博图环境下Modbus-RTU通讯应用入门

基于任务轮询机制的Modbus-RTU主站通讯程序的实现

黄岑（Zane）

本通讯例程涉及的:

编程软件

TIA PORTAL V15

硬件系统

S7-1200/S7-1500/ET200SP CPU/1500 OPEN CONTOLLER

基于RS485的Modbus-RTU通讯

例程需要解决的技术问题：

1. 如何在博图环境下用梯形图（LAD）编写一个标准化的，多任务通用的，适应性强的，可移植性强的，Ready for Use的Modbus-RTU主站通讯程序？
2. 如何实现程序自主循环的任务轮询机制？
3. 是否可以实现CPU运行中通过用户程序修改串口通讯参数？
4. 是否可以实现CPU运行中修改通讯任务的参数？
5. 能否实现优化编程，以及优化数据的通讯？
6. 通讯故障的处理机制的简单分析。

基于任务轮询机制的Modbus-RTU主站通讯程序的实现

Modbus-RTU可以被认为是一种基于数据读/写任务的通讯协议

任务轮询机制有以下几种不同的场景：

1. 一个通讯对象的多个不同的通讯任务

   例：通过MODBUS-RTU控制V90PTI伺服实现EPOS定位功能，需要写入控制字，速度及位置的给定数值，读取状态字，实际速度、位置及扭矩的数值

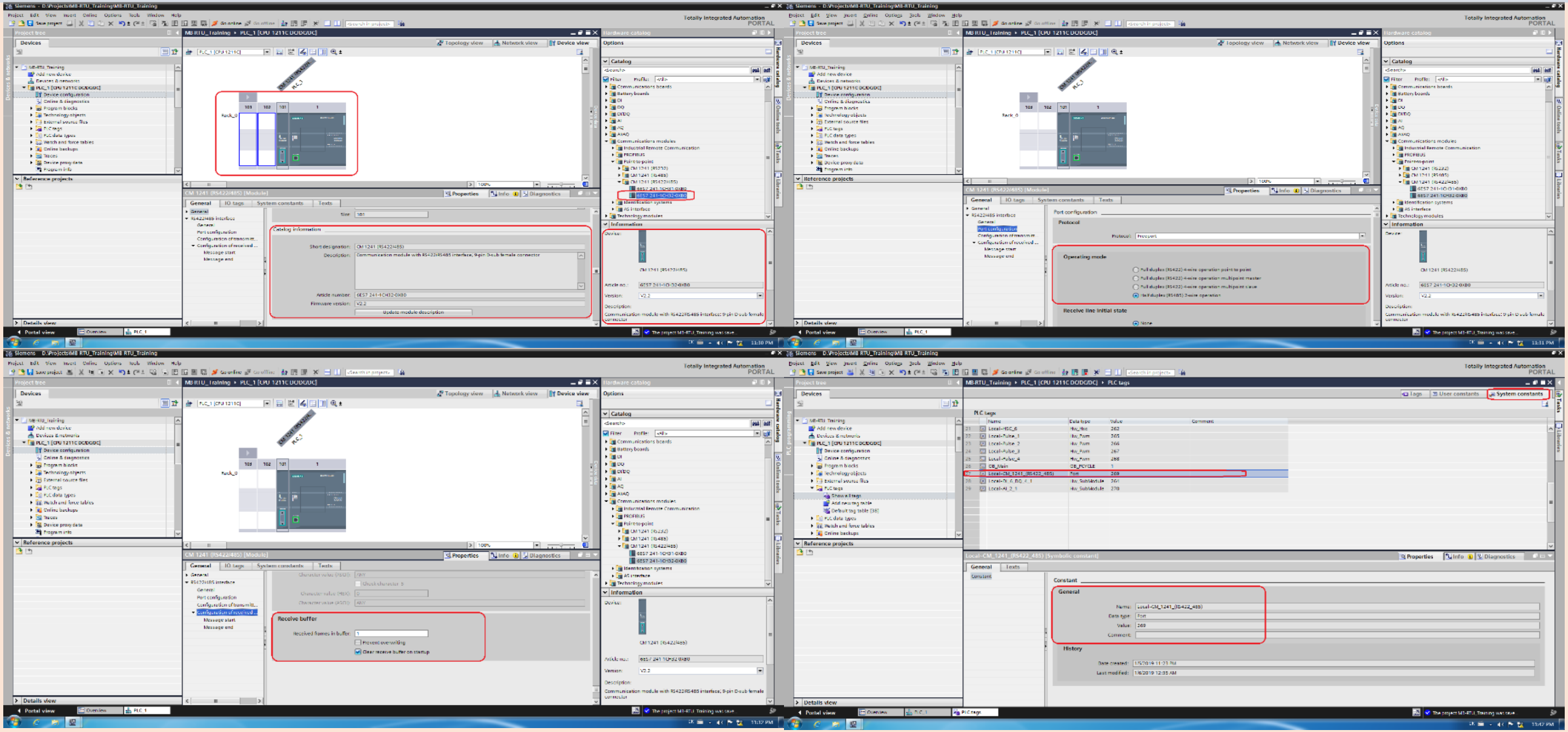
2. 多个相同通讯对象，每个通讯对象有一个或多个不同的通讯任务

   例：通过MODBUS-RTU巡检多个温控回路的温控表，所有的控制任务都一样，写入设定温度，读回反馈温度及输出值

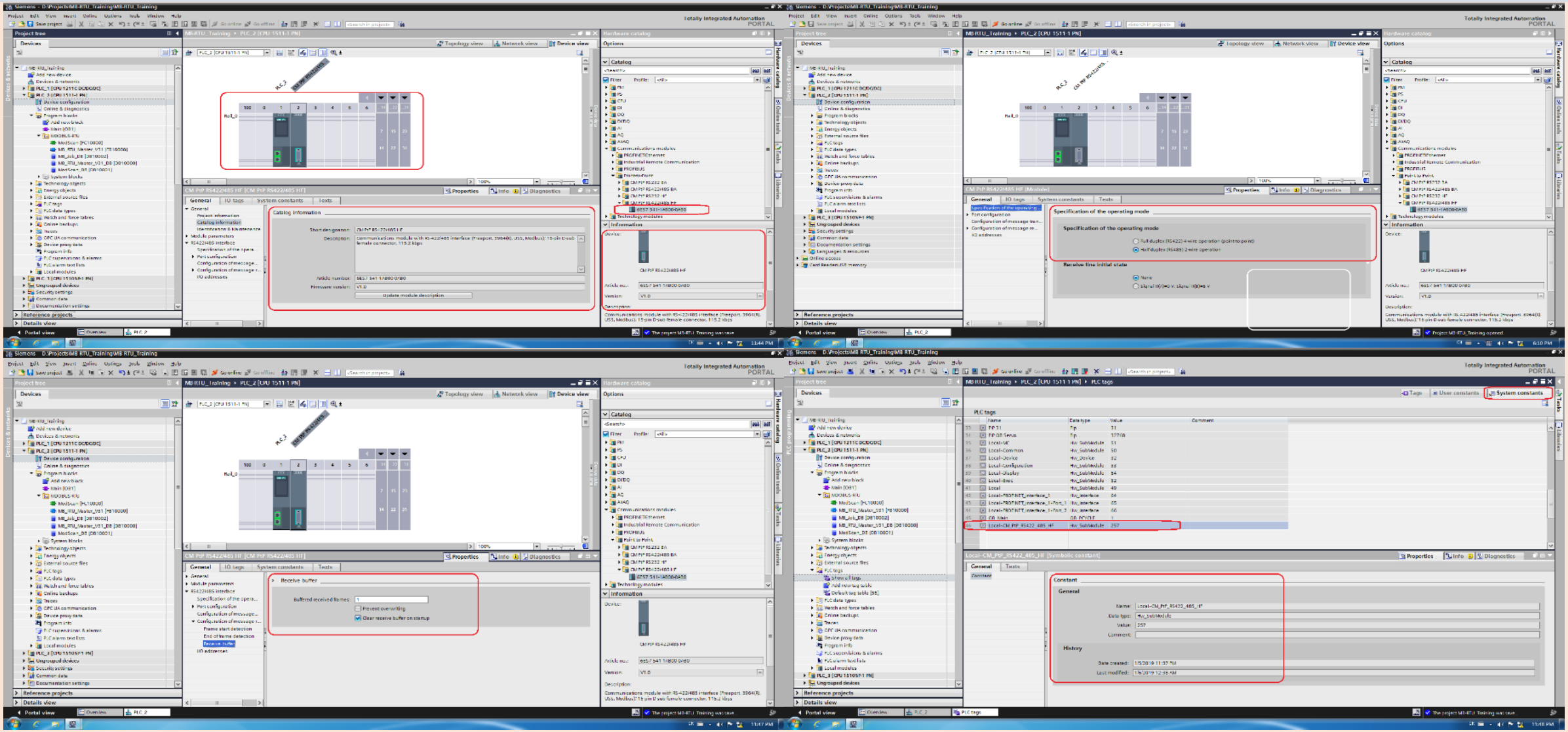
3. 多个不同通讯对象，每个通讯对象有一个或多个不同的通讯任务

   例：一个热水锅炉房控制系统，主PLC通过MODBUS-RTU控制循环泵变频，加热温控表，压力变送器，流量计等设备

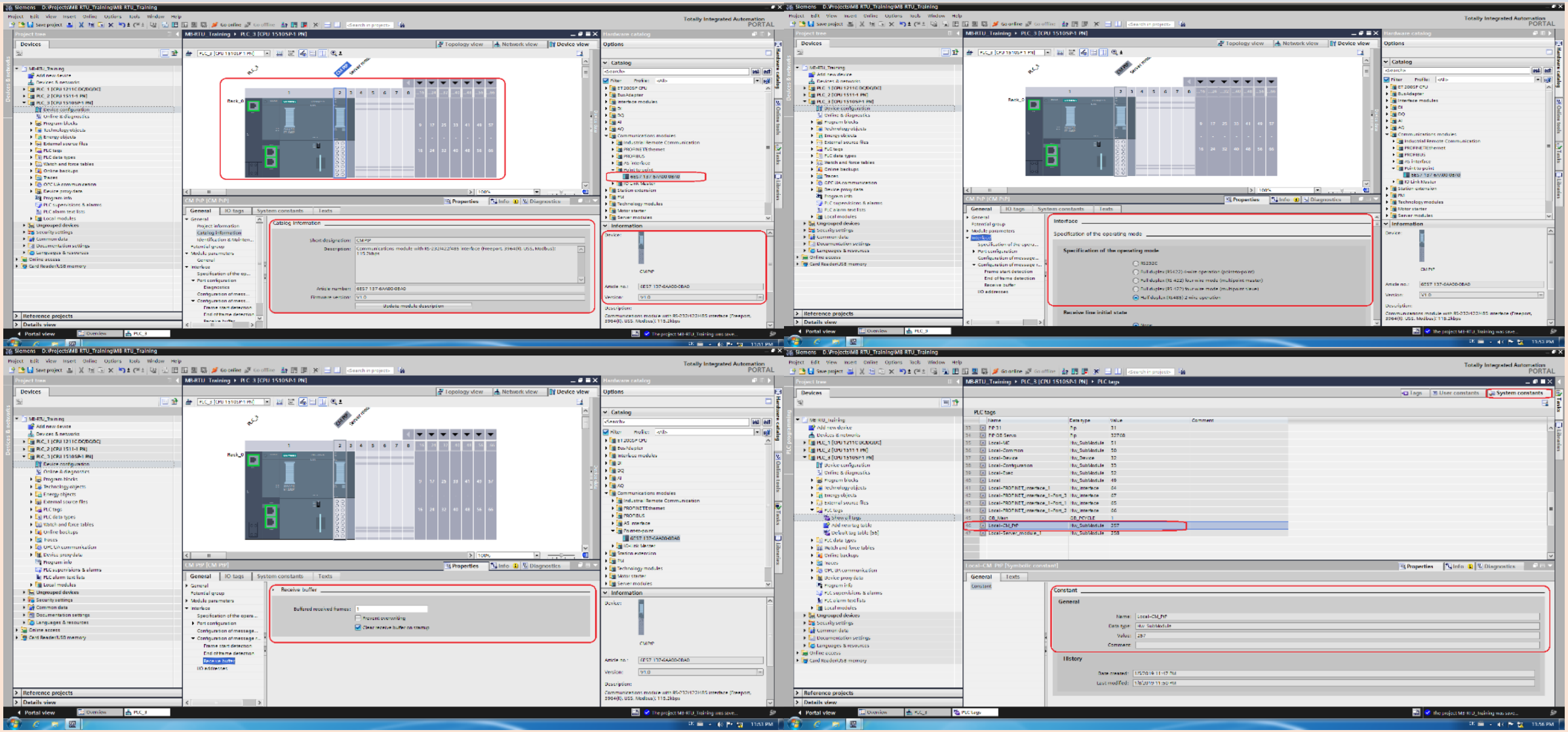
S7-1200的硬件组态及通讯口设置



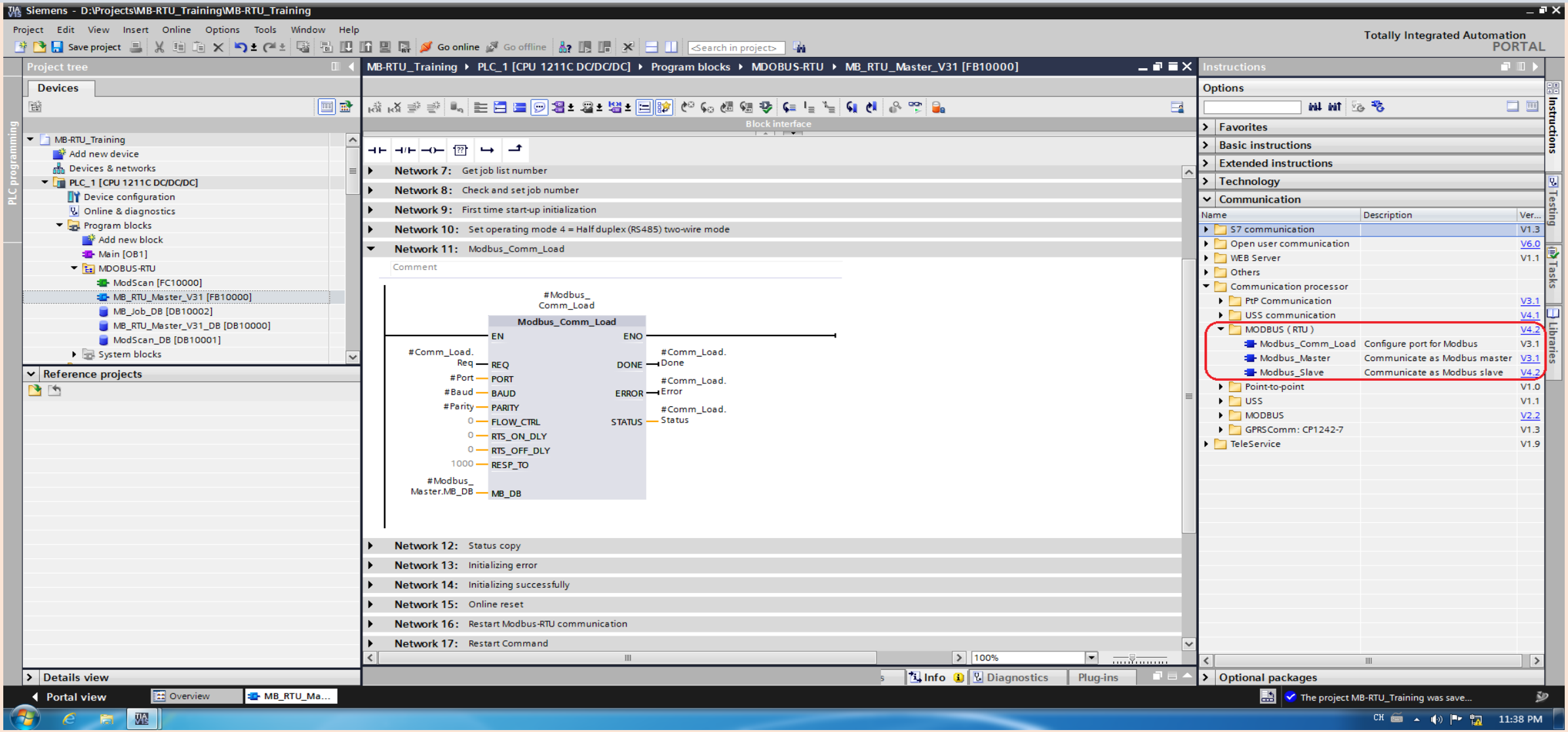
S7-1500的硬件组态及通讯口设置



ET-200SP CPU的硬件组态及通讯口设置



Modbus-RTU主站通讯功能块



Modbus-RTU通讯单个任务数据结构的定义

Siemens - D:\Projects\MB-RTU_Training\MB-RTU_Training

Project tree

MB-RTU_Training ▸ PLC_1 [CPU 1211C DC/DC/DC] ▸ PLC data types ▸ MODBUS-RTU ▸ MB_JOB_UDT

MB_JOB_UDT

	Name	Data type	Default value	Accessible f...	Writa...	Visible in ...	Setpoint	Comment
1	MB_ADDR	UInt	1	☑	☑	☑	☐	Modbus RTU station address:Standard addressing range (1 to 247as well as 0 for Broadcast) Extended addressing range (1 to
2	MODE	USInt	0	☑	☑	☑	☐	Mode selection: Specifies the type of request (read, write or diagnostics)
3	DATA_ADDR	UDInt	0	☑	☑	☑	☐	Start address in the slave: Specifies the start address of the data that is accessed in the Modbus slave. The valid addresses a
4	DATA_LEN	UInt	1	☑	☑	☑	☐	Data length: Specifies the number of bits or words this instruction is to access. The valid lengths are listed in the table of Mod
5	DATA_PTR	Array[0..31] of Word		☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
6	DATA_PTR[0]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
7	DATA_PTR[1]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
8	DATA_PTR[2]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
9	DATA_PTR[3]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
10	DATA_PTR[4]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
11	DATA_PTR[5]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
12	DATA_PTR[6]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
13	DATA_PTR[7]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
14	DATA_PTR[8]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
15	DATA_PTR[9]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
16	DATA_PTR[10]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
17	DATA_PTR[11]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
18	DATA_PTR[12]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
19	DATA_PTR[13]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
20	DATA_PTR[14]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
21	DATA_PTR[15]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
22	DATA_PTR[16]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
23	DATA_PTR[17]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
24	DATA_PTR[18]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
25	DATA_PTR[19]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
26	DATA_PTR[20]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
27	DATA_PTR[21]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
28	DATA_PTR[22]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
29	DATA_PTR[23]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
30	DATA_PTR[24]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
31	DATA_PTR[25]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
32	DATA_PTR[26]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
33	DATA_PTR[27]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
34	DATA_PTR[28]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.
35	DATA_PTR[29]	Word	16#0	☑	☑	☑	☐	Data pointer: Points to the flag or DB address for the data to be written or read.

