FAQ • 04/2018

How do you establish MODBUS-RTU communication?

SIMATIC S7-1200 FW ≥ V4.2 / STEP 7 ≥ V14 (TIA Portal)

https://support.industry.siemens.com/cs/ww/en/view/47756141

This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

Security Informati on

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Contents

1 Description

The SIMATIC S7-1200 enables point-to-point communication via the CPU extension with the interfaces RS485 und RS232. You can extend each S7-1200 controller with up to three communication modules (+ one RS485 communications board). Using the MODBUS library integrated in STEP 7 (TIA Portal) you can define each communication module as a MODBUS master or slave. If you select MODBUS Master, you can communicate

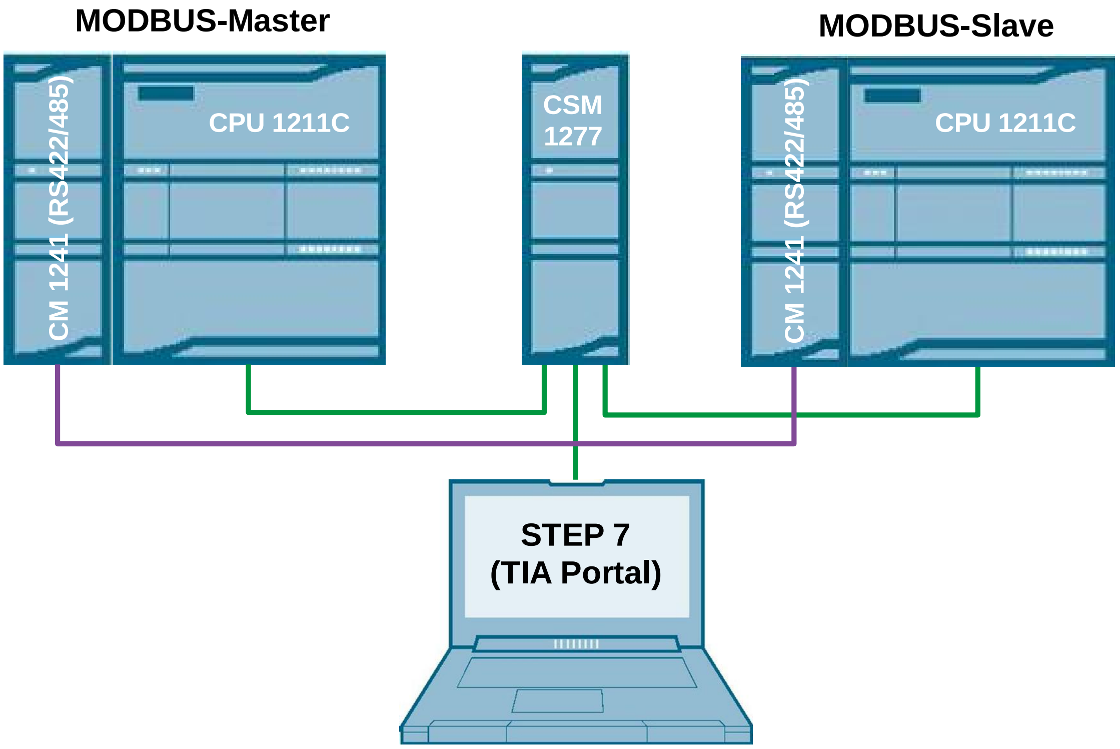
- With only one slave using the CM 1241 RS232 (physical limitation).
- With up to 10 slaves one after the other using the RS422 (via CM 1241 RS422/RS485).
- With up to 32 slaves one after the other using the RS485 (via CM or CB 1241 RS485).

We will take a sample project to describe the configuration procedure in STEP 7 (TIA Portal) V15 for communication with multiple slaves using the CM 1241 RS485.

