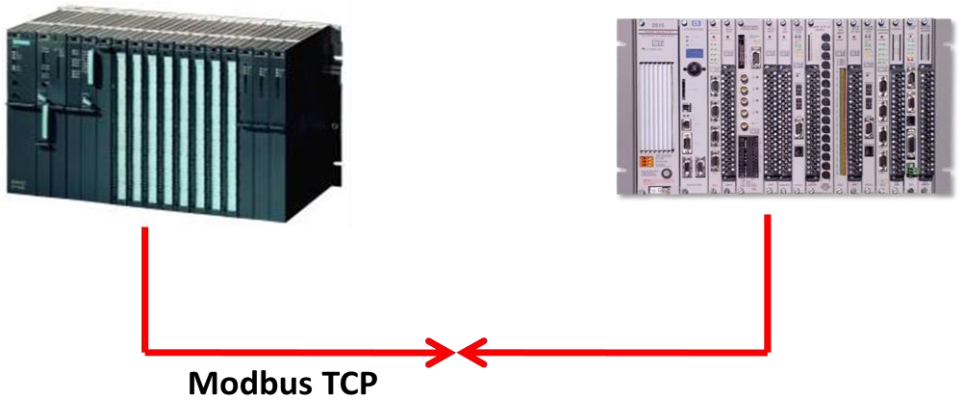
CTI 2500 Series™ System
Application Note

Application Note:

Communication between CTI 2500 Series™ PLC and SIMATIC® S7 PLC using the Open MODBUS /TCP protocol

Application

A CTI 2500 Series™ or Simatic® 505 PLC is used to exchange data with a Siemens® S7 PLC. Modbus Registers can be written to or read from the CTI CPU. The S7 PLC is functioning as a Client and the CTI PLC as a Server.



Assumptions

- The CTI PLC uses the 2572-A/B 100Mbit Ethernet Adapter card as a network interface. Note the CTI 2572 10Mbit Ethernet Adapter cannot be used since it doesn't support the Open Modbus TCP protocol.
- The S7 PLC uses a CP343-1/443-1 card with a configured active connection to the CTI PLC – the Siemens® CP cards which are released for this application are 6GK74(3)43-1EX11-0XE0 or later versions.
- The S7 PLC is functioning as Client and the CTI PLC as Server – no programm is needed in the CTI PLC
- The IP address for the CP443-1 is 192.168.0.88
- The IP address for the 2572-A/B ia 192.168.0.87
- In this example the S7 PLC will send 100 words to the modbus register 40001 – 40100 which correpsonds to address V1 – V100 in the CTI PLC.
- FB100 "MODBUS" is used – this Function Block is not part of the standard Step7 package but has to be ordered separately - the MODBUS library can be ordered with the Siemens® partnumber 2XV9450-1MB00 and can be used in Step7 V5.1 or higher

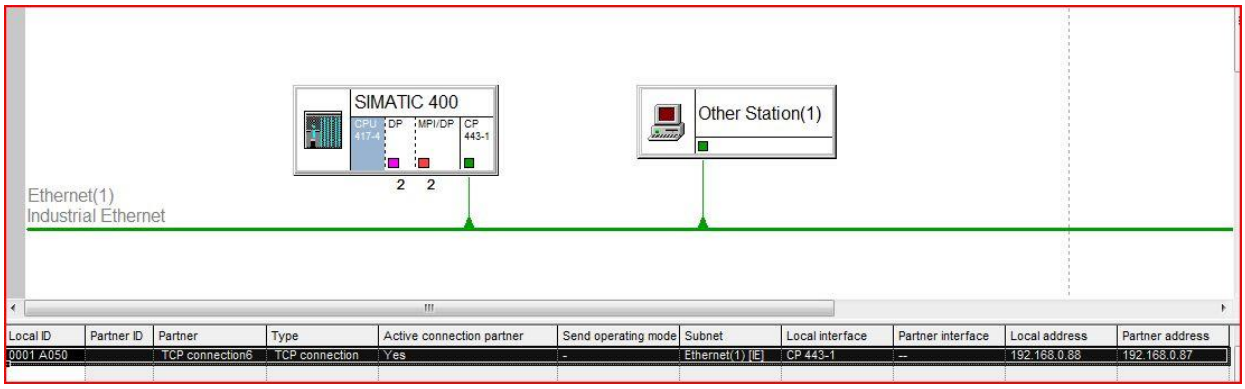
Description

All the configuration is done at the S7 side – only the IP address in the 2572-A/B should be adjusted. The S7 Modbus library comes with two Function Blocks FB100 “Modbus” and FB101 “Modb4”.