Modbus-RTU主站轮询通讯的任务列表

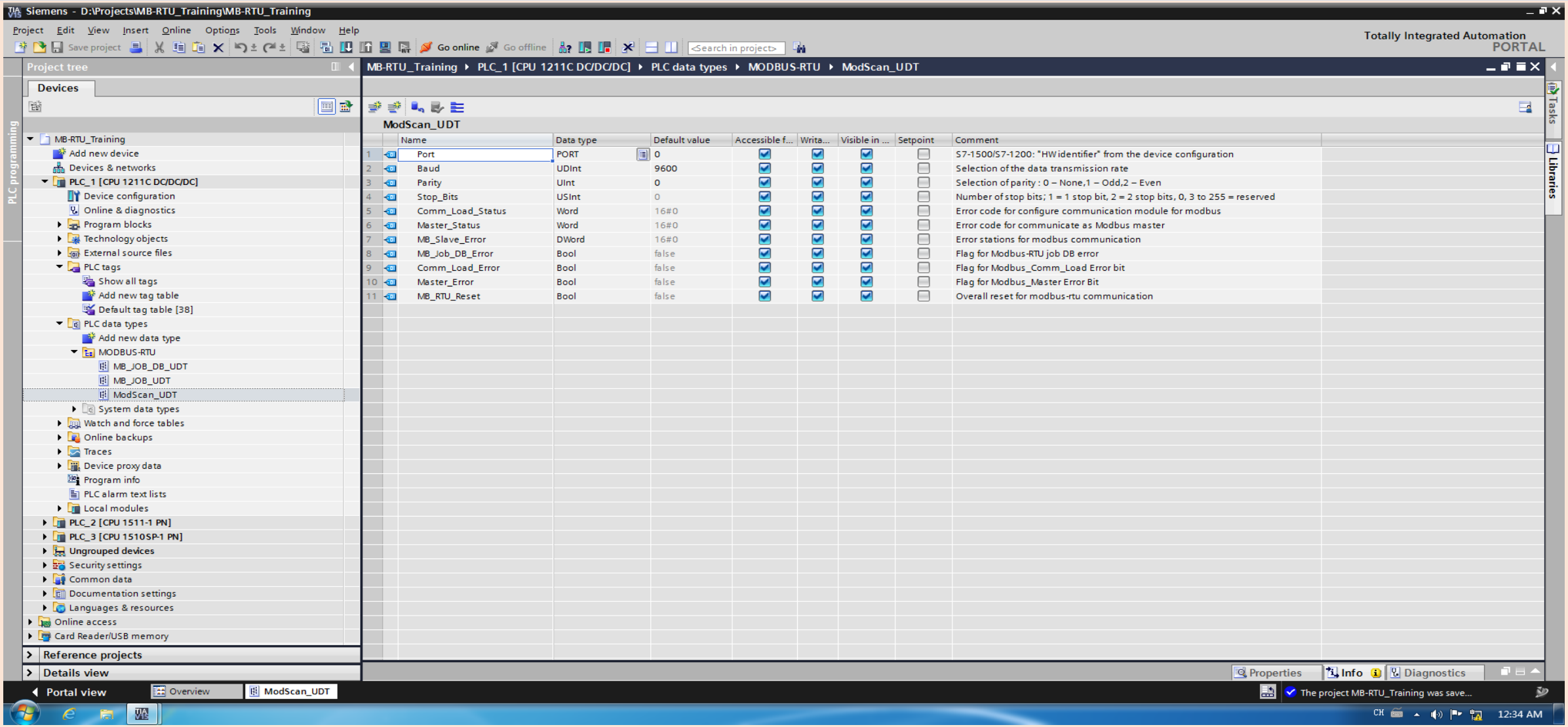
Siemens - D:\Projects\MB-RTU_Training\MB-RTU_Training

MB-RTU_Training ▸ PLC_1 [CPU 1211C DC/DC/DC] ▸ Program blocks ▸ MDOBUS-RTU ▸ MB_Job_DB [DB10002]

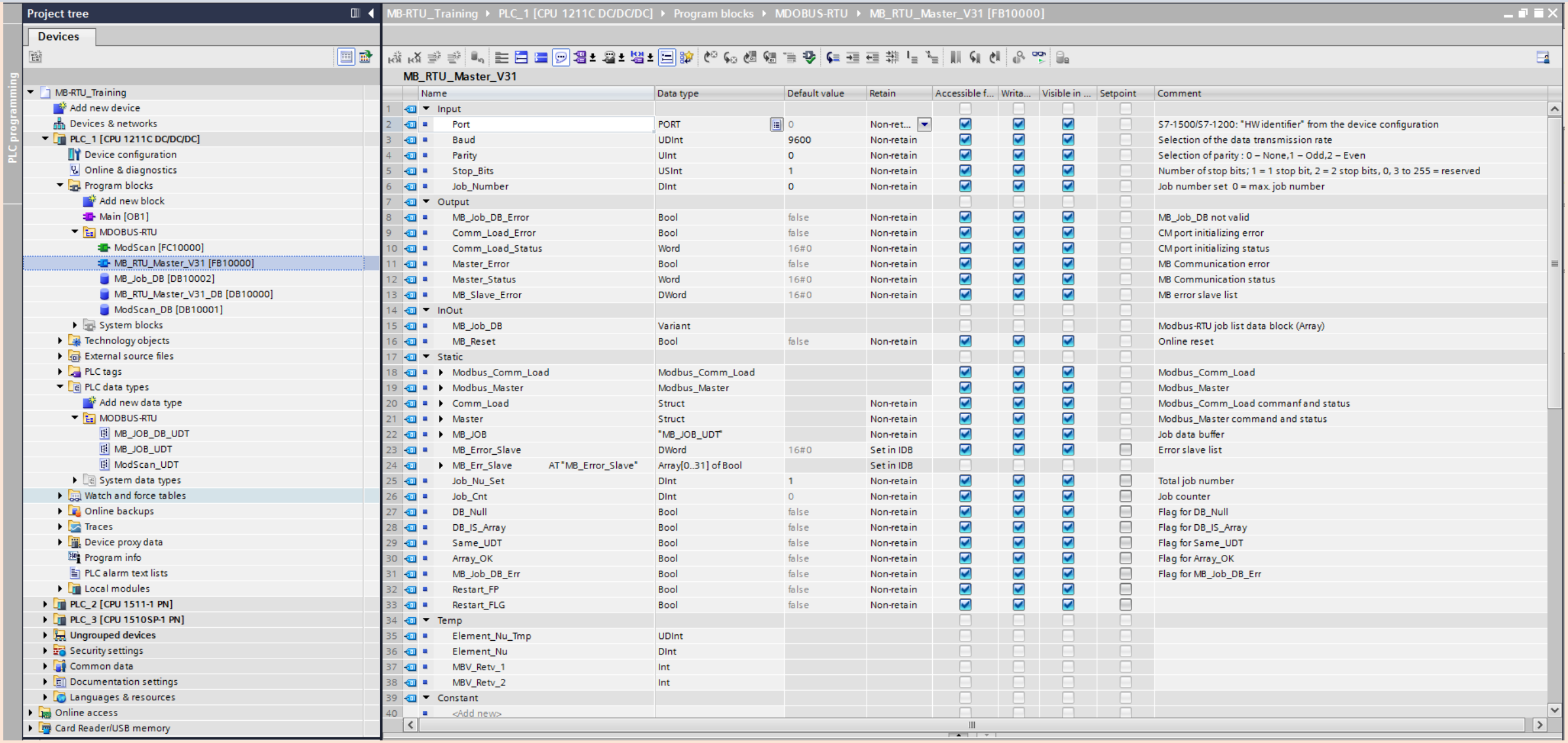
MB_Job_DB

	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Comment
1	Static								
2	MB_Job	Array[0..31] ...							
3	MB_Job[0]	"MB_JOB_UDT"							
4	MB_ADDR	UInt	1						Modbus RTU station address:Standard addressing range (1 to 247as well as 0 for Broadcast) Extended addre
5	MODE	USInt	0						Mode selection: Specifies the type of request (read, write or diagnostics)
6	DATA_ADDR	UDInt	40001						Start address in the slave: Specifies the start address of the data that is accessed in the Modbus slave. The v
7	DATA_LEN	UInt	1						Data length: Specifies the number of bits or words this instruction is to access. The valid lengths are listed in
8	DATA_PTR	Array[0..31] of Word							Data pointer: Points to the flag or DB address for the data to be written or read.
9	MB_Job[1]	"MB_JOB_UDT"							
10	MB_ADDR	UInt	1						Modbus RTU station address:Standard addressing range (1 to 247as well as 0 for Broadcast) Extended addre
11	MODE	USInt	1						Mode selection: Specifies the type of request (read, write or diagnostics)
12	DATA_ADDR	UDInt	40003						Start address in the slave: Specifies the start address of the data that is accessed in the Modbus slave. The v
13	DATA_LEN	UInt	2						Data length: Specifies the number of bits or words this instruction is to access. The valid lengths are listed in
14	DATA_PTR	Array[0..31] of Word							Data pointer: Points to the flag or DB address for the data to be written or read.
15	MB_Job[2]	"MB_JOB_UDT"							
16	MB_ADDR	UInt	2						Modbus RTU station address:Standard addressing range (1 to 247as well as 0 for Broadcast) Extended addre
17	MODE	USInt	0						Mode selection: Specifies the type of request (read, write or diagnostics)
18	DATA_ADDR	UDInt	40001						Start address in the slave: Specifies the start address of the data that is accessed in the Modbus slave. The v
19	DATA_LEN	UInt	1						Data length: Specifies the number of bits or words this instruction is to access. The valid lengths are listed in
20	DATA_PTR	Array[0..31] of Word							Data pointer: Points to the flag or DB address for the data to be written or read.
21	MB_Job[3]	"MB_JOB_UDT"							
22	MB_ADDR	UInt	2						Modbus RTU station address:Standard addressing range (1 to 247as well as 0 for Broadcast) Extended addre
23	MODE	USInt	0						Mode selection: Specifies the type of request (read, write or diagnostics)
24	DATA_ADDR	UDInt	40003						Start address in the slave: Specifies the start address of the data that is accessed in the Modbus slave. The v
25	DATA_LEN	UInt	2						Data length: Specifies the number of bits or words this instruction is to access. The valid lengths are listed in
26	DATA_PTR	Array[0..31] of Word							Data pointer: Points to the flag or DB address for the data to be written or read.
27	MB_Job[4]	"MB_JOB_UDT"							
28	MB_Job[5]	"MB_JOB_UDT"							
29	MB_Job[6]	"MB_JOB_UDT"							
30	MB_Job[7]	"MB_JOB_UDT"							
31	MB_Job[8]	"MB_JOB_UDT"							
32	MB_Job[9]	"MB_JOB_UDT"							
33	MB_Job[10]	"MB_JOB_UDT"							
34	MB_Job[11]	"MB_JOB_UDT"							
35	MB_Job[12]	"MB_JOB_UDT"							
36	MB_Job[13]	"MB_JOB_UDT"							

