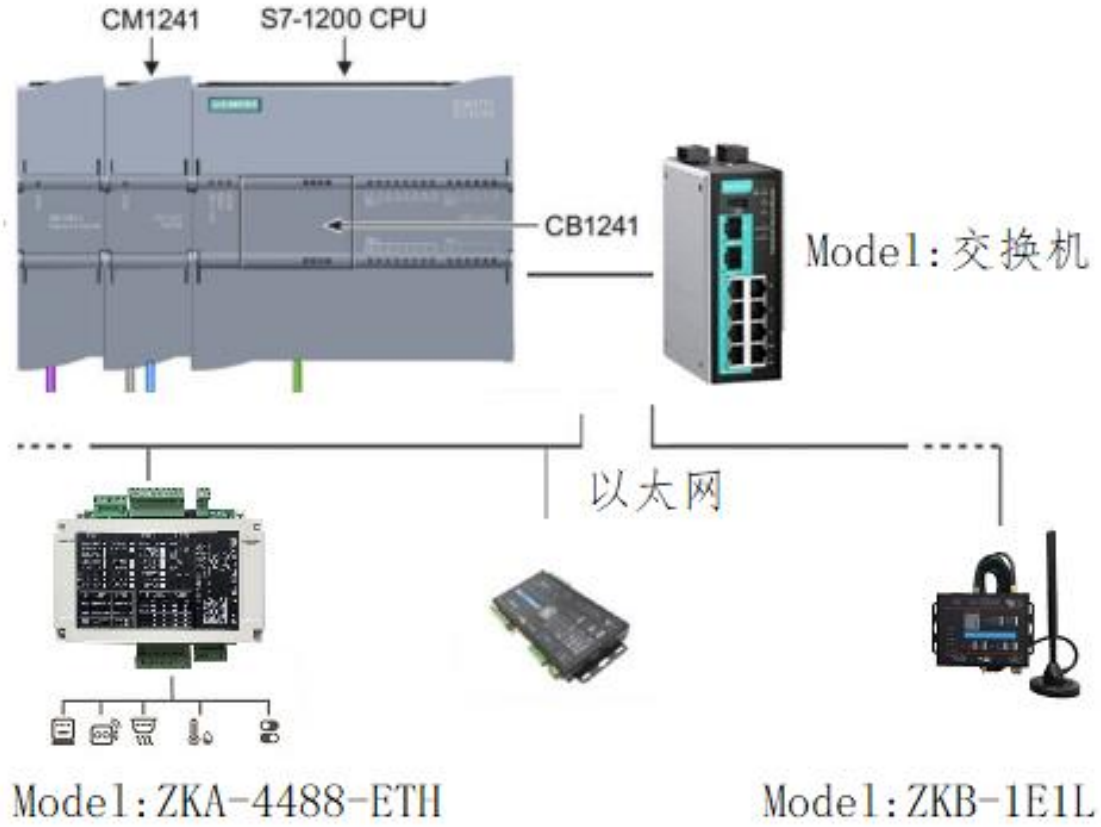
西门子S7-1200 Modbus-TCP 通信例子

【】绝密
【】NDA
【X】公开

一、 组网概述

本文以 ZKA-4488-ETH 为例介绍西门子PLC与深圳市综科智控科技开发有限公司的IO设备进行Modbus通讯的步骤设置。ZKA-4488-ETH 是 8 路数字量输入（DI），8 路数字量输出（DO），4 路模拟量输入（AI，0/4-20mA），4 路模拟量输出设备（AO，0/4-20mA），以太网通信。



以 ZKA-4488-ETH 为例，出厂默认通讯参数如下：

ZK模块 IP 为：192.168.0.105

TCP 端口为：10001
(注意：我们模块出厂时默认端口为10001，客户也可以通过ZK模块的配置文件把ZK通讯端口改成modbus-tcp的默认端口502)

工作模式为：服务器模式

二、 S7-200 Modbus TCP 通信

1 S7-200 Modbus TCP 通信简介

Modbus 是公开通信协议，详细的协议和规范，请访问 Modbus 组织的网站：http://www.modbus.org/

S7-1200 CPU 本体上集成了一个 PROFINET 通信口，支持以太网和基于 TCP/IP 和 UDP 的通信标准。这个 PROFINET 物理接口是支持 10/100Mb/s 的 RJ45 口，支持电缆交叉自适应，因此一个标准的或是交叉的以太网线都可以用于这个接口。使用这个通信口可以实现 S7-1200 CPU 与编程设备的通信，与 HMI 触摸屏的通信，以及与其它 CPU 之间的通信，

S7-1200 CPU 的 PROFINET 通信口主要支持以下通信协议及服务

- Profinet IO （V2.0 开始）
- S7 通信 （V2.0 开始支持客户端）
- TCP
- ISO on TCP
- UDP（V2.0 开始）
- Modbus TCP
- HMI 通信
- Web 通信（V2.0 开始）。

硬件版本 V4.1 支持的协议和最大的连接资源：

S7-1200 的连接资源

分配给每个类别的预留连接资源数为固定值；您无法更改这些值。 但可组态 6个"可用自由连接"以按照应用要求增加任意类别的连接数。

	编程终端 (PG)	人机界面 (HMI)	GET/PUT 客户端/服务器	开放式用户通信	Web 浏览器
连接资源的最大数量	3（保证支持 1 个 PG 设备）	12（保证支持 4 个 HMI 设备）	8	8	30（保证支持 3 个 Web 浏览器）

● 示例 1: 1 个 PG 具有 3 个可用连接资源。 根据当前使用的 PG 功能，该 PG 实际可能使用其可用连接资源的 1、2 或 3。 在 S7-1200 中，始终保证至少有 1 个 PG，但不允许超过 1 个 PG。

在 CPU 属性>常规>连接资源显示:

连接资源

	站资源			模块资源
	预留		动态	PLC [CPU 1215FC DC/DC/DC
最大资源数：		62	6	68
	最大	已组态	已组态	已组态
PG 通信：	4	-	-	-
HMI 通信：	12	2	0	2
S7 通信：	8	0	0	0
开放式用户通信：	8	0	0	0
Web 通信：	30	-	-	-
其它通信:	-	-	0	0
使用的总资源：		2	0	2
可用资源：		60	6	66

硬件版本 V3.0 支持的协议和最大的连接资源：

- 3 个连接用于操作面板
- 1 个连接用于编程设备（PG）与 CPU 的通信
- 8 个连接用于 Open IE (TCP, ISO on TCP, UDP) 的编程通信，使用 T-block 指令来实现
- 3 个连接用于 S7 通信的服务器端连接，可以实现与 S7-200，S7-300 以及 S7-400 的以太网 S7 通信
- 8 个连接用于 S7 通信的客户端连接，可以实现与 S7-200，S7-300 以及 S7-400 的以太网 S7 通信