FB100 is applied to Conformance Class 0 with the functions read and write holding register FC3 and 16. FB101, which is a part of Conformance Class 1, supplies the additional function read input register FC4. In this example only FB100 is used to send 100 words from the S7 to the CTI PLC. For data transfer between the CP443-1 and the S7-400 CPU the functions FC50(AG_LSEND) and FC60(AG_LRECV) are used. The FB100 “Modbus” has to be called both in the startup OB100 as well as in the cyclic OB1. It is not allowed to call FB100 in a cyclic interrupt OB.

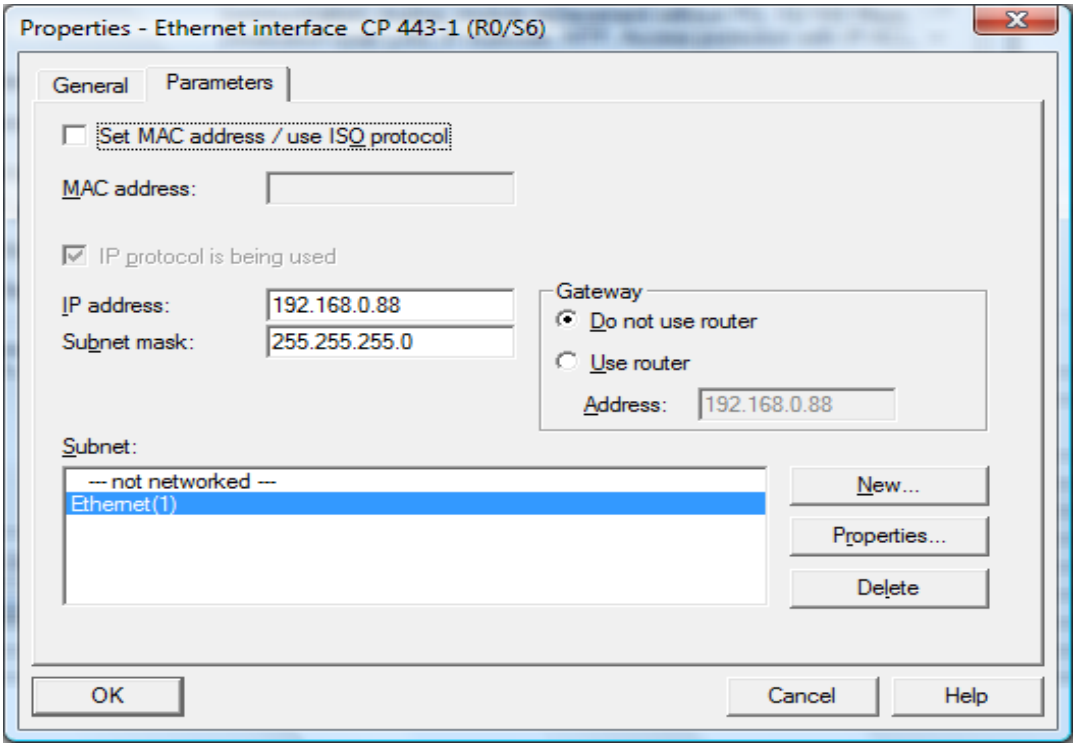
S7 Configuration

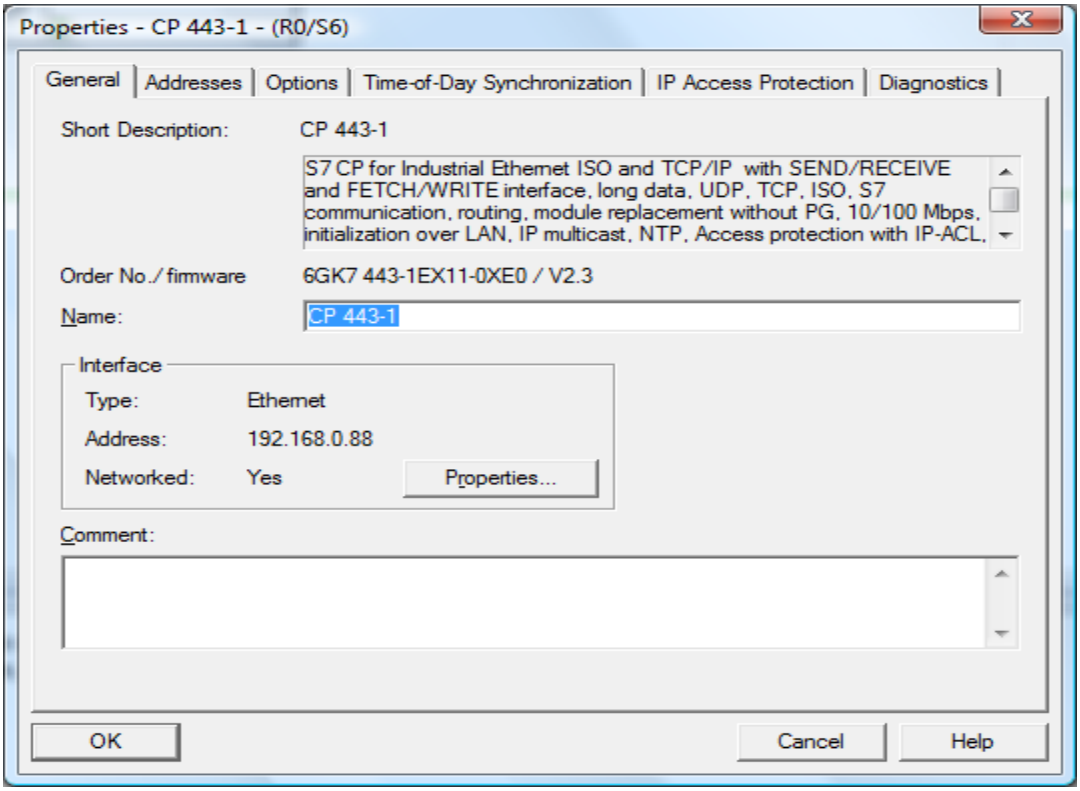
Using Step7, the hardware needs to be configured including an Ethernet network. For the CTI PLC the object “Other Station” is added in NetPro and both are connected to the network as shown below. On the CPU417-4 an active connection with the CTI PLC is configured which is used by the FB100 “Modbus” function.



Configuring the CP443-1 Ethernet Module

The CP443-1 uses the IP address 192.168.0.88 and is connected to the Ethernet network as shown below.