Modbus-RTU主站通讯口参数设置及功能块状态反馈

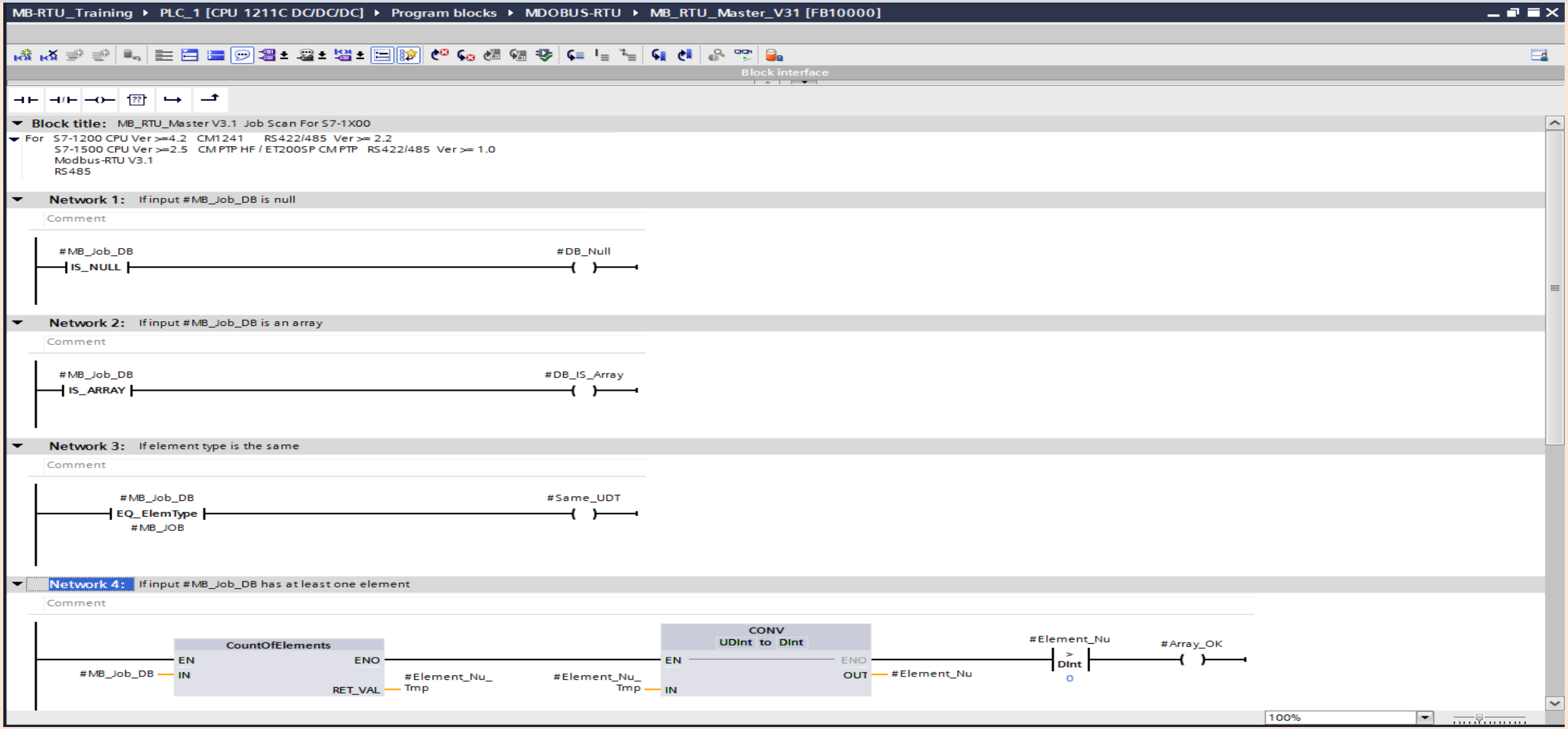


MB_RTU_Master_3.1通讯功能块变量表定义

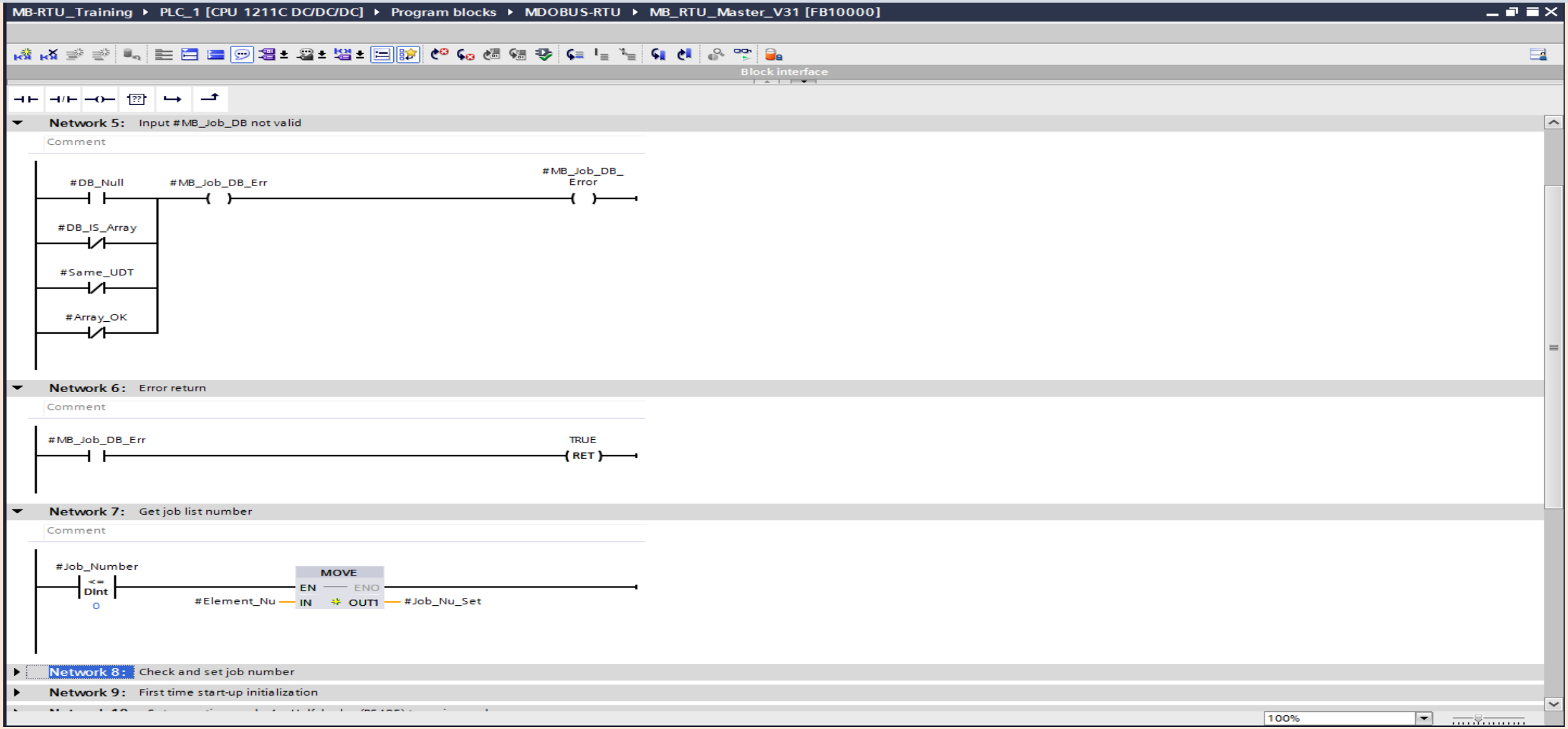


	Name	Data type	Default value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Comment
1	Input								
2	Port	PORT	0	Non-ret...	☑	☑	☑	☐	S7-1500/S7-1200: "HW identifier" from the device configuration
3	Baud	UDInt	9600	Non-retain	☑	☑	☑	☐	Selection of the data transmission rate
4	Parity	UInt	0	Non-retain	☑	☑	☑	☐	Selection of parity : 0 – None,1 – Odd,2 – Even
5	Stop_Bits	USInt	1	Non-retain	☑	☑	☑	☐	Number of stop bits; 1 = 1 stop bit, 2 = 2 stop bits, 0, 3 to 255 = reserved
6	Job_Number	DInt	0	Non-retain	☑	☑	☑	☐	Job number set 0 = max. job number
7	Output								
8	MB_Job_DB_Error	Bool	false	Non-retain	☑	☑	☑	☐	MB_Job_DB not valid
9	Comm_Load_Error	Bool	false	Non-retain	☑	☑	☑	☐	CM port initializing error
10	Comm_Load_Status	Word	16#0	Non-retain	☑	☑	☑	☐	CM port initializing status
11	Master_Error	Bool	false	Non-retain	☑	☑	☑	☐	MB Communication error
12	Master_Status	Word	16#0	Non-retain	☑	☑	☑	☐	MB Communication status
13	MB_Slave_Error	DWord	16#0	Non-retain	☑	☑	☑	☐	MB error slave list
14	InOut								
15	MB_Job_DB	Variant							Modbus-RTU job list data block (Array)
16	MB_Reset	Bool	false	Non-retain	☑	☑	☑	☐	Online reset
17	Static								
18	Modbus_Comm_Load	Modbus_Comm_Load			☑	☑	☑	☐	Modbus_Comm_Load
19	Modbus_Master	Modbus_Master			☑	☑	☑	☐	Modbus_Master
20	Comm_Load	Struct		Non-retain	☑	☑	☑	☐	Modbus_Comm_Load commanf and status
21	Master	Struct		Non-retain	☑	☑	☑	☐	Modbus_Master command and status
22	MB_JOB	"MB_JOB_UDT"		Non-retain	☑	☑	☑	☐	Job data buffer
23	MB_Error_Slave	DWord	16#0	Set in IDB	☑	☑	☑	☐	Error slave list
24	MB_Err_Slave AT "MB_Error_Slave"	Array[0..31] of Bool		Set in IDB	☐	☐	☐	☐	
25	Job_Nu_Set	DInt	1	Non-retain	☑	☑	☑	☐	Total job number
26	Job_Cnt	DInt	0	Non-retain	☑	☑	☑	☐	Job counter
27	DB_Null	Bool	false	Non-retain	☑	☑	☑	☐	Flag for DB_Null
28	DB_IS_Array	Bool	false	Non-retain	☑	☑	☑	☐	Flag for DB_IS_Array
29	Same_UDT	Bool	false	Non-retain	☑	☑	☑	☐	Flag for Same_UDT
30	Array_OK	Bool	false	Non-retain	☑	☑	☑	☐	Flag for Array_OK
31	MB_Job_DB_Err	Bool	false	Non-retain	☑	☑	☑	☐	Flag for MB_Job_DB_Err
32	Restart_FP	Bool	false	Non-retain	☑	☑	☑	☐	
33	Restart_FLG	Bool	false	Non-retain	☑	☑	☑	☐	
34	Temp								
35	Element_Nu_Tmp	UDInt							
36	Element_Nu	DInt							
37	MBV_Retv_1	Int							
38	MBV_Retv_2	Int							
39	Constant								
40	<Add new>								