1.1 Instructions

We have taken the example of MODBUS communication between a master and a slave. There is alternate writing to the holding register of the slave (function code 16) and reading from the holding register of the slave (function code 03). Since the RS485 has a two-wire interface (half-duplex), writing and reading must be conducted consecutively. By the same principle, the address of the slave to be addressed can be changed between two actions (here writing and reading), thus making it possible to exchange data with multiple slaves.

Figure 1-1

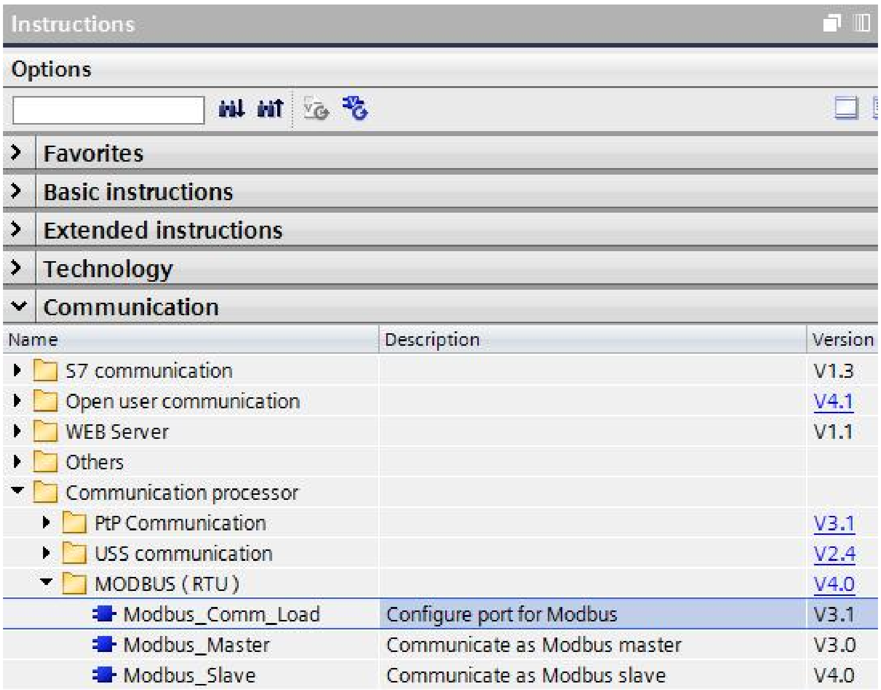


The CM 1241 RS485 communication modules are linked to each other via a PROFIBUS cable. You can continue with the PROFIBUS cable to connect up to 31 additional MODBUS slaves to the master. The configuration is made in STEP 7 (TIA Portal) and the program code is transferred to the controllers with the switch CSM 1277.

1.2 Application Library "MODBUS (RTU)"

The required blocks are located in STEP 7 (TIA Portal) in the communication instructions under "Communication processor" in the "MODBUS (RTU)" folder.