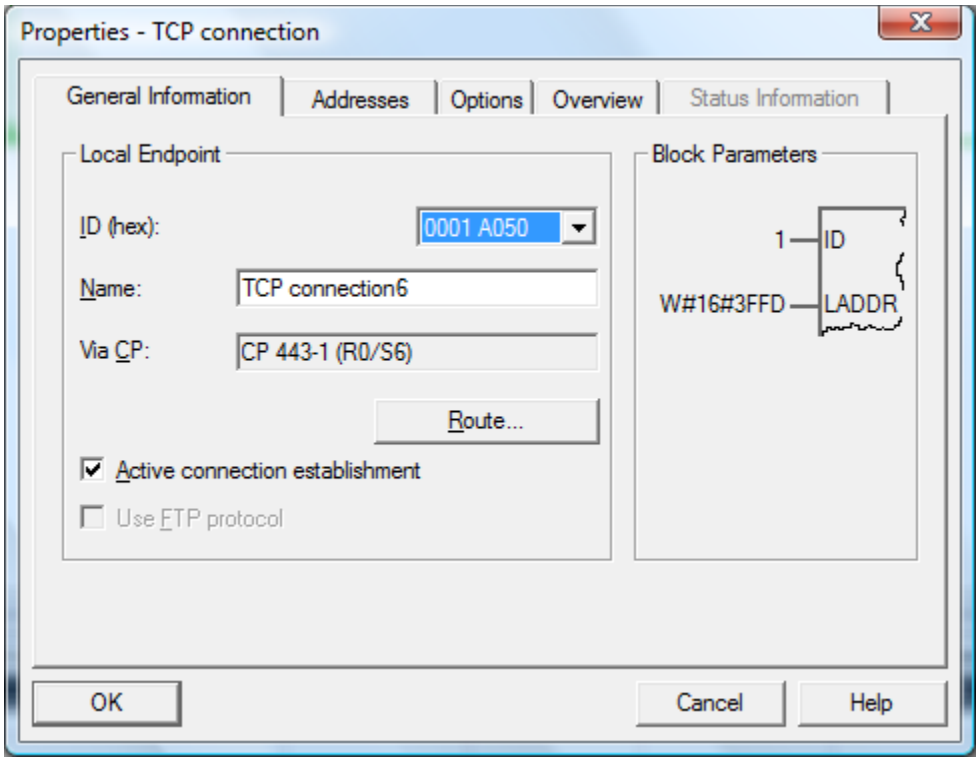


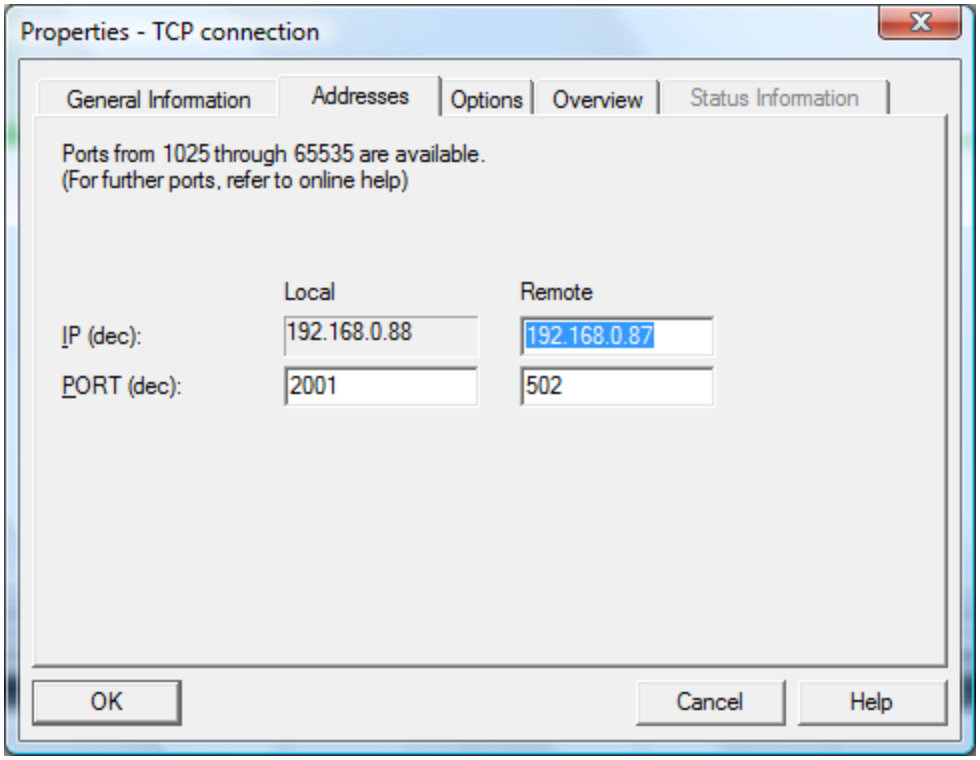


Configuring the TCP connection for the Open Modbus TCP protocol

Under General Information the ID number “1” and the CP LADDR “W#16#3FFD” can be read out. The “active connection establishment” feature needs to be selected.

For the Modbus TCP Server as a standard TCP port 502 is used and for the Client a different TCP port number – in this example 2001.





Data and Standard Functions used by the FB100 “Modbus”

The function block “Modbus” reads/stores its data from/in an instance DB. The instance DB contains parameters of the type Input, Output as well as static variables that it needs for its execution.

Parameters of the Function Block MODBUS

Parameter	Decl.	Type	Description	Value range
ID	IN	WORD	Connection-ID as per configuration in NetPro 1 to 64	W#16#1 to W#16#40
LADDR	IN	WORD	LADDR-Address of the CP from HW Config	CPU dependent
TIMER_NR	IN	TIMER	Timer number for response monitoring time	CPU dependent
MONITOR	IN	WORD	Monitoring Time: Wait for	W#16#1 to W#16#3E7

			data from communication partner; 100 ms units 1 to 999	
DB_1	IN	WORD	Data block number, first range 1 to 65535	W#16#1 to W#16#FFFF
START_1	IN	WORD	First MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
END_1	IN	WORD	Last MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
DB_2	IN	WORD Data block number, second range;	NULL if not used 1 to 65535 W#16#1 to W#16#FFFF	0
START_2	IN	WORD	First MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
END_2	IN	WORD	Last MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
DB_3	IN	WORD Data block number, third range;	NULL if not used 1 to 65535 W#16#1 to W#16#FFFF	0
START_3	IN	WORD	First MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
END_3	IN	WORD	Last MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF