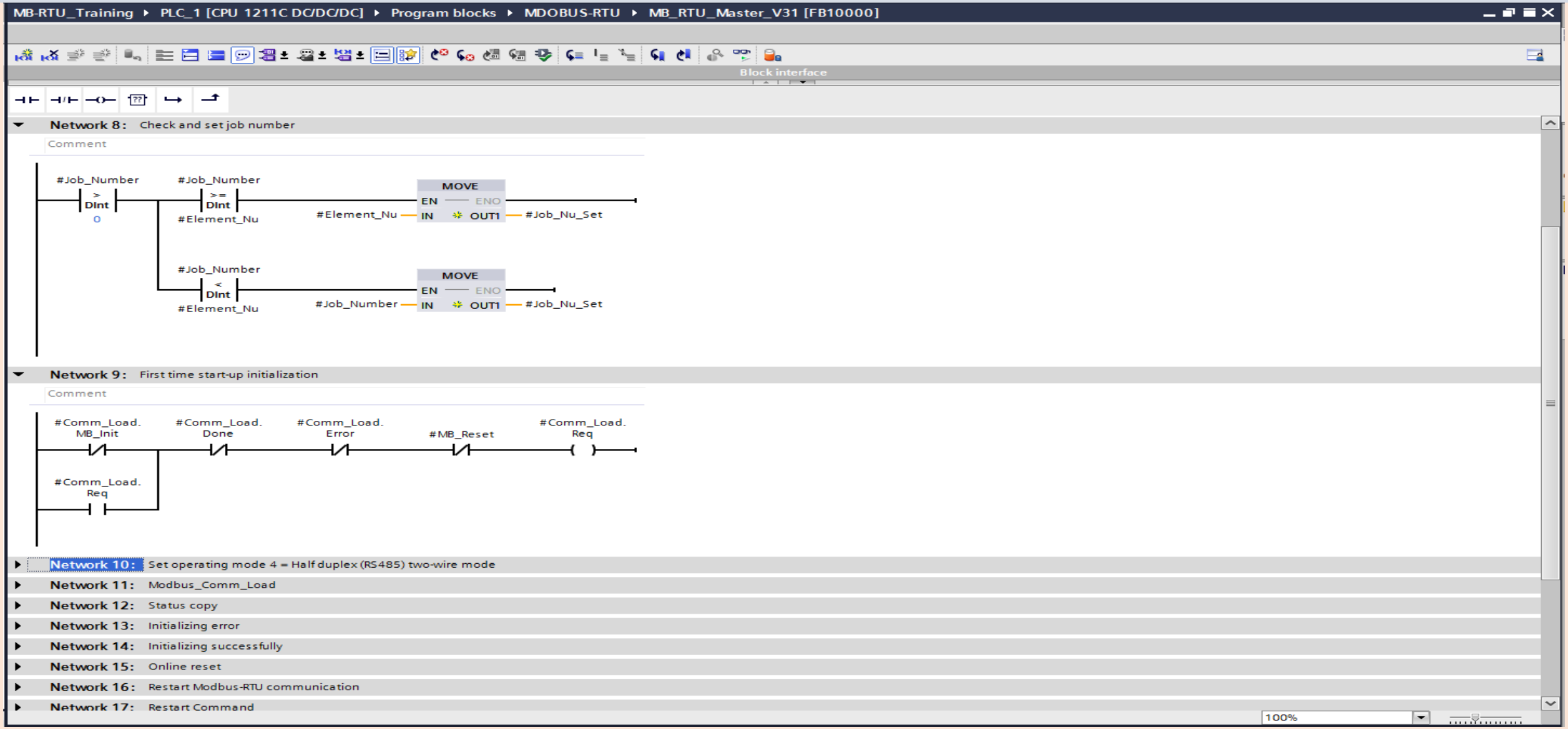
MB_RTU_Master_3.1通讯功能块（1）



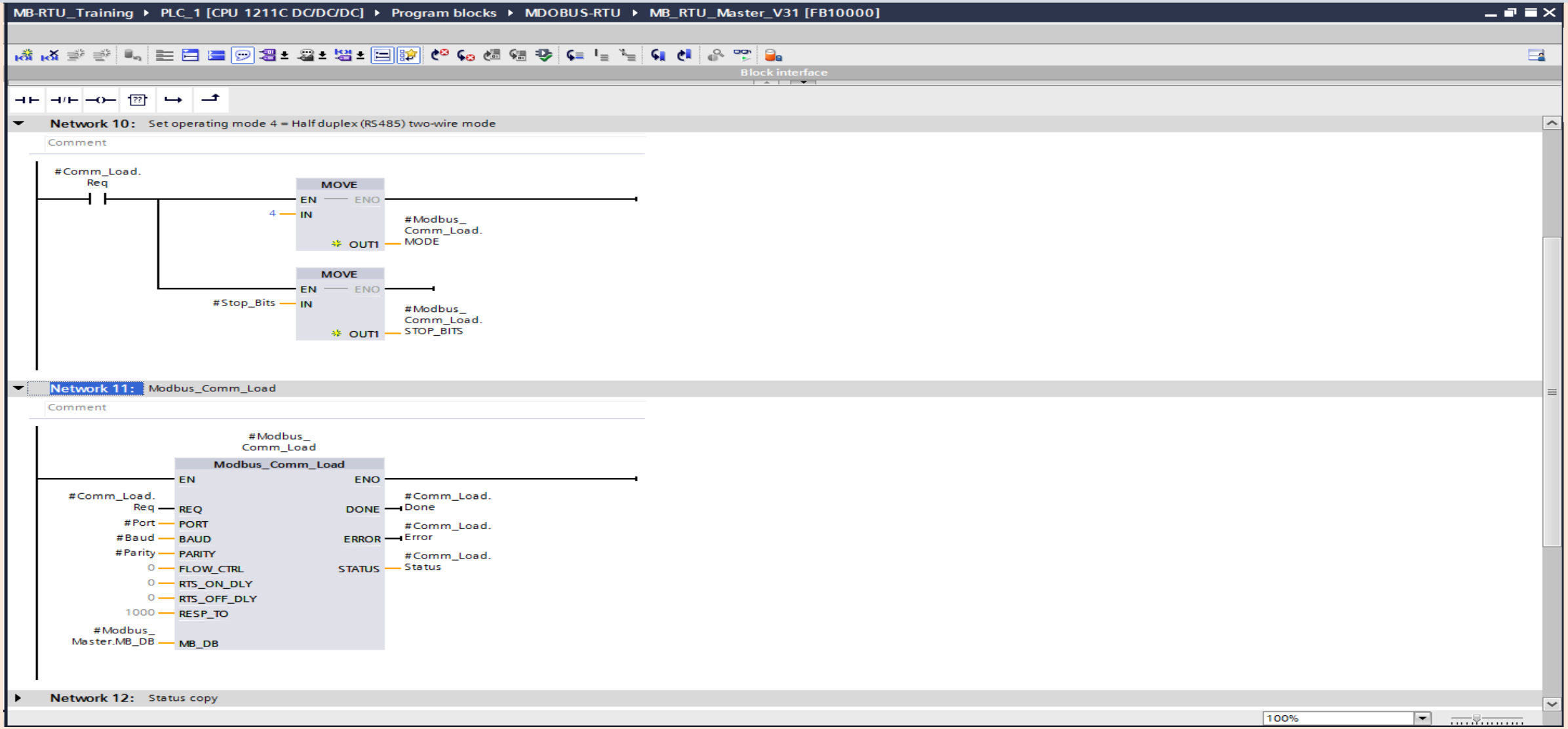
MB_RTU_Master_3.1通讯功能块（2）



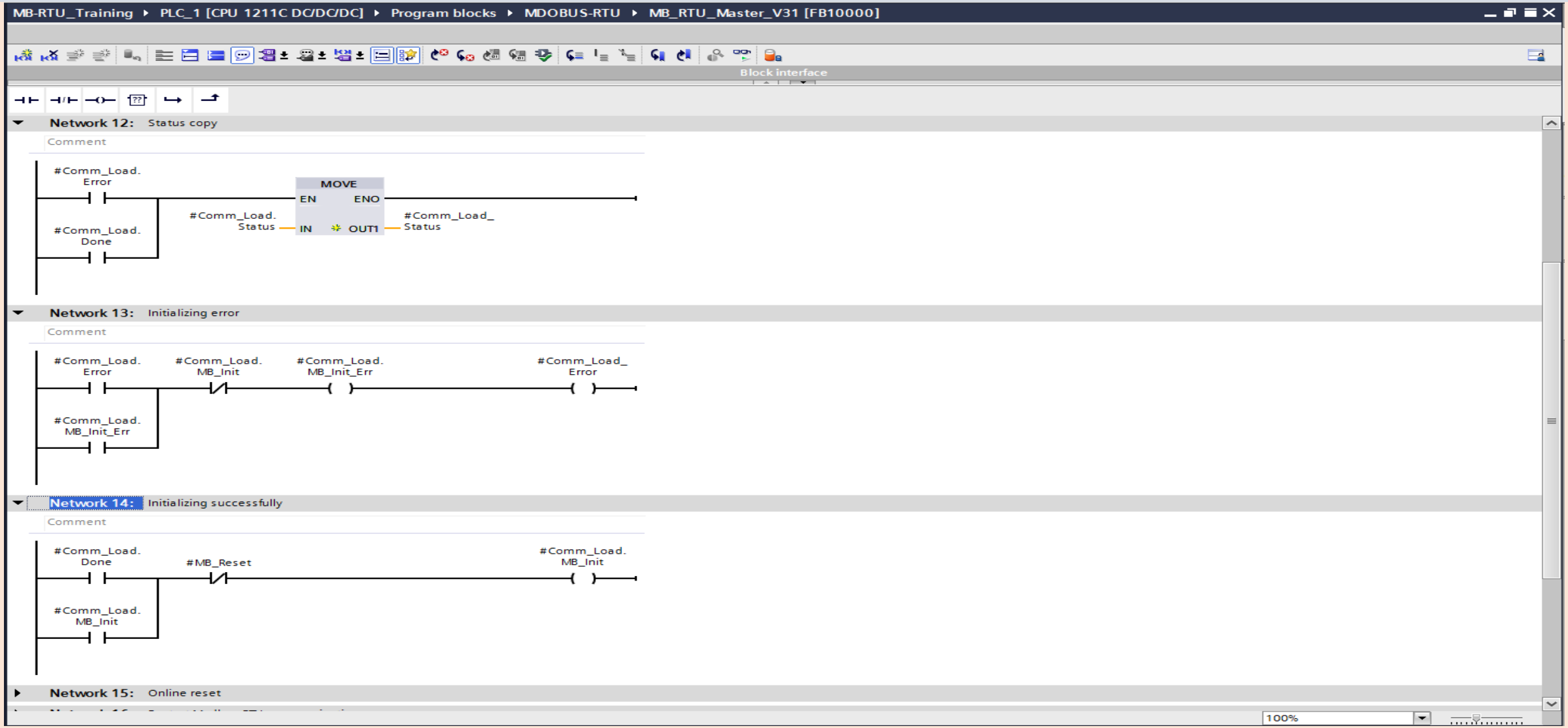
MB_RTU_Master_3.1通讯功能块（3）



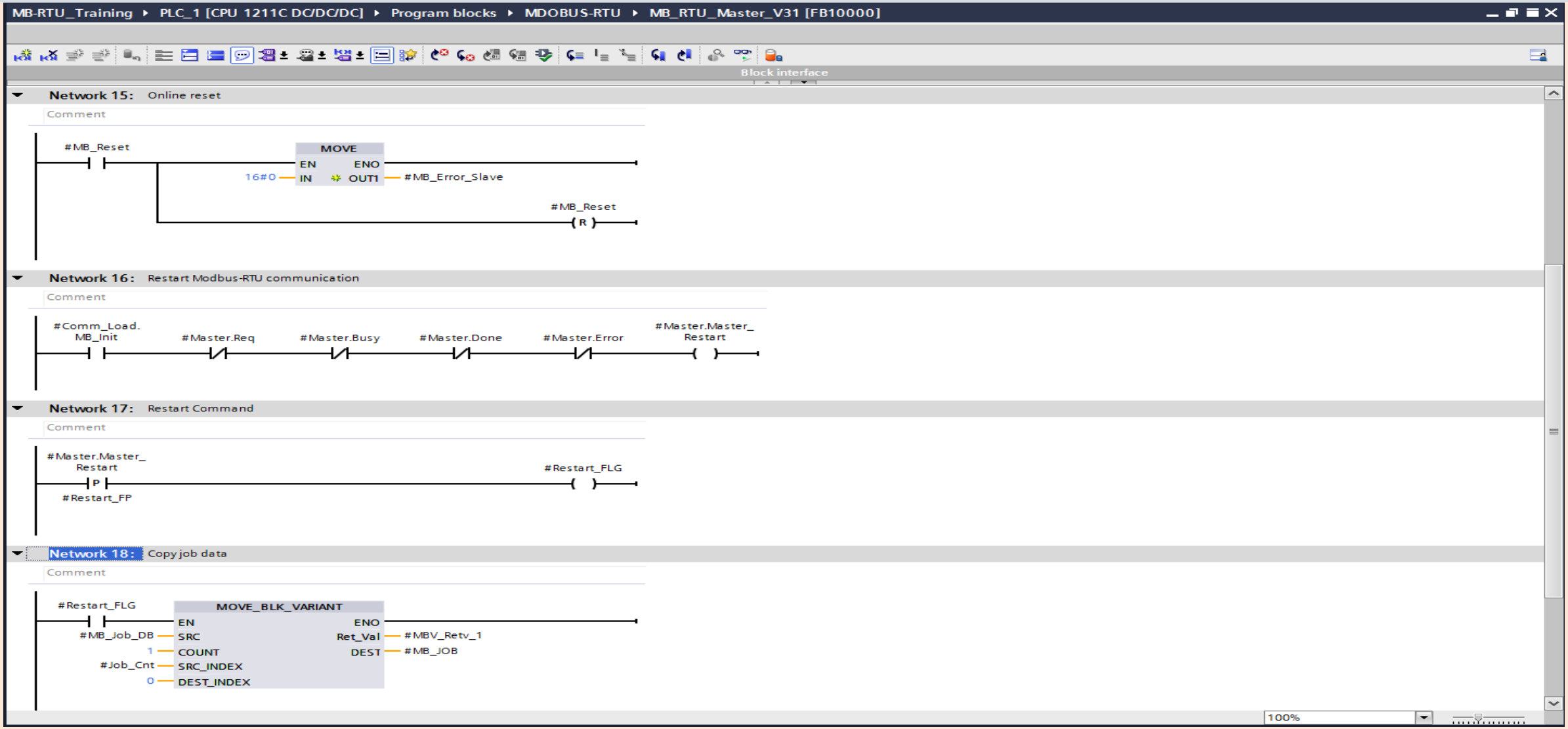
MB_RTU_Master_3.1通讯功能块（4）



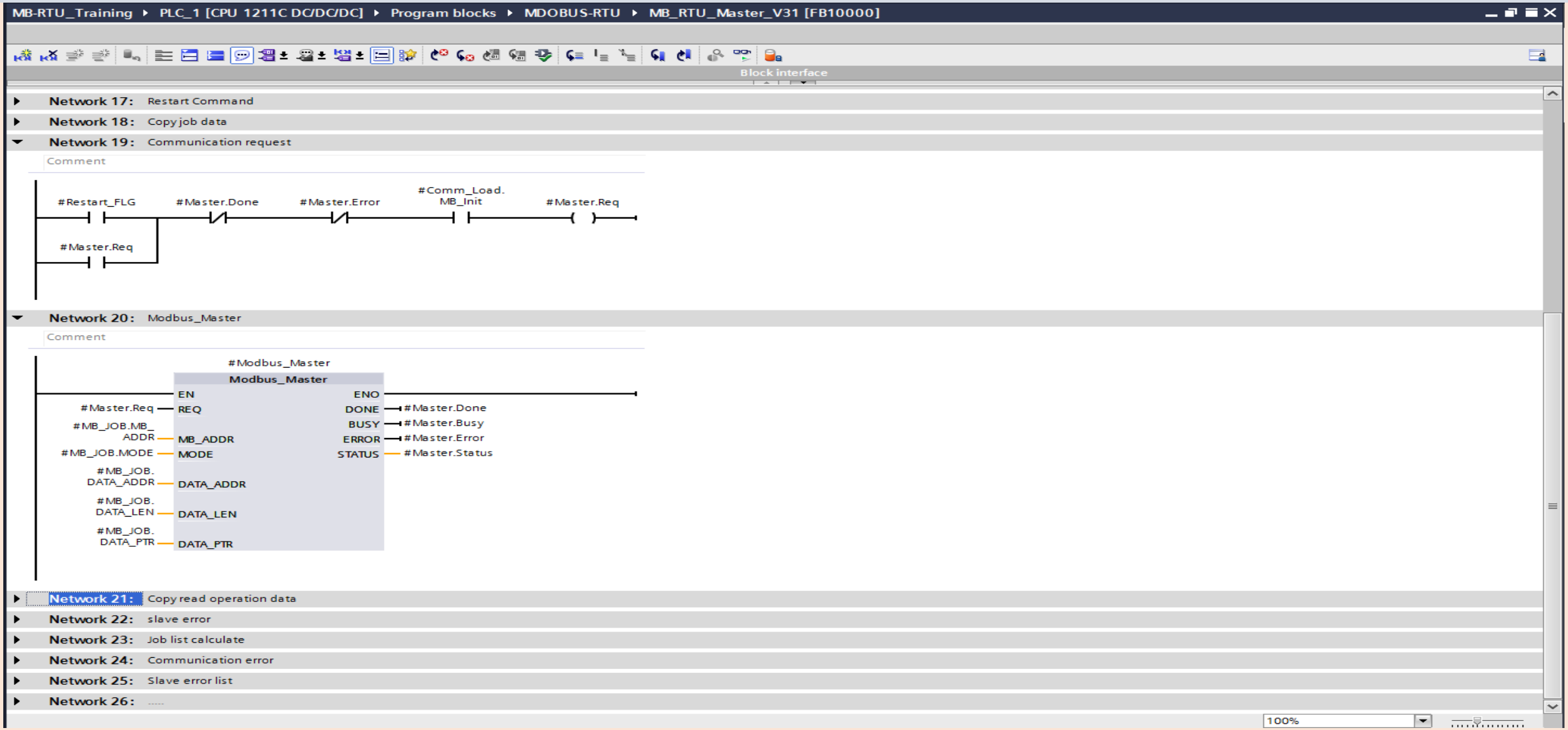
MB_RTU_Master_3.1通讯功能块（5）