连接数是固定不变的，不能自定义。

注意：建立被动的 TCP 、ISO on TCP 和 UDP 的连接时，建议使用端口范围: 2000~5000。一些端口号和 TSAP 号是受到限制不能被使用的。 下列端口号和 TSAP 号不能使用：

- ISO TSAP (passive): 01.00, 01.01, 02.00, 02.01, 03.00, 03.01
- TCP/UDP port (passive): 20, 21, 25, 80, 102, 135, 161, 34962 … 34964,53, 80, 162, 443, 520, 9001

2 Modbus TCP 指令库

S7-1200集成PN接口MODBUS TCP通信概述

Modbus TCP 是标准的网络通信协议，通过 CPU 上 PN 接口进行 TCP/IP 通信，不需要额外的通信硬件模块，Modbus TCP 使用开放式用户通信连接作为 Modbus 通信路径，所支持的混合客户机和服务器连接数最大为 CPU 所允许的最大开放式用户通信连接数 8 个。

软件 STEP7 V11 SP1 版本开始，S7-1200CPU 从 Firmware V1.0.2 开始，不再需要安装 Modbus TCP 的库文件，可以直接调用 Modbus TCP 的库指令“MB_CLIENT”和“MB_SERVER”使用实现 Modbus TCP 通信功能，如图 1 所示。

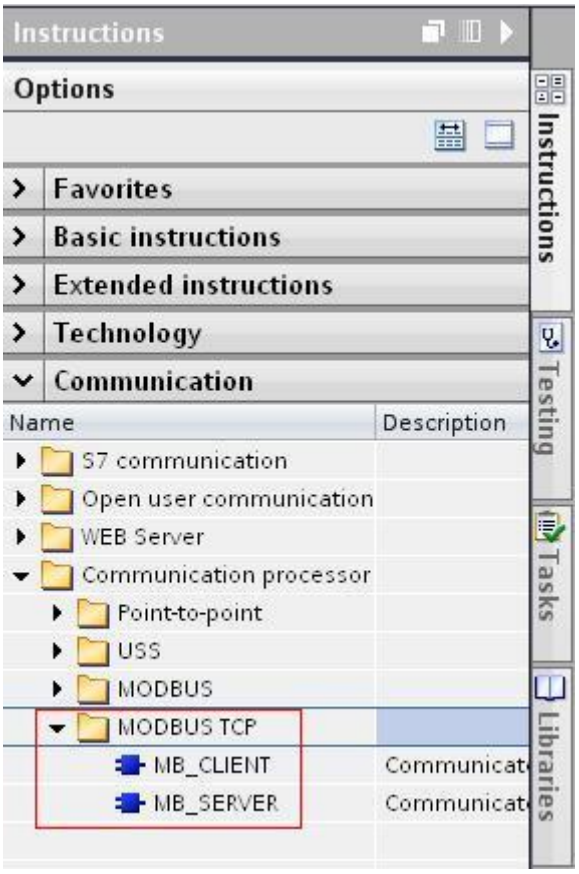


图 1. Modbus TCP 的库指令

3 Modbus TCP 功能编程

S7-1200 做Modbus Tcp Client（客户端）

MB_CLIENT 进行客户机和服务器 TCP 连接、发送命令消息、接收响应以及控制服务器的断开。

1.调用 MB_CLIENT 通信指令，进入 “Program blocks” > “OB1” 主程序中，调用 MODBUS TCP 客户机指令，如图 2 所示。