DB_4	IN	WORD	Data block number, fourth range; NULL if not used 1 to 65535 W#16#1 to	0

			W#16#FFFF	
START_4	IN	WORD	First MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
END_4	IN	WORD	Last MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
DB_5	IN	WORD	Data block number, fifth range; NULL if not used 1 to 65535 W#16#1 to W#16#FFFF	0
START_5	IN	WORD	First MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
END_5	IN	WORD	Last MODBUS register address 0 to 65535	W#16#0000 to W#16#FFFF
WRITE_ PROTECT1	IN	BOOL	Area 1 is write protected (only in SERVER mode)	TRUE FALSE
WRITE_ PROTECT2	IN	BOOL	Area 2 is write protected (only in SERVER mode)	TRUE FALSE
WRITE_ PROTECT3	IN	BOOL	Area 3 is write protected (only in SERVER mode)	TRUE FALSE
WRITE_ PROTECT4	IN	BOOL	Area 4 is write protected (only in SERVER mode)	TRUE FALSE
WRITE_ PROTECT5	IN	BOOL	Area 5 is write protected (only in SERVER mode)	TRUE FALSE
ENQ_ENR	IN	BOOL CP is Client: Initiate request at TRUE signal	CP is Server: Ready to receive at TRUE signal	TRUE FALSE
SERVER_ CLIENT	IN	BOOL	CP/FB	TRUE FALSE

			operates in server mode or client mode	
DONE_NDR	OUT	BOOL CP is Client: Active request finished without errors	CP is Server: Request from the client was executed and answered	TRUE FALSE
ERROR	OUT	BOOL	An error has occurred.	TRUE FALSE
STATUS	OUT	WORD	Error number	0 to FFFF
START_ ADDRESS	IN/ OUT	WORD	MODBUS start address (INPUT if in CLIENT mode, OUTPUT if in SERVER mode) 0 to 65535	W#16#0000 to W#16#FFFF
LENGTH	IN/ OUT	BYTE Number of registers to be processed (INPUT if in CLIENT mode, OUTPUT if in SERVER mode) Read function	Write function 1 to 125 B#16#1 to B#16#7D 1 to 100	B#16#1 to B#16#64
WRITE_ READ	IN/ OUT	BOOL	Read or write access (INPUT if in CLIENT mode, OUTPUT if in SERVER mode)	TRUE FALSE
TI	IN/ OUT	WORD	Transaction Identifier (INPUT if in CLIENT mode, OUTPUT if in SERVER mode) 0 to 65535	W#16#0 to W#16#FFFF
UNIT	IN/ OUT	BYTE	Unit identification (INPUT if in CLIENT mode, OUTPUT if in SERVER mode) 0 to 255	B#16#0 to B#16#FF

Programming example when the CP443-1 is Client

100 words of data are written from DB11 in the S7 PLC into V1-V100 in the CTI PLC. The used blocks in the S7 programm are OB1 (cyclic OB which executes each cycle), OB100 (startup OB for restart), DB222 (datablock for Control Data) and DB700 (instance datablock for Modbus Data).

Programming Example

The blocks are listed as follows:

Block	Comment
OB 1	Cyclic Program Processing
OB 100	Start-Up OB for Re-start
DB 222	work-DB "CONTROL DAT" for FB MODBUS

In OB100, which is the startup OB, the connection to DB_1 is 11 (this means DB11 is connected) and the start_1 and end_1 are configured as 0 and 100 resp. Here also the parameter Server_Client is set to false which means that the CP443-1 acts as Client.

