA_LEN
P#DB3.DBX0.0 BYTE 20 P#DB3.DBX... MB_DATA_PTR
"DB1".TCON CONNECT
DONE FALSE "MB_Client1".DONE
BUSY TRUE "MB_Client1".BUSY
ERROR FALSE "MB_Client1".ERROR
STATUS 16#7006 "MB_Client1".STATUS





	元件名称	数据类型	显示格式	当前值	注释
1	D0	16位整数	十进制	424	
2	D1	16位整数	十进制	5	
3	D2	16位整数	十进制	35	
4	D3	16位整数	十进制	0	
5	D4	16位整数	十进制	11	
6	D5	16位整数	十进制	0	
7	D6	16位整数	十进制	-12	
8	D7	16位整数	十进制	0	
9	D8	16位整数	十进制	-14	
10	D9	16位整数	十进制	56	
11	D10	16位整数	十进制	0	
12	D11	16位整数	十进制	0	
13	D12	16位整数	十进制	0	
14	D13	16位整数	十进制	0	
15	D14	16位整数	十进制	0	

3. 汇川 H3u AutoShop3.0 设置

H3u 做从站，服务器。只需要在以太网配置中，设置好 IP 地址即可。

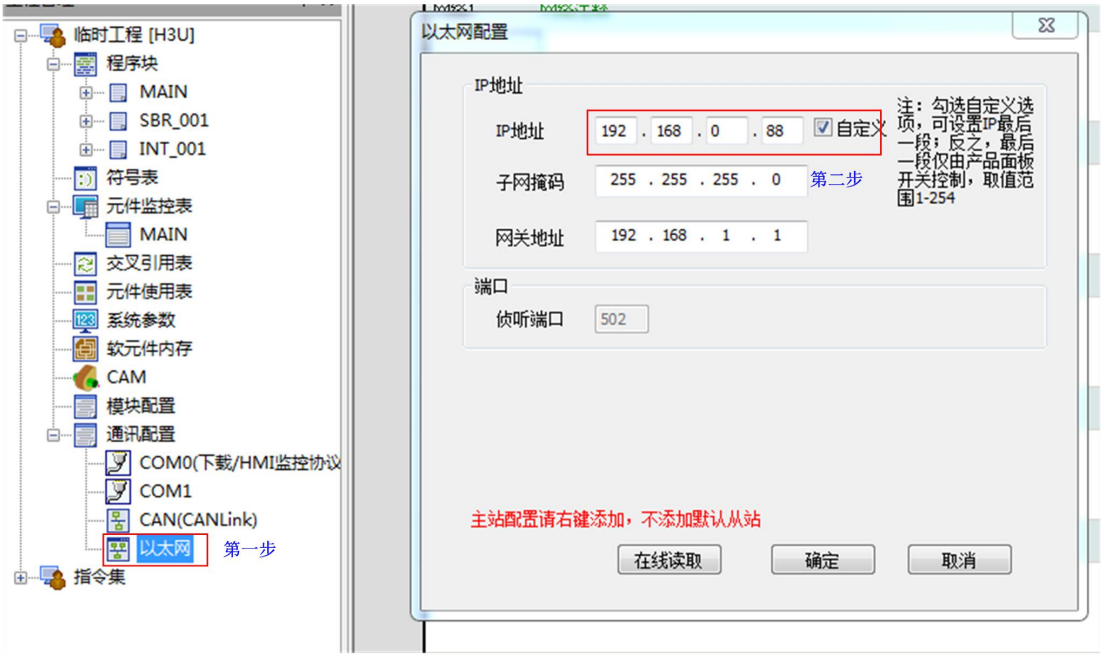


图 2.3.0 H3u 以太网设置