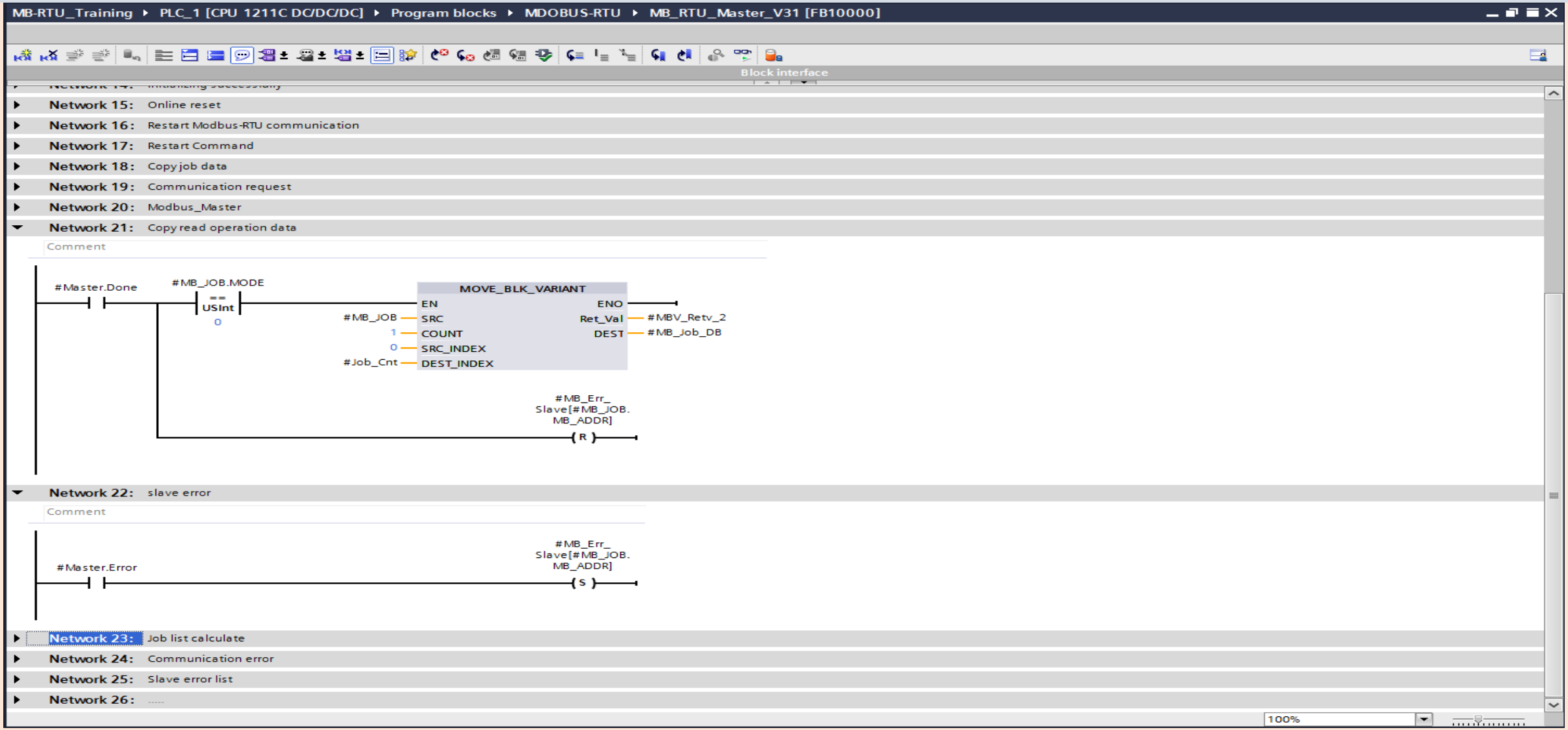
MB_RTU_Master_3.1通讯功能块（6）



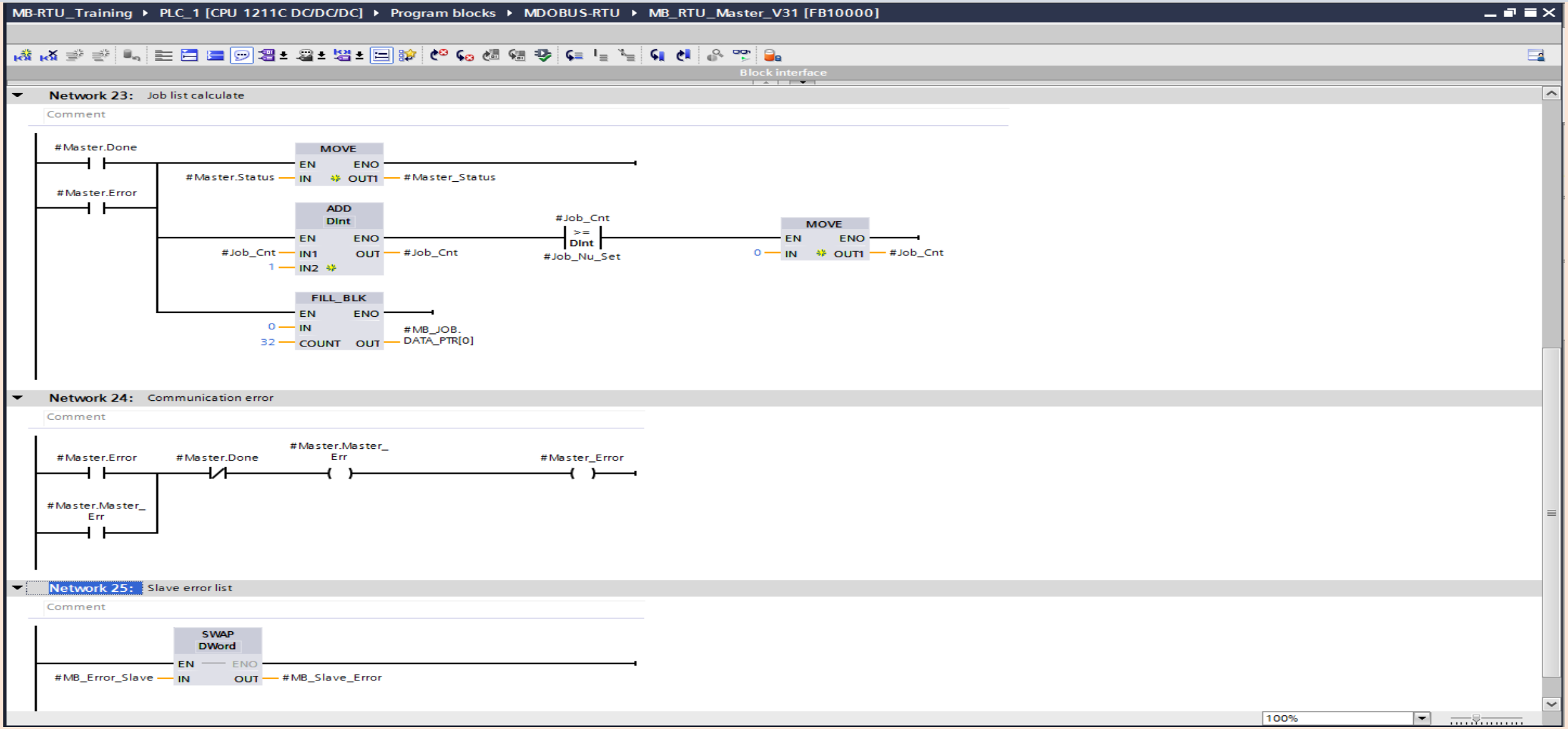
MB_RTU_Master_3.1通讯功能块（7）



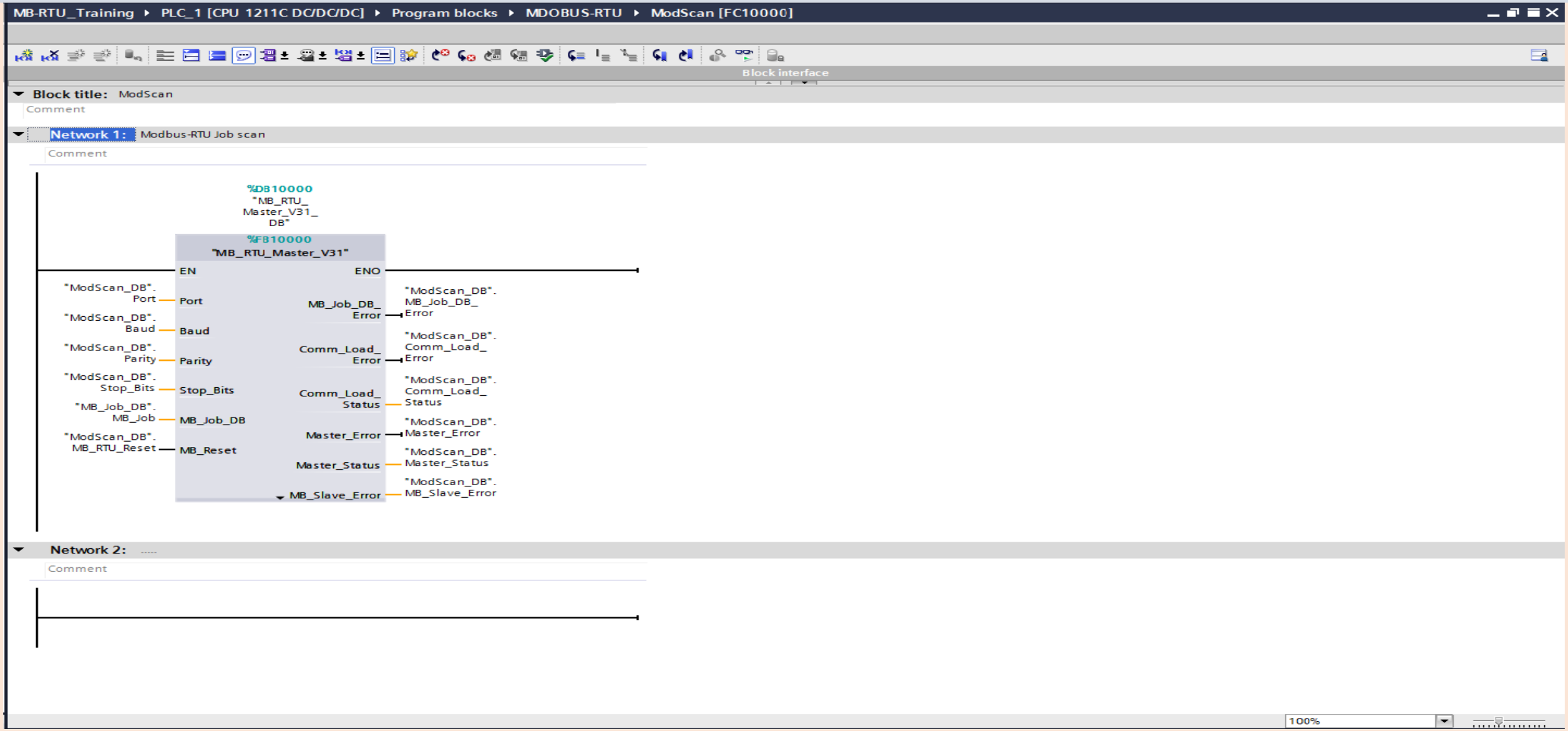
MB_RTU_Master_3.1通讯功能块（8）



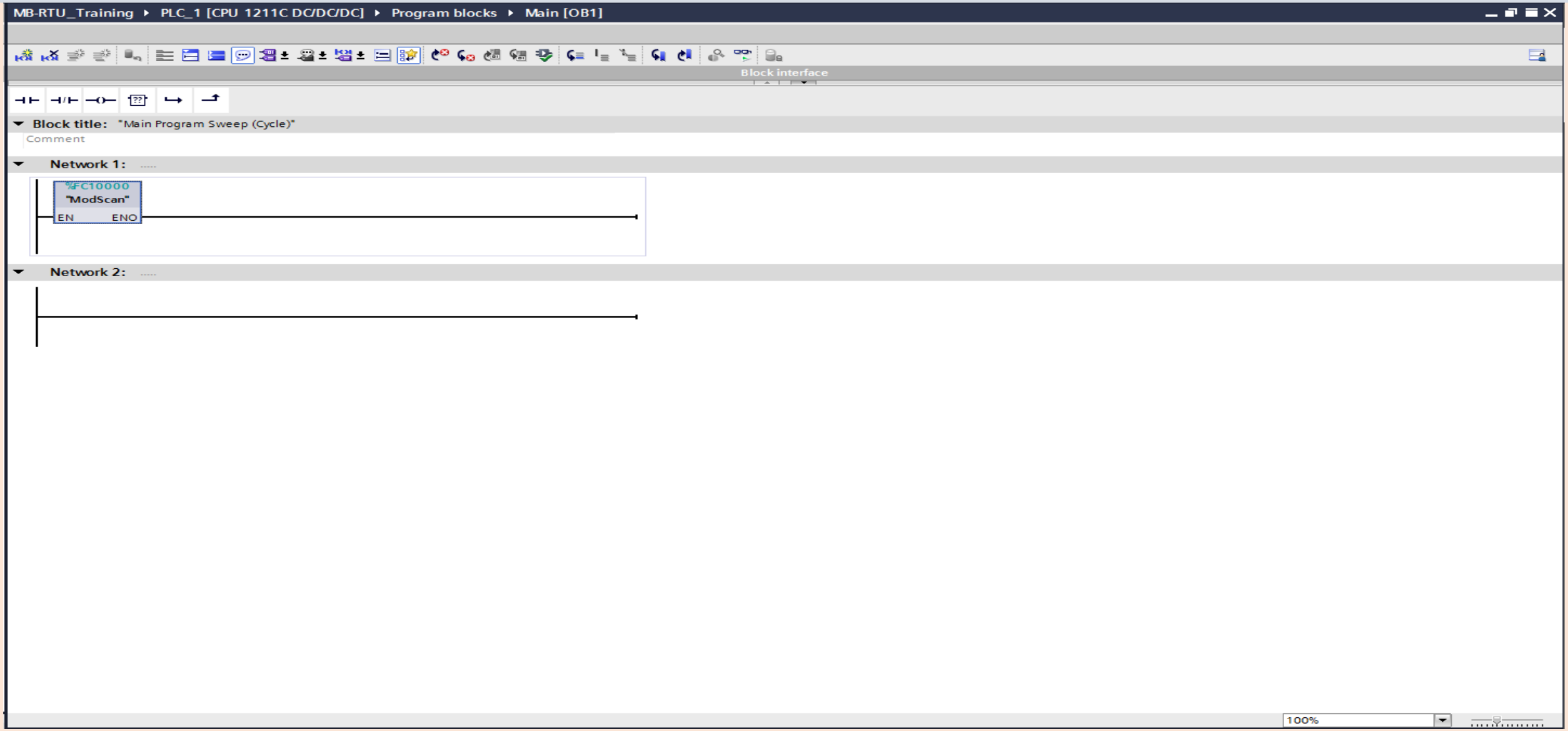
MB_RTU_Master_3.1通讯功能块（9）



MB_RTU_Master_3.1通讯功能块（10）



MB_RTU_Master_3.1通讯功能块（11）