OB100 Start-Up-OB

```
Initialization of  FB MODBUS

OPN   "CONTROL DAT"                    //DB 222

L    1                                 //from NETPRO connection table
T    "CONTROL DAT".ID

L    2044                              //from HW Config
T    "CONTROL DAT".LADDR

L    11                                //first memory area
T    "CONTROL DAT".DB_1                //Register 1 to 500
L    1
T    "CONTROL DAT".START_1
L    500
T    "CONTROL DAT".END_1

L    12                                //second memory area
T    "CONTROL DAT".DB_2                //Register 501 to 600
L    501
T    "CONTROL DAT".START_2
L    600
T    "CONTROL DAT".END_2

L    13                                //third memory area
T    "CONTROL DAT".DB_3                //Register 601 to 700
L    601
T    "CONTROL DAT".START_3
L   700
T    "CONTROL DAT".END_3

L    0                                 //fourth memory area
T    "CONTROL DAT".DB_4                //not used
T    "CONTROL DAT".START_4
T    "CONTROL DAT".END_4

L    0                                 //fifth memory area
T    "CONTROL DAT".DB_5                //not used
T    "CONTROL DAT".START_5
T    "CONTROL DAT".END_5

CLR
=    "CONTROL DAT".SERVER_CLIENT       //CP is client
```

```
CALL  "MODBUS" , "MODBUS_DAT"
      ID                    :="CONTROL DAT".ID
      LADDR                 :="CONTROL DAT".LADDR
      TIMER_NR              :=
      MONITOR               :=
      DB_1                  :="CONTROL DAT".DB_1
      START_1               :="CONTROL DAT".START_1
      END_1                 :="CONTROL DAT".END_1