Figure 1-2

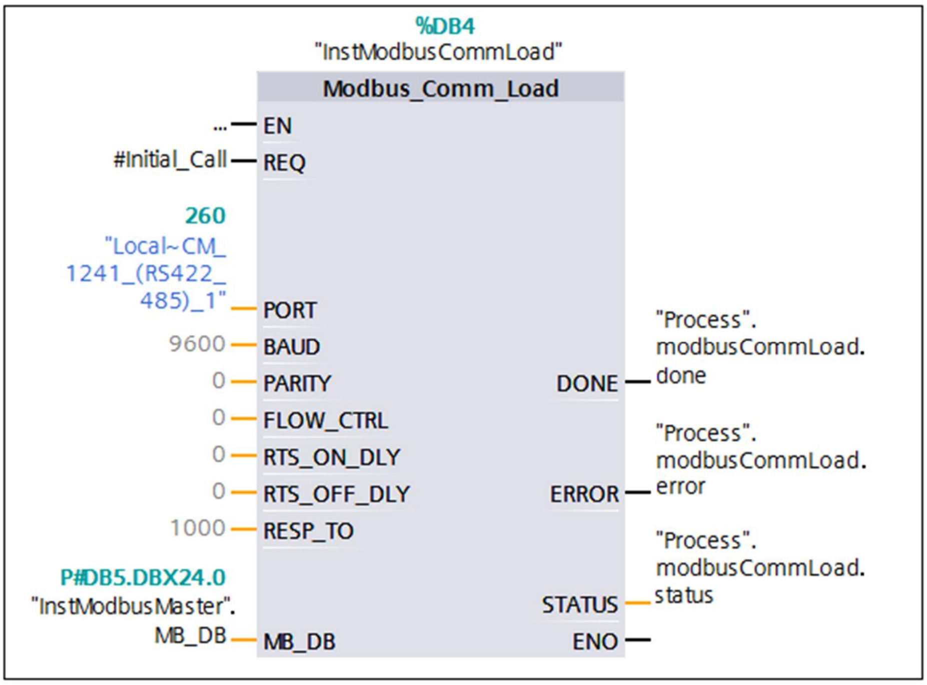


Name	Description	Version
S7 communication		V1.3
Open user communication		V4.1
WEB Server		V1.1
Others		
Communication processor		
PtP Communication		V3.1
USS communication		V2.4
MODBUS (RTU)		V4.0
Modbus_Comm_Load	Configure port for Modbus	V3.1
Modbus_Master	Communicate as Modbus master	V3.0
Modbus_Slave	Communicate as Modbus slave	V4.0

1.2.1 Modbus_Comm_Load

The configuration block "Modbus_Comm_Load" is called on both sides (master and slave) for MODBUS communication.

Figure 1-3

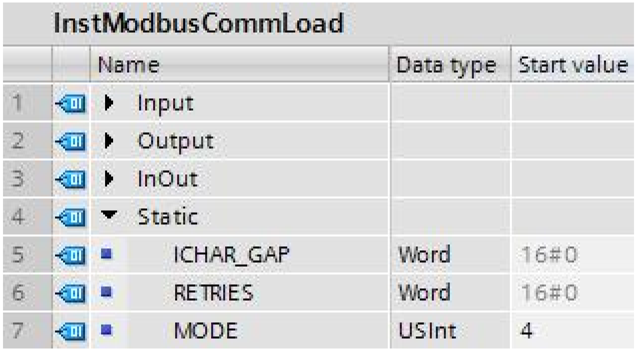


%DB4
"InstModbusCommLoad"
Modbus_Comm_Load
... EN
#Initial_Call REQ
260 "Local~CM_1241_(RS422_485)_1" PORT
9600 BAUD
0 PARITY
0 FLOW_CTRL
0 RTS_ON_DLY
0 RTS_OFF_DLY
1000 RESP_TO
P#DB5.DBX24.0 "InstModbusMaster".MB_DB MB_DB
DONE "Process".modbusCommLoad.done
ERROR "Process".modbusCommLoad.error
STATUS "Process".modbusCommLoad.status
ENO

The "Modbus_Comm_Load" block is used to select the communication module, set the communication parameters and parameterize the connection with the master or slave parameters. The "Modbus_Comm_Load" block must be called in the first program cycle (by activating the "Initial Call" of a cyclic OB, for example, or as a call in Startup OB 100). After inserting the communication module in the hardware configuration you can select the symbolic name of the communication module at the PORT parameter. The communication parameters BAUD (transmission rate) and PARITY (parity) must be identical for all nodes. The port configuration of the RS485 interface in the STEP 7 (TIA Portal) device view is irrelevant here. The "MB_DB" parameter of the instance data block of the master or slave block is transferred at the MB_DB parameter and thus defines the communication module (PORT parameter) as MODBUS master or slave.

In addition, you must change the static parameter MODE in the instance data of the "Modbus_Comm_Load" for the duplex operating mode, preferably via the start value (0 = full duplex (RS232), 1 = full duplex (RS422) four-wire mode, 4 = half duplex (RS485) two-wire mode).