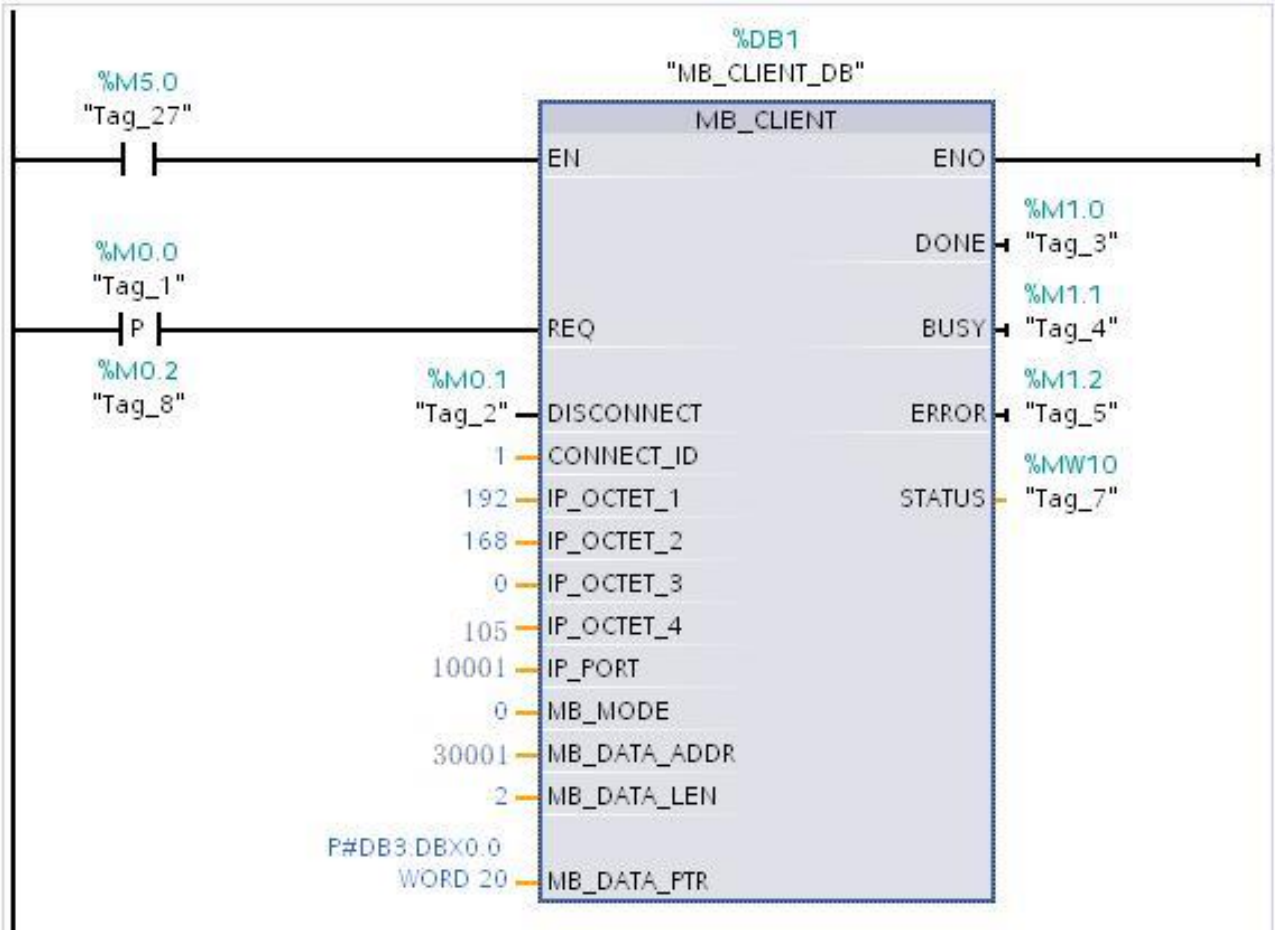


图 2. MB_CLIENT 通信指令

功能块参数意义如下表 1.：

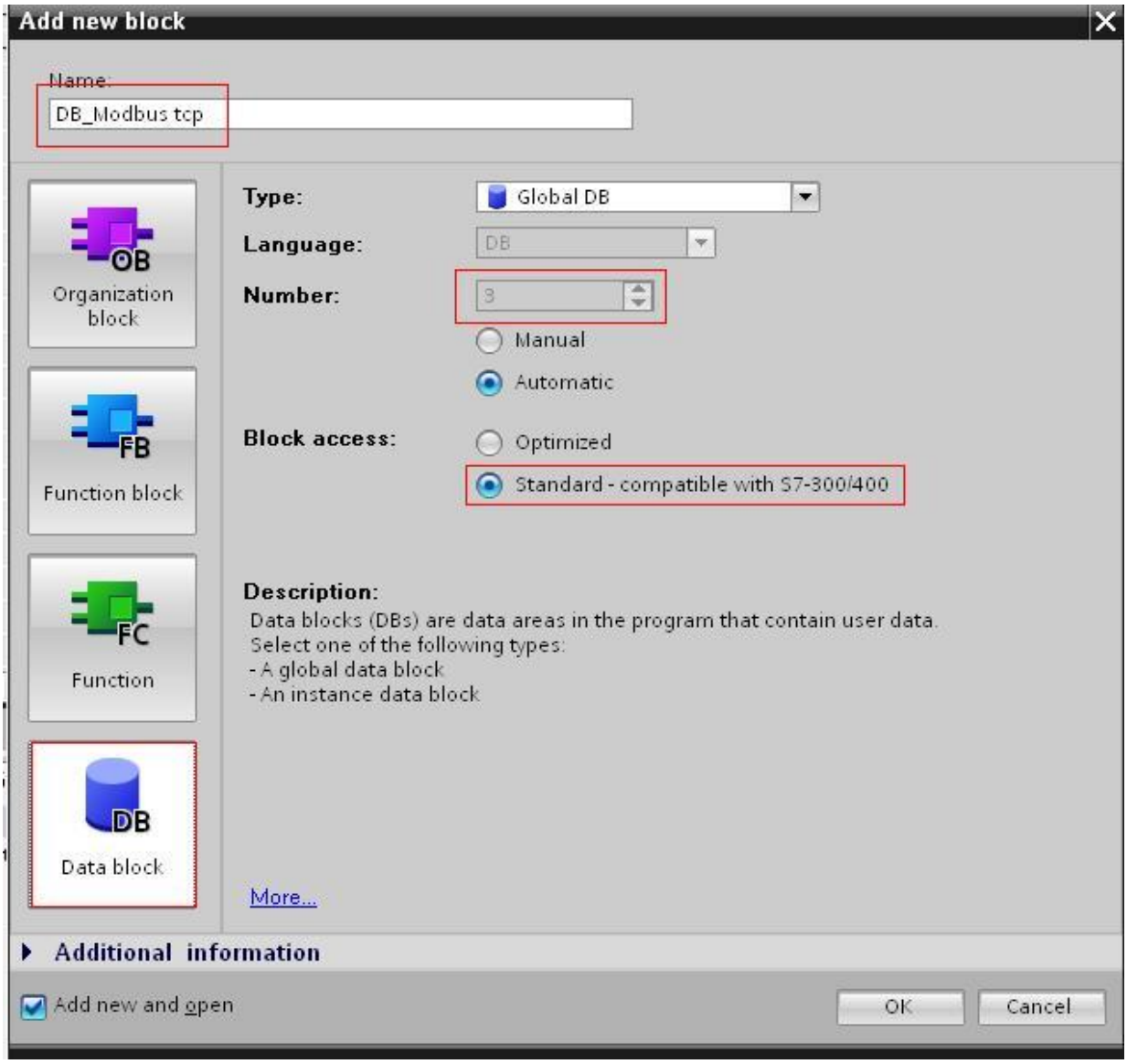
管脚	说明
REQ	使能： False-无Modbus通讯请求，True-请求与服务器通讯，Done完成位来后才可以执行下次请求，建议采用上升沿触发请求；
DISCONNECT	控制与服务器建立和终止连接：0-建立与指定IP地址和端口号的通讯连接，默认为0；1-断开通讯连接，在终止连接的过程中，不执行任何其他功能；
CONNECT_ID	连接的ID号：每个连接只有一个唯一的ID号；
IP_OCTET_1~4	ZKA-4488-ETH的IP地址
IP_PORT	ZKA-4488-ETH上使用TCP/IP协议与客户端建立通讯的IP端口号
MB_MODE	选择请求模式（读取、写入或诊断），具体对照参照表1.；
MB_DATA_ADDR	访问数据的起始地址；
MB_DATA_LEN	数据长度：数据访问的位数或字数；
MB_DATA_PRT	指向Modbus数据寄存器的指针：用于缓存从Modbus服务器接收的数据或将发送到Modbus服务器数据的缓冲区，可以是DB块或M区，如果是DB块则需要定

	义为“标准与S7- 300/400兼容”的类型，见下图3；
DONE	完成位：作业完成，无错误，该位置1；
BUSY	作业状态位：0-当前没有正在处理的“MB_CLIENT”作业；1-“MB_CLIENT”作业正在处理；
ERROR	错误位：0-无错误；1-出现错误，错误原因查看STATUS；
STATUS	错误代码；

表 1. 功能块参数意义

2.MB_DATA_PTR 数据块的新建

通过“Program blocks”>“Add new block”，选择“Data block”创建 DB 块，选择“标准与 S7-300/400 兼容”，点击“OK”键，定义数据区为 100 个字的数组，如图 3 所示。



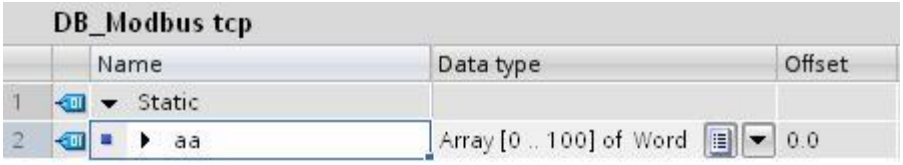


图 3. 创建 MB_DATA_PTR 数据块

3. MB_MODE、MB_DATA_ADDR 和功能码的关系

MB_CLIENT 指令中，MB_MODE、MB_DATA_ADDR 和 MB_DATA_LEN 三个参数组合定义了当前 Modbus 消息中所用的功能代码，如表 2.。