      DB_2                  :="CONTROL DAT".DB_2
      START_2               :="CONTROL DAT".START_2
      END_2                 :="CONTROL DAT".END_2
      DB_3                  :="CONTROL DAT".DB_3
      START_3               :="CONTROL DAT".START_3
      END_3                 :="CONTROL DAT".END_3
      DB_4                  :="CONTROL DAT".DB_4
      START_4               :="CONTROL DAT".START_4
      END_4                 :="CONTROL DAT".END_4
      DB_5                  :="CONTROL DAT".DB_5
      START_5               :="CONTROL DAT".START_5
      END_5                 :="CONTROL DAT".END_5
      WRITE_PROTECT1        :=
      WRITE_PROTECT2        :=
      WRITE_PROTECT3        :=
      WRITE_PROTECT4        :=
      WRITE_PROTECT5        :=
      ENQ_ENR               :="
      SERVER_CLIENT         :="CONTROL DAT".SERVER_CLIENT
      DONE_NDR              :=
      ERROR                 :="CONTROL DAT".ERROR
      STATUS                :="CONTROL DAT".STATUS
      START_ADDRESS         :=
      LENGTH                :=
      WRITE_READ            :=
      TI                    :=
      UNIT                  :=
```

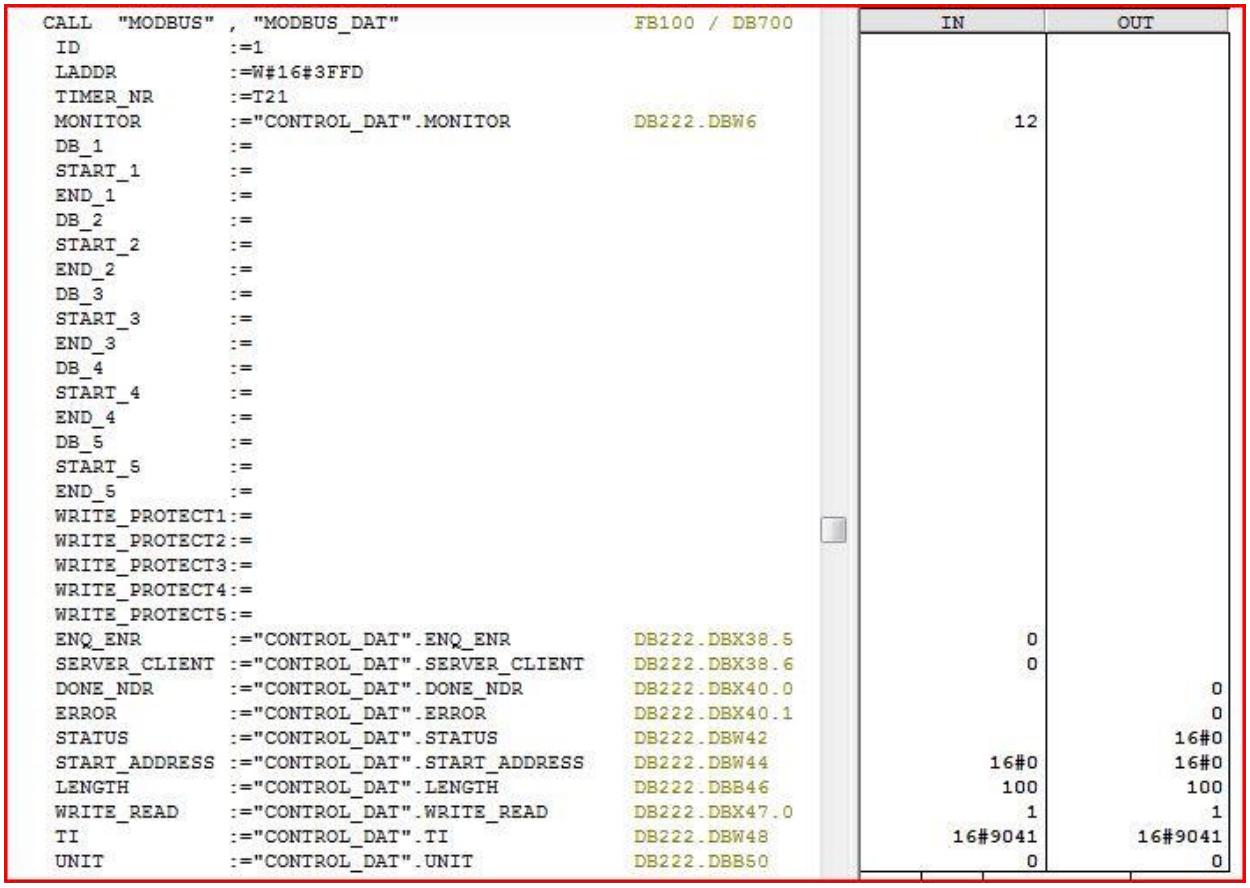
In OB1, which is the cyclic OB, the communication is triggered by the parameter ENQ_ENR. When writing data to the CTI PLC the parameter WRITE_READ should be true. The amount of data words sent to the CTI CPU is configured with the LENGTH parameter. The register in which the data is written is configured in the START_ADDRESS (0 means Modbus Register 40001 – this is V1 in the CTI CPU).