Figure 1-4



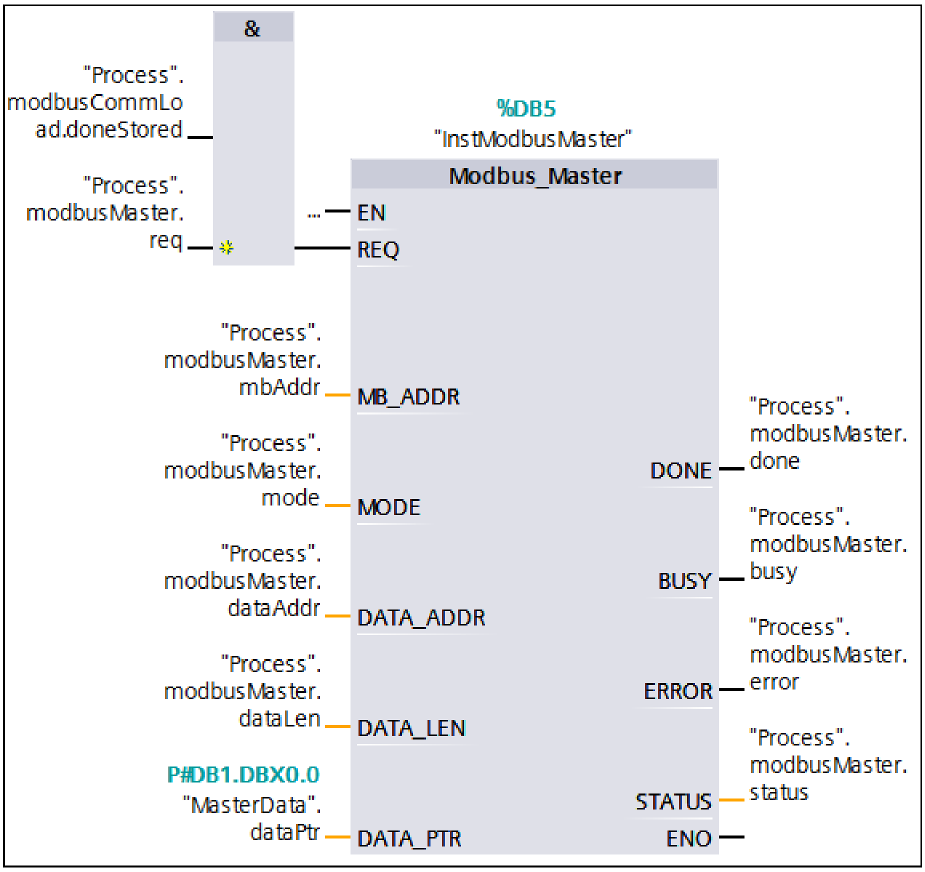
InstModbusCommLoad

	Name	Data type	Start value
1	▸ Input		
2	▸ Output		
3	▸ InOut		
4	▾ Static		
5	▪ ICHAR_GAP	Word	16#0
6	▪ RETRIES	Word	16#0
7	▪ MODE	USInt	4

1.2.2 Modbus_Master

You use the "Modbus_Master" block to define as MODBUS master the communication module selected with the "Modbus_Comm_Load" configuration block.

Figure 1-5



The "Modbus_Master" block is used to select the MODBUS slave to be addressed, select the function code and define the local data storage area. The table below explains the parameters.