Modbus 功能	MB_MODE	MB_DATA_ADDR	操作和数据类型	数据长度
FC01	0	00001~09999	读取输出位 每个请求1~2000个位	1~2000
FC02	0	10001~19999	读取输入位 每个请求1~2000个位	1~2000
FC03	0	40001~49999 或 400001~465535	读取保持寄存器 每个请求1~125个字	1~125
FC04	0	30001~39999	读取输入字 每个请求1~125个字	1~125
FC05	1	00001~09999	写一个输出位 每个请求1个位	1
FC06	1	40001~49999 或 400001~465535	写一个保持寄存器 每个请求1个字	1
FC15	1	00001~09999	写多个输出位 每个请求2~1968个位	2~1968
FC16	1	40001~49999 或 400001~465535	写多个保持寄存器 每个请求2~123个字	2~123
FC15	2	00001~09999	写一个或多个输出位 每个请求1~1968个位	1~1968
FC16	2	40001~49999 或 400001~465535	写一个或多个保持寄存器 每个请求1~123个字	1~123
FC11	11		读取服务器通信状态字和事件计数器：状态字反映处理状态（0-未处理；0XFFFF-处理中）；每次成功发送一条消息后，事件计数器都将递增。执行功能时，MB_CLIENT指令的MB_DATA_ADDR和MB_DATA_LEN参数都将被忽略。	0
FC08	80		通过数据诊断代码0X0000检查服务器状态 每次请求1个字	1

FC08	81		通过数据诊断代码0X000A重新设置服务器事件计数器 每次请求1个字	1
	3~10、12~79、82~255		保留	

表 2. MB_MODE、MB_DATA_ADDR 和功能码的关系

如上例中 S7-1200 作客户机，用 **FC04** 功能码读取 ZKA-4488-ETH 的模拟输入 AI1 通道的读数的两个字，起始从 Modbus 地址 30001 开始，接收的数据存放在缓冲区 DB3.DBX0.0 开始区域，设置如上：MB_MODE=0，MB_DATA_ADDR=30001，MB_DATA_LEN=2，对应关系为：30001->DB3.DBW0 ，30002->DB3.DBW2。

注意：Slave ID 是 ZKA-4488-ETH 的站地址，和客户机中“MB_CLIENT” 中的“CONNECT_ID” 不是一个概念，实际上与客户机中“MB_CLIENT”的背景数据块中的 STAT 变量“MB_UNIT_ID”需要一致，在 1200 中该地址默认为 16#00FF，实际使用时可以改成 1，即：与 ZKA-4488-ETH 配置文件中的站号保持一致，当 S7-1200 挂接了多个 ZKA-4488-ETH 时，该值可以按序编号，也可以都使用值 1，因为 modbus-tcp 依然可以根据指向的 IP 地址发送数据。

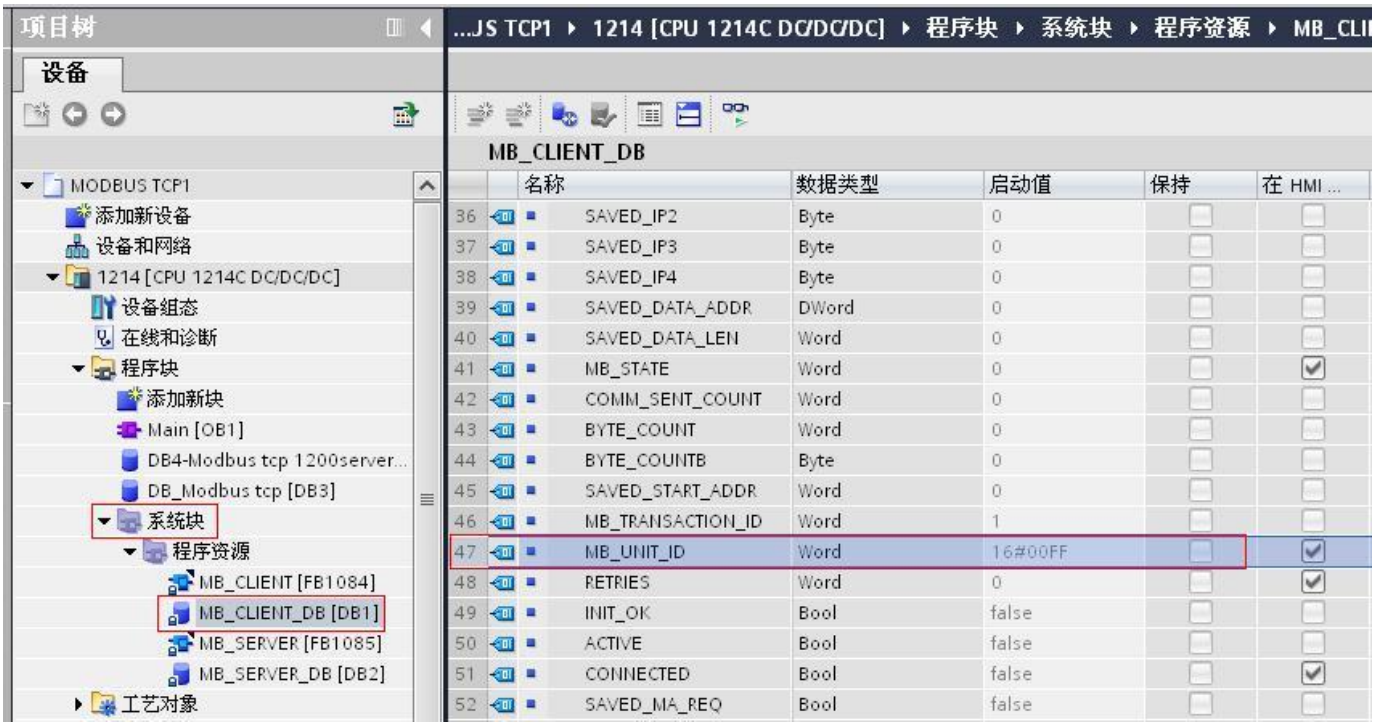


图 7. 客户机中“MB_CLIENT”的背景数据块中的 STAT 变量“MB_UNIT_ID”

5.通讯测试

S7-1200 作客户机，用 FC04 功能码读取 ZKA-4488-ETH 的两个字，设置客户机和 ZKA-4488-ETH 的功能、起始地址、端口等参数相对应，具体设置如上，设置 M5.0 和 M0.0 为 1，触发请求，如图 8 所示。