If also data should be read from the CTI PLC, a second MODBUS FB call is needed where the parameter WRITE_READ is set to false . In the connected instance DB the parameters should be filled in correctly.

```
OB1              Cyclic-OB

    OPN  "CONTROL DAT"

    CALL "MODBUS" , "MODBUS_DAT"
         ID                :=
         LADDR             :=
         TIMER_NR          := T5                    //nonattached Timer
         MONITOR           :="CONTROL DAT".MONITOR
         DB_1              :=
         START_1           :=
         END_1             :=
         DB_2              :=
         START_2           :=
         END_2             :=
         DB_3              :=
         START_3           :=
         END_3             :=
         DB_4              :=
         START_4           :=
         END_4             :=
         DB_5              :=
         START_5           :=
         END_5             :=
         WRITE_PROTECT1    :=
         WRITE_PROTECT2    :=
         WRITE_PROTECT3    :=
         WRITE_PROTECT4    :=
         WRITE_PROTECT5    :=
         ENQ_ENR           :="CONTROL DAT".ENQ_ENR
         SERVER_CLIENT     :=
         DONE_NDR          :="CONTROL DAT".DONE_NDR
         ERROR             :="CONTROL DAT".ERROR
         STATUS            :="CONTROL DAT".STATUS
         START_ADDRESS     :="CONTROL DAT".START_ADDRESS
         LENGTH            :="CONTROL DAT".LENGTH
         WRITE_READ        :="CONTROL DAT".WRITE_READ
         TI                :="CONTROL DAT".TI
         UNIT              :="CONTROL DAT".UNIT

    A    "CONTROL DAT".ENQ_ENR
    R    "CONTROL DAT".ENQ_ENR          //reset trigger

    A    "CONTROL DAT".DONE_NDR         //job finished without error
    FP   #EDGE
    JC   TRIG                           //trigger new job

    A    "CONTROL DAT".ERROR            //job finished with error
                                        //put your error handling here

    BEU                                 //wait until job finished

TRIG:
    L    "CONTROL DAT".TI               //increment TI with each job
    L    1
    +I
    T    "CONTROL DAT".TI

    SET
    =    "CONTROL DAT".ENQ_ENR          //trigger
                                        //initialize values for a
                                        //new job here
```

Online view in the S7 blocks OB1 and DB222

Online “Modbus” call in OB1 : the start_address is 0 which means Reg 40001 (V1 in the CTI PLC), the length is 100 (V1-V100) and the write_read is 1 (which means a write). So in this case the first 100 words from DB11 are sent to V1-V100 in the CTI.