基于任务轮询机制的Modbus-RTU主站通讯程序实现的总结

1. 梯形图(LAD)，优化模式编程，轮询程序的本质就是数据的间址化处理；
2. 通讯数据亦采用优化模式，MODBUS-RTU/MODBUS-TCP通讯适合博图的数据优化模式，推荐使用；
3. 程序自动识别任务列表数据块的最大通讯任务数量，以及比对任务数据结构的定义是否符合使用规定；
4. 程序具备自动初始化，自主循环工作的能力，无须外部变量干预控制，也无须额外编写程序；
5. 可在CPU运行中动态修改通讯接口参数，无须重新下载程序及硬件组态；
6. 支持动态修改任务参数及任务数量，通过数据块的修改来改变通讯任务类型及数量，无须修改通讯程序；
7. 支持动态故障从站地址（地址1~31）报警；
8. 标准化模块化可移植，支持博图下S7-1200/1500/OpenController所有CPU及对应通讯接口，即考即用
9. 基础性的通用通讯程序，适合所有支持Modbus-RTU协议的通讯对象（仪表，驱动，PLC，执行机构等）；
10. 更适合Modbus-RTU通讯***轮询场景1***及***轮询场景3***的应用；

基于任务轮询机制的Modbus-RTU主站通讯程序的实现

基于任务轮询机制的Modbus-RTU主站通讯程序例程：

https://yunpan.360.cn/surl_yH2cm8RukyI （提取码：9ca5）

课后思考题：

在上述例程的基础上，如何简便地实现***轮询场景2***中所描述的，针对多个相同的通讯对象，每个通讯对象都有的一个或多个不同的通讯任务的轮询通讯。