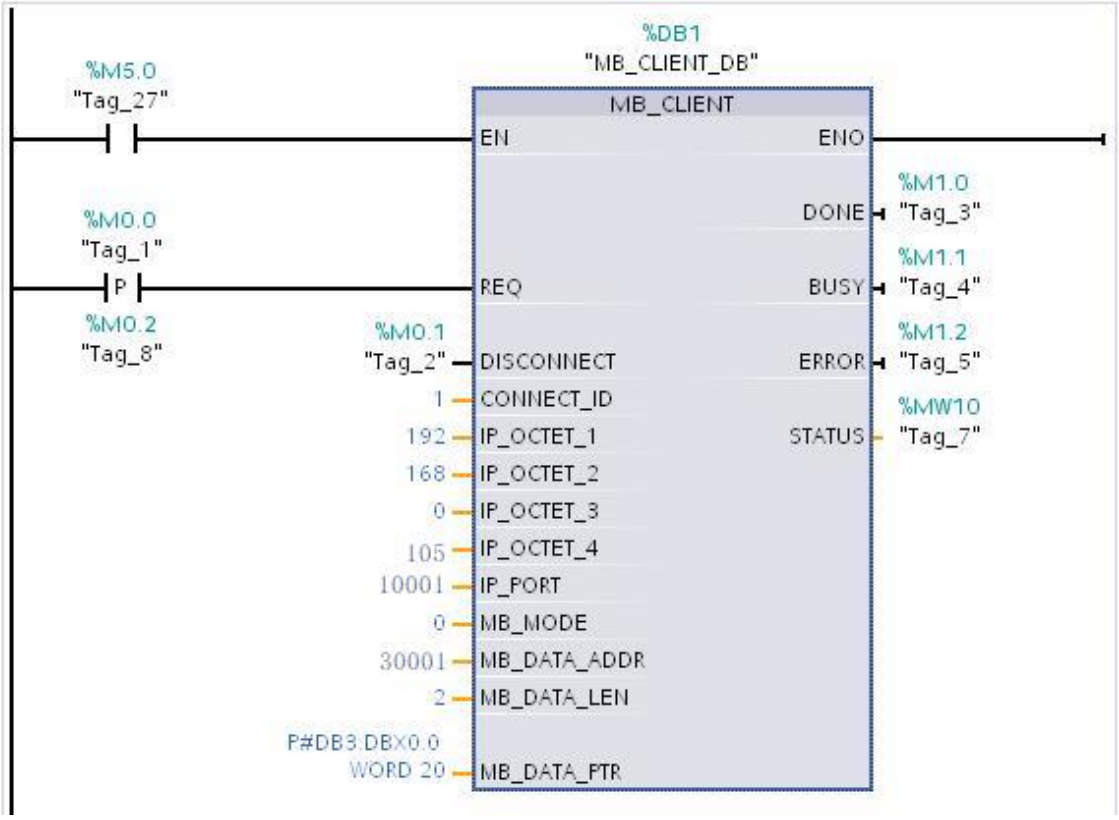


图 8. S7-1200 作客户机，用 FC04 功能码读取服务器的两个字

通讯结果如图 9 所示，从服务器读到数据 00，11 到客户机的 DB3.DBW0 和 DB3.DBW2 区域。

	i	名称	地址	显示格式	监视值
1		"DB_Modbus tcp".aa[0]	%DB3.DBW0	无符号十进制	00
2		"DB_Modbus tcp".aa[1]	%DB3.DBW2	无符号十进制	11

图 9. 通讯结果

6.MB_CLIENT 参数 STATUS 错误代码查询参考下面两个列表 3.和表 4.。

STATUS(W#16#)	Modbus服务器返回的代码（B#16#）	错误说明
8381	01	不支持功能代码
8382	03	数据长度错误
8383	02	数据地址错误或访问的数据超出MB_DATA_PTR的地址区
8384	03	数据值错误
8385	03	不支持诊断错误代码（功能代码08）

表 3. 协议错误代码

STATUS(W#16#)	错误说明
7001	MB_CLIENT 正在等待Modbus服务器响应指定TCP端口处的连接或断开连接请求，仅在第一次执行连接或断开操作时才报告此代码
7002	MB_CLIENT 正在等待Modbus服务器响应指定TCP端口处的连接或断开连接请求，等待连接或断开操作完成时，将针对任何后续执行报告此代码
7003	断开操作已成功完成（仅在一个PLC扫描周期内有效）
80C8	服务器在指定的时间内无响应，请检查与Modbus服务器设备的连接，尝试过任何组态的重试操作后，才报告此错误
8188	参数MB_MODE的值无效
8189	参数MB_DATA_ADDR的值无效
818A	参数MB_DATA_LEN的长度无效
818B	参数MB_DATA_PTR中的指针无效
818C	参数MB_DATA_PTR指向优化的区域，必须为“标准与S7- 300/400兼容”的DB或M区
8200	端口正在处理另一个Modbus请求
8380	接收到的Modbus桢有缺陷或接收到的字节太少
8387	指定的连接ID与用于先前请求的ID不同，只能有一个单个连接ID与每个MB_CLIENT背景数据块配合使用
8388	Modbus服务器返回一些和请求内容不同的数据，这只适合Modbus功能15或16

表 4. 参数错误代码

除了上面列出的 MB_CLIENT 错误外，也可以从底层传输通信指令（TCON、TDISCON、TSEND 和 TRCV）返回错误，参考相应指令的错误代码。

5 Modbus TCP 常问问题

MB_CLIENT 指令的背景数据块中的 "MB_Unit_ID" 有什么功能？

注意：Slave ID 是 ZKA-4488-ETH 的站地址，和客户机中“MB_CLIENT” 中的“CONNECT_ID” 不是一个概念，实际上与客户机中“MB_CLIENT”的背景数据块中的 STAT 变量“MB_UNIT_ID”需要一致，在 1200 中该地址默认为 16#00FF，实际使用时可以改成 1，即：与 ZKA-4488-ETH 配置文件中的站号保持一致，当 S7-1200 挂接了多个 ZKA-4488-ETH 时，该值可以按序编号，也可以都使用值 1，因为 modbus-tcp 依然可以根据指向的 IP 地址发送数据：