CALL "MODBUS" , "MODBUS_DAT"		FB100 / DB700	IN	OUT
ID	:=1			
LADDR	:=W#16#3FFD			
TIMER_NR	:=T21			
MONITOR	:="CONTROL_DAT".MONITOR	DB222.DBW6	12	
DB_1	:=			
START_1	:=			
END_1	:=			
DB_2	:=			
START_2	:=			
END_2	:=			
DB_3	:=			
START_3	:=			
END_3	:=			
DB_4	:=			
START_4	:=			
END_4	:=			
DB_5	:=			
START_5	:=			
END_5	:=			
WRITE_PROTECT1	:=			
WRITE_PROTECT2	:=			
WRITE_PROTECT3	:=			
WRITE_PROTECT4	:=			
WRITE_PROTECT5	:=			
ENQ_ENR	:="CONTROL_DAT".ENQ_ENR	DB222.DBX38.5	0	
SERVER_CLIENT	:="CONTROL_DAT".SERVER_CLIENT	DB222.DBX38.6	0	
DONE_NDR	:="CONTROL_DAT".DONE_NDR	DB222.DBX40.0		0
ERROR	:="CONTROL_DAT".ERROR	DB222.DBX40.1		0
STATUS	:="CONTROL_DAT".STATUS	DB222.DBW42		16#0
START_ADDRESS	:="CONTROL_DAT".START_ADDRESS	DB222.DBW44	16#0	16#0
LENGTH	:="CONTROL_DAT".LENGTH	DB222.DBB46	100	100
WRITE_READ	:="CONTROL_DAT".WRITE_READ	DB222.DBX47.0	1	1
TI	:="CONTROL_DAT".TI	DB222.DBW48	16#9041	16#9041
UNIT	:="CONTROL_DAT".UNIT	DB222.DBB50	0	0

DB222 is the Control Data Block and the complete online contents is shown below

Address	Name	Type	Initial value	Actual value
0.0	ID	INT	0	1
2.0	LADDR	WORD	W#16#0	W#16#3FFD
4.0	RESERVED1	INT	0	0
6.0	MONITOR	INT	12	12
8.0	DB_1	WORD	W#16#0	W#16#000B
10.0	START_1	WORD	W#16#0	W#16#0000
12.0	END_1	WORD	W#16#0	W#16#0100
14.0	DB_2	WORD	W#16#0	W#16#000C
16.0	START_2	WORD	W#16#0	W#16#03E8
18.0	END_2	WORD	W#16#0	W#16#04E8
20.0	DB_3	WORD	W#16#0	W#16#0000
22.0	START_3	WORD	W#16#0	W#16#0000
24.0	END_3	WORD	W#16#0	W#16#0000
26.0	DB_4	WORD	W#16#0	W#16#0000
28.0	START_4	WORD	W#16#0	W#16#0000
30.0	END_4	WORD	W#16#0	W#16#0000
32.0	DB_5	WORD	W#16#0	W#16#0000
34.0	START_5	WORD	W#16#0	W#16#0000
36.0	END_5	WORD	W#16#0	W#16#0000
38.0	WRITE_PROTECT1	BOOL	FALSE	TRUE
38.1	WRITE_PROTECT2	BOOL	FALSE	FALSE
38.2	WRITE_PROTECT3	BOOL	FALSE	FALSE
38.3	WRITE_PROTECT4	BOOL	FALSE	FALSE
38.4	WRITE_PROTECT5	BOOL	FALSE	FALSE
38.5	ENQ_ENR	BOOL	FALSE	FALSE
38.6	SERVER_CLIENT	BOOL	FALSE	FALSE
39.0	RESERVED2	BYTE	B#16#0	B#16#00
40.0	DONE_NDR	BOOL	FALSE	FALSE
40.1	ERROR	BOOL	FALSE	FALSE
42.0	STATUS	WORD	W#16#0	W#16#0000
44.0	START_ADDRESS	WORD	W#16#0	W#16#0000
46.0	LENGTH	BYTE	B#16#0	B#16#64
47.0	WRITE_READ	BOOL	FALSE	TRUE
48.0	TI	WORD	W#16#0	W#16#D150
50.0	UNIT	BYTE	B#16#0	B#16#00

Additional information can be found in the manual which comes with the Modbus software or can be downloaded from the internet from the Siemens® site
https://support.automation.siemens.com

Control Technology Inc.
5734 Middlebrook Pike, Knoxville, TN 37921-5962
Phone: 865/584-0440 Fax: 865/584-5720 www.controltechnology.com