Table 1-1

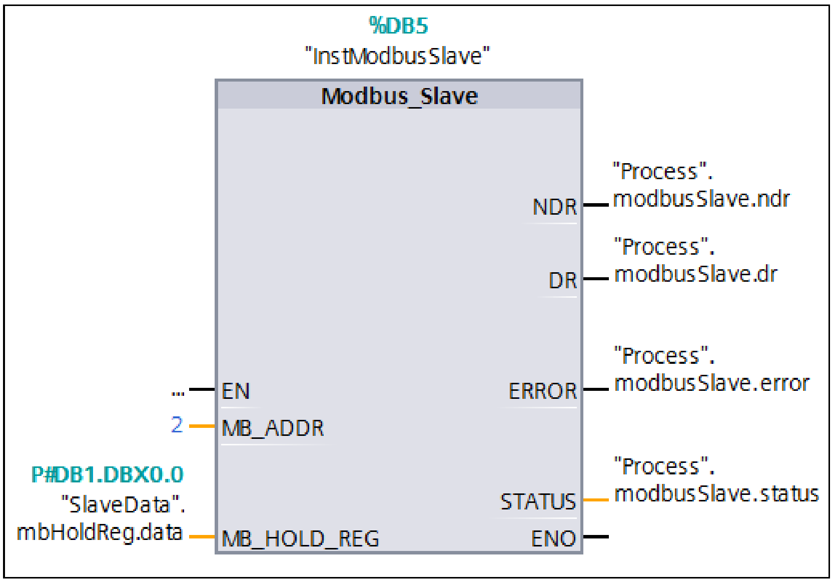
Parameter	Description
REQ	Enables communication.
MB_ADDR	MODBUS-RTU station address.
MODE	Selects the direction of transmission ("0" = read, "1" = write or additional diagnostics functions).
DATA_ADDR	Specifies the MODBUS start address.
DATA_LEN	Specifies the MODBUS data length.
DATA_PTR	Defines the local receive and send data areas of the master. The DATA_PTR parameter must refer to a global data block whose attribute "Optimized block access" has been disabled.

NOTE You will find a detailed description of the instruction „Modbus_Master“ in the manual „SIMATIC S7-1200 Programmable controller“.

1.2.3 Modbus_Slave

You use the "Modbus_Slave" block to define as MODBUS slave the communication module selected with the "Modbus_Comm_Load" configuration block.

Figure 1-6



The "Modbus_Slave" block is used to define the MODBUS-RTU station address and specify the local data storage area for the holding register data transfer.

Table 1-2

Parameter	Description
MB_ADDR	Transfers the MODBUS-RTU station address.
MB_HOLD_REG	Holding register of the slave. The MB_HOLD_REG parameter must refer to a global data block whose attribute "Optimized block access" has been disabled.

At the "MB_HOLD_REG" parameter you transfer an array of the data type "Word".