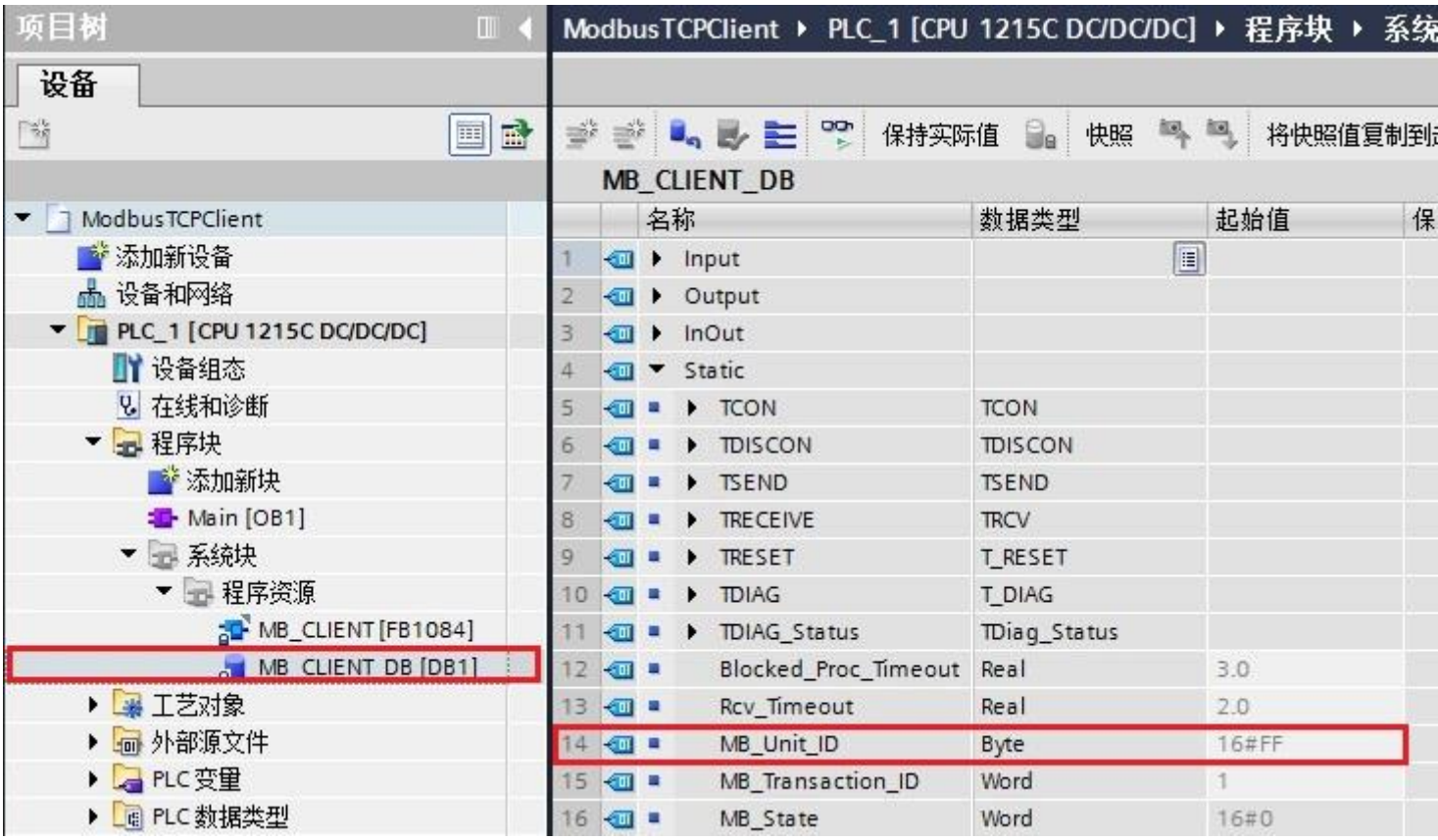


图 11. MB_Unit_ID

S7-1200 MODBUS TCP 通信多请求处理怎么做?

单独的客户机连接需要遵循的规则：

1.每个“MB_CLIENT”连接需要使用一个不同的背景数据块；

2.每个“MB_CLIENT”连接必须指定一个服务器 IP 地址；

3.每个“MB_CLIENT”连接必须指定一个唯一的连接 ID；

4.是否需要唯一的 IP 端口号取决于服务器组态；

连接 ID 和背景数据块组合成对，对每个连接来说，组合对都是唯一的。

对于多请求处理，有两种方法：

方法一：如果 TCP 连接充裕，可以建立多个不同的连接发送请求，即每个请求使用一个独立的连接，调用独立的“MB_CLIENT”功能块，具体操作参考“Modbus TCP”部分。通过不同的连接发送多个请求，“MB_CLIENT”功能块多次调用，但是需要使用不同的背景数据块，不同的 ID 号和不同的端口号。

方法二：通过公共的连接发送多个请求。

通过公共的连接发送多个请求，“MB_CLIENT”功能块多次调用，但是需要使用相同的背景数据块，连接 ID 号，IP 地址和端口号。在任意时间，只能有一个 MB_CLIENT 请求处于激活状态，在一个请求完成执行后，下一个请求再开始执行，轮循处理。

在此，我们以方法二为例，介绍 S7-1200 如何通过分次请求获取 ZKA-4488-ETH 内部寄存器的数据：

1.S7-1200 的 IP 地址 192.168.1.218，将系统存储器字节设置为 MB1，如图 1 所示，图 2 所示。

图 1 IP 地址设置

图 2 系统存储器字节设置

1.新建数据块，访问指向 ZKA-4488-ETH 的 IP 地址和端口号

如图 6 所示，新建 DB，添加变量类型为 TCON_IP_V4，设置 InterfaceId，ID，ActiveEstablished，RemoteAddress，RemotePort 等参数，具体含义参见链接。

DB1

名称	数据类型	起始值
Static		
Static_1	TCON_IP_v4	
InterfaceId	HW_ANY	64
ID	CONN_OUC	1
ConnectionType	Byte	16#0B
ActiveEstablished	Bool	1
RemoteAddress	IP_V4	
ADDR	Array[1..4] of Byte	
ADDR[1]	Byte	192
ADDR[2]	Byte	168
ADDR[3]	Byte	0
ADDR[4]	Byte	105
RemotePort	UInt	10001
LocalPort	UInt	0

图 6 设置连接变量

如图 7 所示，在 DB 中建立结构数组，用于轮询控制位以及数据，其中元素 0 用于第一次读取，元素 1 用于第二次读取。Init 用于初始标志位。

DB1

名称	数据类型	起始值
Static		
Static_1	TCON_IP_v4	
Static_2	Array[0..1] of Struct	
Static_2[0]	Struct	
Data	Array[0..1] of Word	
Data[0]	Word	16#0
Data[1]	Word	16#0
Enable	Bool	false
Enable_Trig	Bool	false
Done	Bool	false
Error	Bool	false
Static_2[1]	Struct	
Data	Array[0..1] of Word	
Data[0]	Word	16#0
Data[1]	Word	16#0
Enable	Bool	false
Enable_Trig	Bool	false
Done	Bool	false
Error	Bool	false
Init	Bool	false