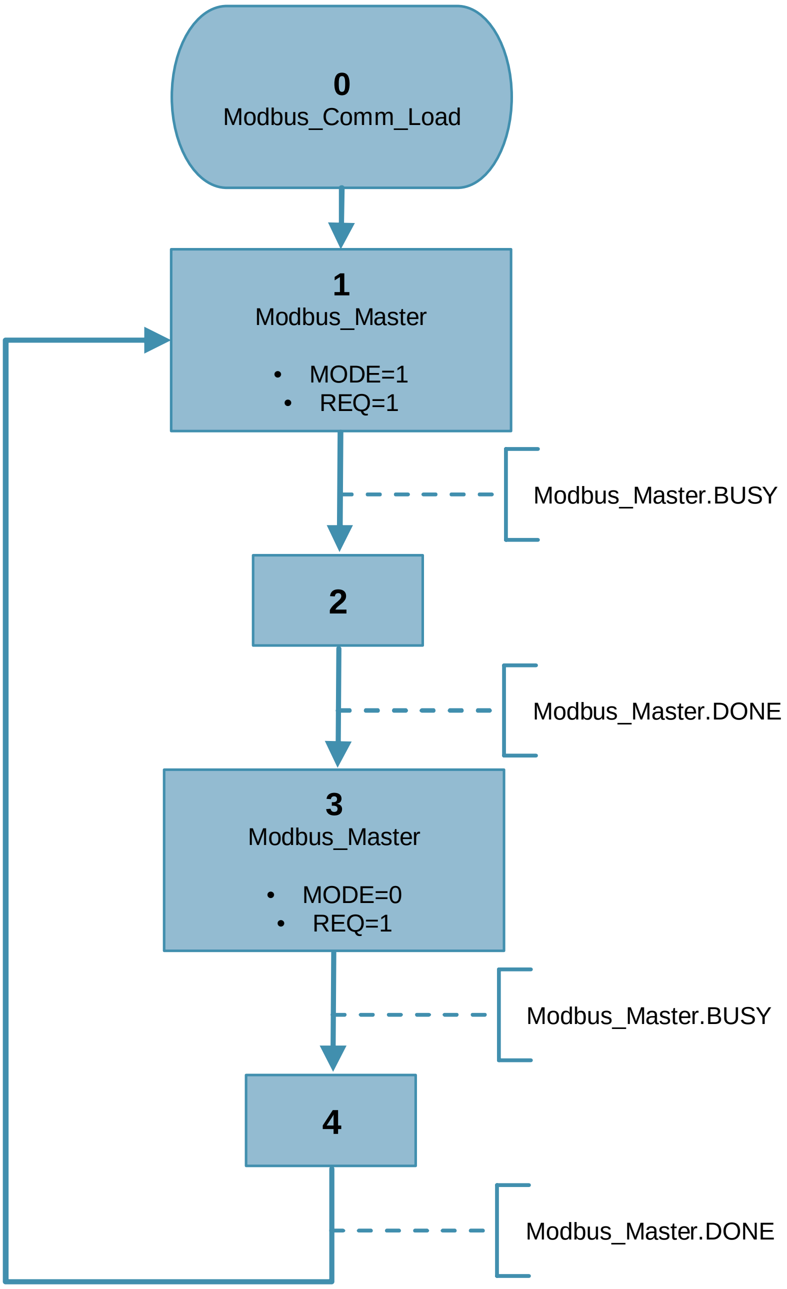
The size of the array at the "MB_HOLD_REG" parameter must be large enough to cover the specified data volume of the master (DATA_ADDR and DATA_PTR). The first word of the array corresponds to the initial address 40001 des MODBUS holding register.

NOTE You will find a detailed description of the instruction „Modbus_Slave“ in the manual „SIMATIC S7-1200 Programmable controller“.

1.3 Sample Project

In the master project, the alternate writing to/reading from the holding register of the slave is done via a sequencer.

Figure 1-7



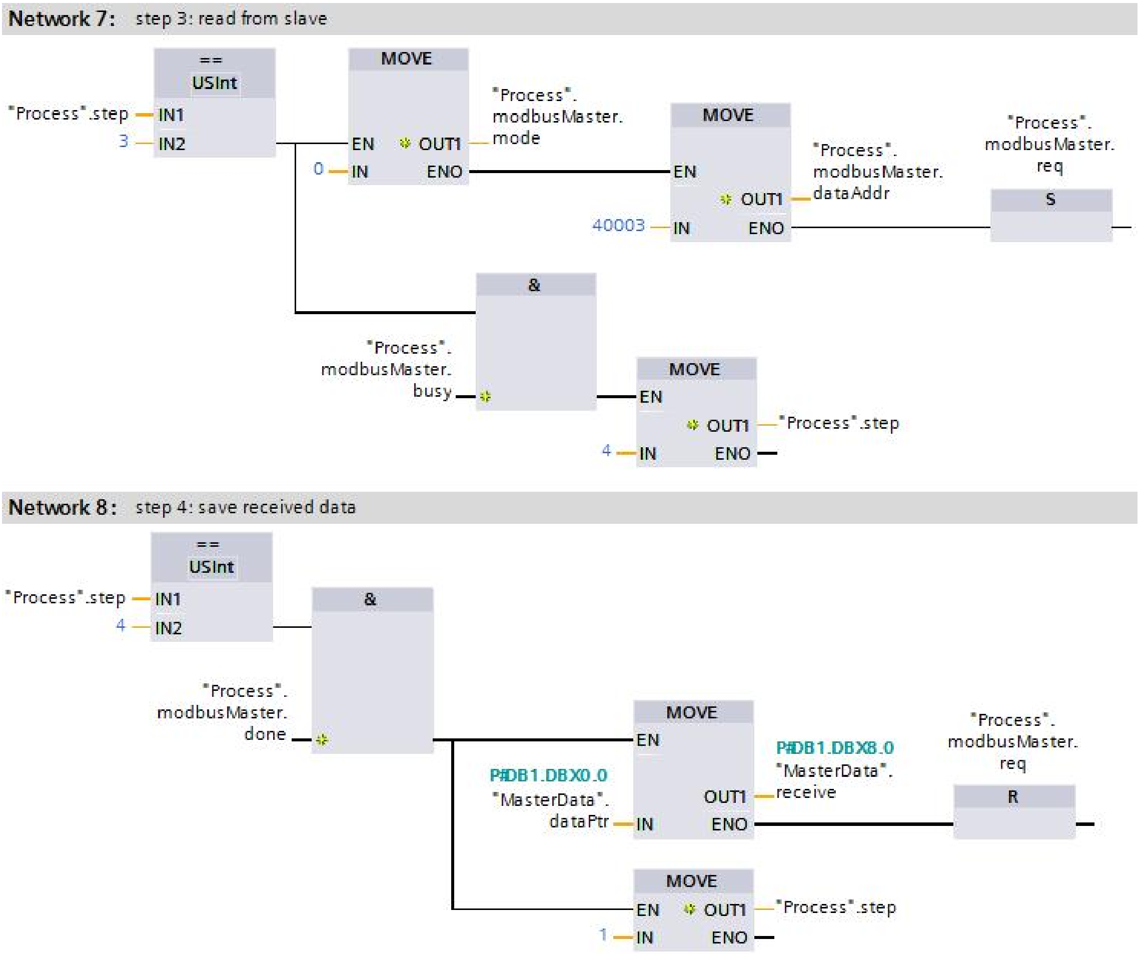
1. The "Modbus_Comm_Load" configuration block is called in the initialization step 0.
2. In Step 1, the data to be written is copied into the DATA_PTR and the "Modbus_Master" with the communication parameters for writing to the slave (MODE = 1) is called and executed (REQ = 1).

- The transition to Step 2 is done by the execution feedback (BUSY) of the "Modbus_Master".
- The transition to Step 3 is done by the successful feedback (DONE) of the "Modbus_Master".
- The transition resets the execution of the "Modbus_Master" (REQ = 0).

3. In Step 3 the communication parameter for reading out of the slave (MODE = 0) is transferred to the "Modbus_Master".
   - Execution and transition to Step 4 are the same as in Step 1.
   - After successful feedback (DONE) of the "Modbus_Master", the data read from the DATA_PTR must be saved (copied).

The execution of an action (here the reading of the data out of the slave with storage) is shown in the figure below.

Figure 1-8


Network 7: step 3: read from slave
==
USInt
"Process".step
IN1
3
IN2
MOVE
EN
OUT1
"Process".modbusMaster.mode
0
IN
ENO
MOVE
EN
OUT1
"Process".modbusMaster.dataAddr
40003
IN
ENO
"Process".modbusMaster.req
S
&
"Process".modbusMaster.busy
MOVE
EN
OUT1
"Process".step
4
IN
ENO
Network 8: step 4: save received data
==
USInt
"Process".step
IN1
4
IN2
&
"Process".modbusMaster.done
MOVE
EN
P#DB1.DBX0.0
"MasterData".dataPtr
IN
OUT1
P#DB1.DBX8.0
"MasterData".receive
ENO
"Process".modbusMaster.req
R
MOVE
EN
OUT1
"Process".step
1
IN
ENO

By additional changing of parameter MB_ADDR by the variable "Process".modbusMasters.mbAddr you could address an other slave in network 7.

If an error occurs (ERROR) the STATUS is stored in the *"Process".modbus___.errorStatus* tag.
Further information about the STATUS evaluation is available in the TIA Portal Online Help via F1.