图 7 轮询数据

2.编写轮循功能

1）如图 8 所示，用“FirstScan”在第一次扫描中将初始标志位置位。

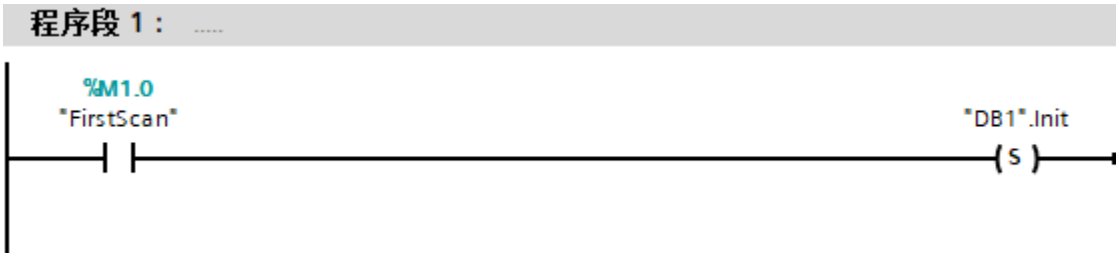
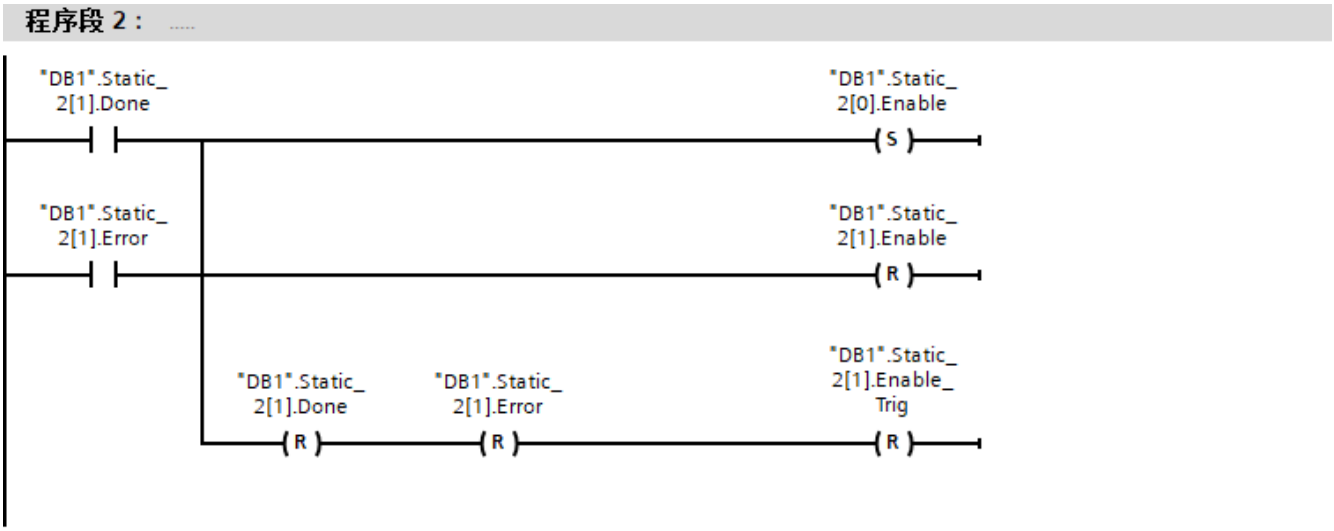


图 8 初始化标志位

2）如图 9 所示，程序段 2 中，第二步的完成位或者错误位去置位第一步的使能位复位第二步的使能位，同时复位第二步的完成位、错误位、触发的沿变量。

程序段 3 中，一般情况下是 EN 通过第一步的使能位使能，REQ 通过使能位的上升沿触发，设置模式、读取数据地址、长度、存储地址、连接数据、完成、错误位等。此外需要考虑第一次触发轮询，可以使用手动触发，在这里使用初始化标志位实现指令的第一次使能，去进行 CPU 和调试软件的 TCP 连接，使用 Connected 标志位触发第一次的 REQ 触发。



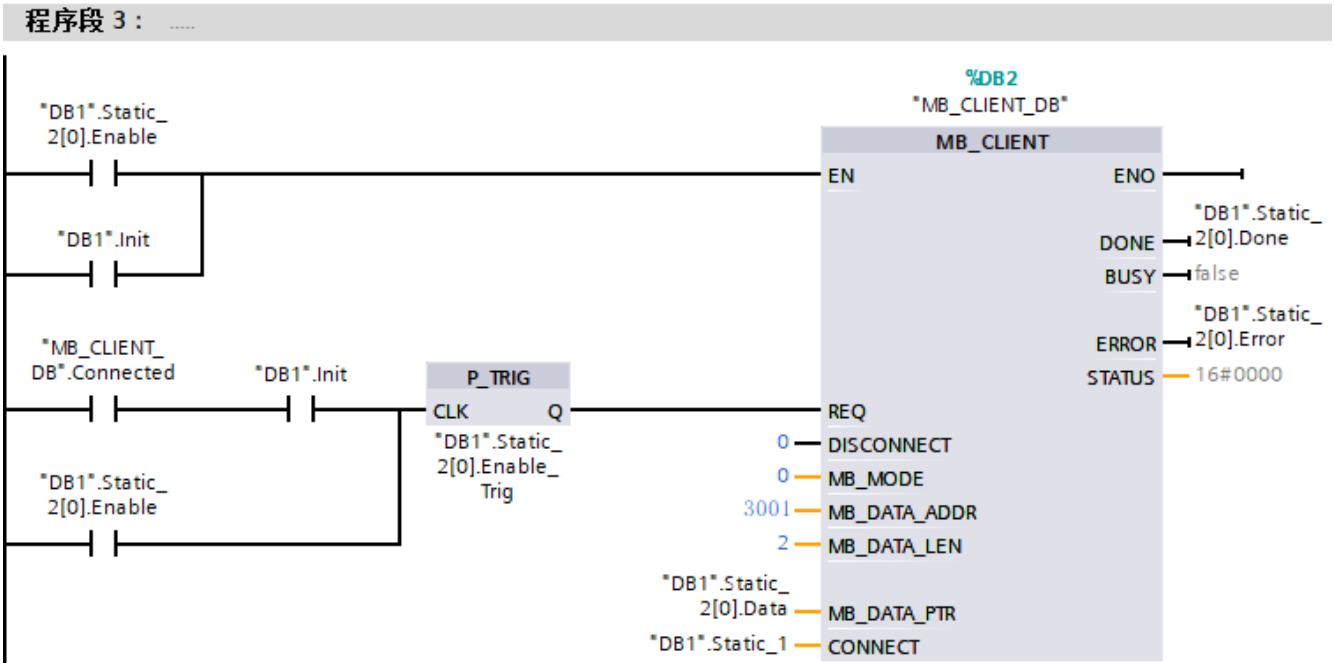
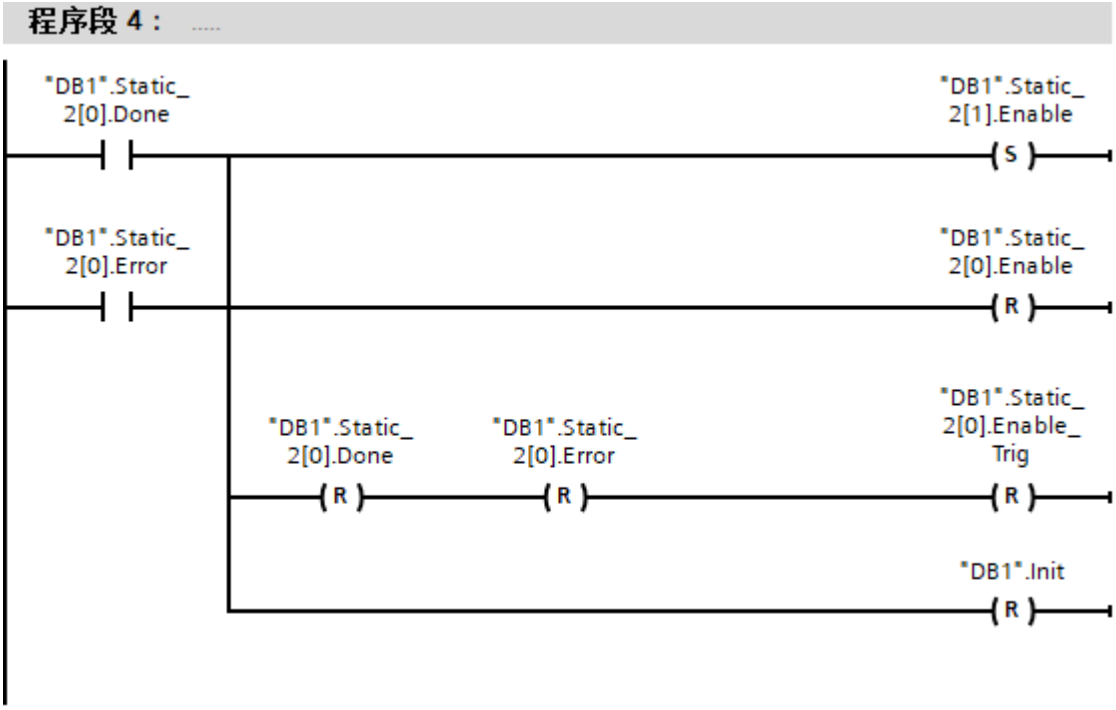


图 9 请求 1 触发

如图 10 所示，程序段 4 中，第一步的完成位或者错误位去置位第二步的使能位复位第一步的使能位，同时复位第一步的完成位、错误位、触发的沿变量，最后复位初始化标志位，确保第一个 MB_CLIENT 不会一直接通。

程序段 5 中，EN 通过第二步的使能位使能，REQ 通过使能位的上升沿触发，设置模式、读取数据地址、长度、存储地址、连接数据、完成、错误位等。



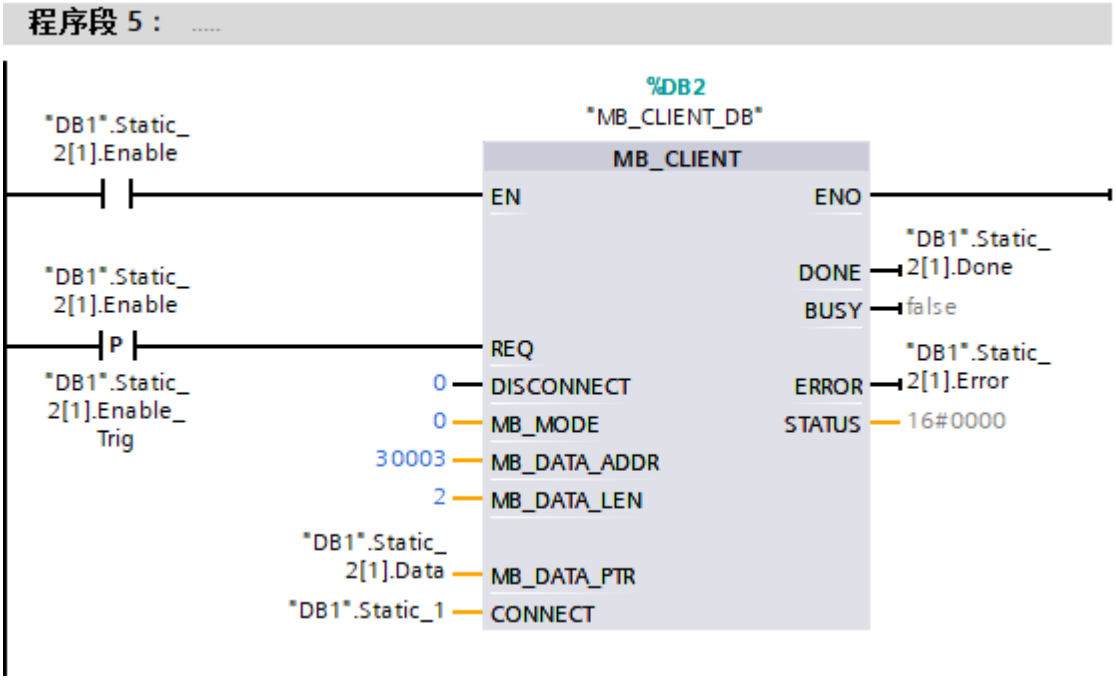


图 10 请求 2 触发

五.通讯测试

通讯结果如图 11 所示。

DB1

名称	数据类型	起始值	监视值
Static			
Static_1	TCON_IP_v4		
Static_2	Array[0..1] of Struct		
Static_2[0]	Struct		
Data	Array[0..1] of Word		
Data[0]	Word	16#0	16#0001
Data[1]	Word	16#0	16#0002
Enable	Bool	false	FALSE
Enable_Trig	Bool	false	FALSE
Done	Bool	false	FALSE
Error	Bool	false	FALSE
Static_2[1]	Struct		
Data	Array[0..1] of Word		
Data[0]	Word	16#0	16#0003
Data[1]	Word	16#0	16#0004
Enable	Bool	false	TRUE
Enable_Trig	Bool	false	TRUE
Done	Bool	false	FALSE
Error	Bool	false	FALSE
Init	Bool	false	FALSE

图 11 测试结果

注意：

1.如果需要更多的读写任务可以按照例子自行添加。