CIP Modbus Object Read Example

Quantum 140NOC77101 using
Explicit Messaging via MBP_MSTR

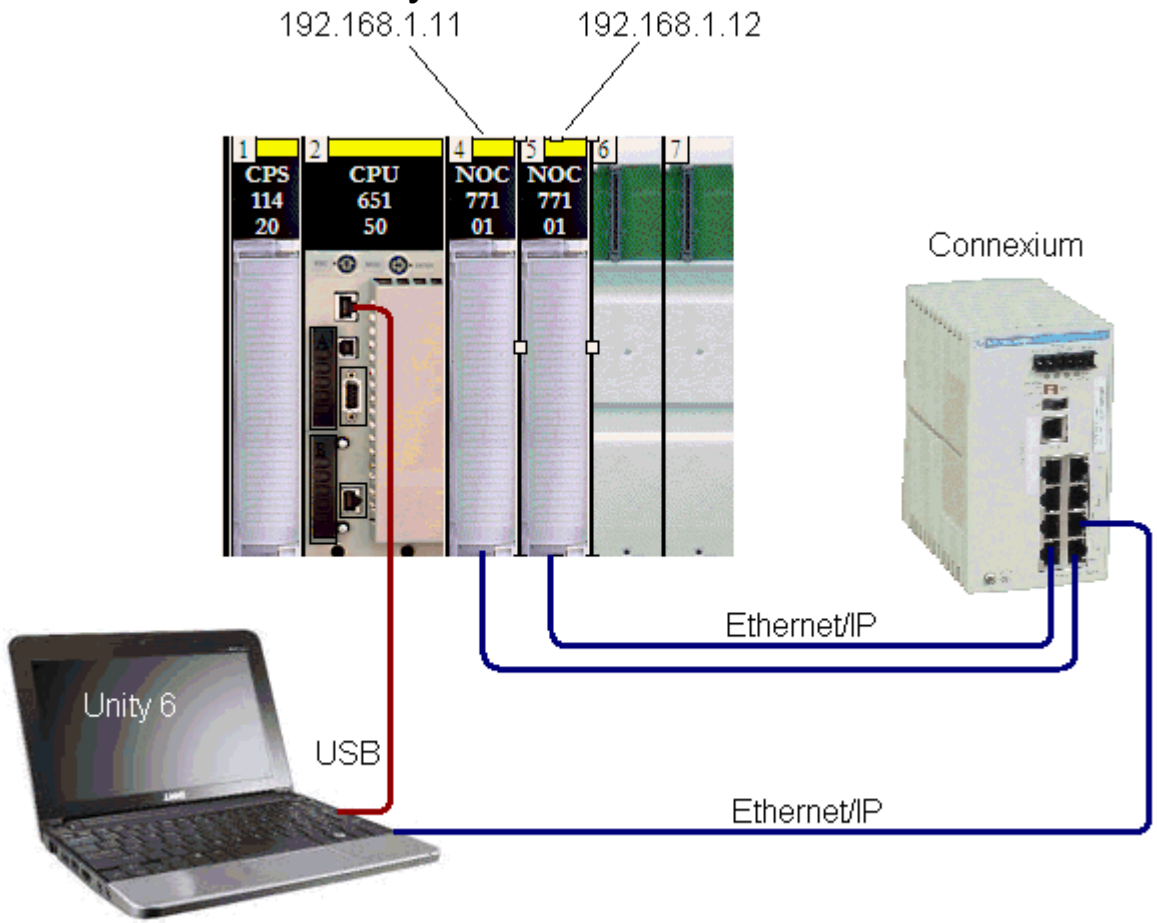
Dec 15, 2012

Version 1.0

Schneider Electric

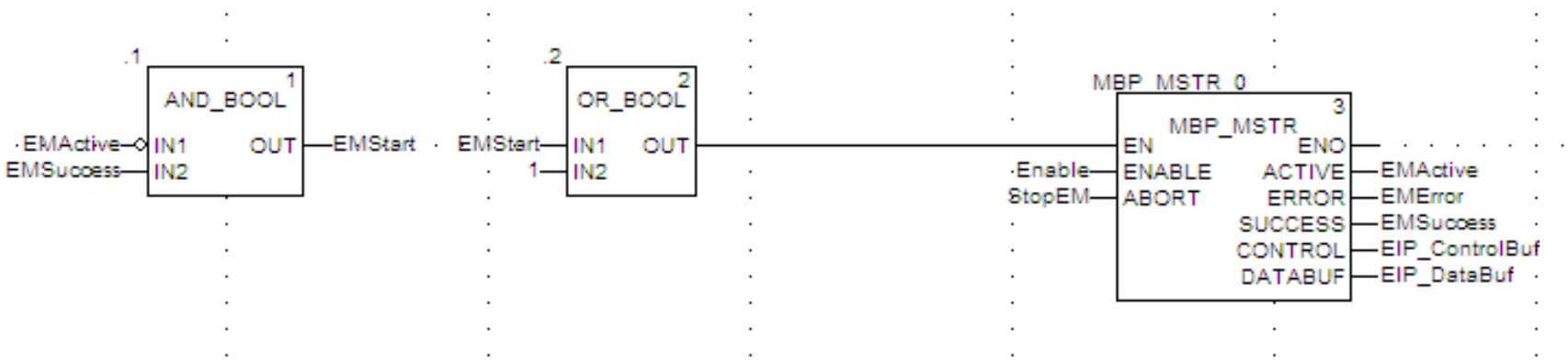
PLC Hardware Configuration

- NOC77101 (192.168.1.11) to query NOC77101 (192.168.1.12) with Explicit Messaging CIP Modbus Object READ.
- The USB connection is for Unity to PLC communications.

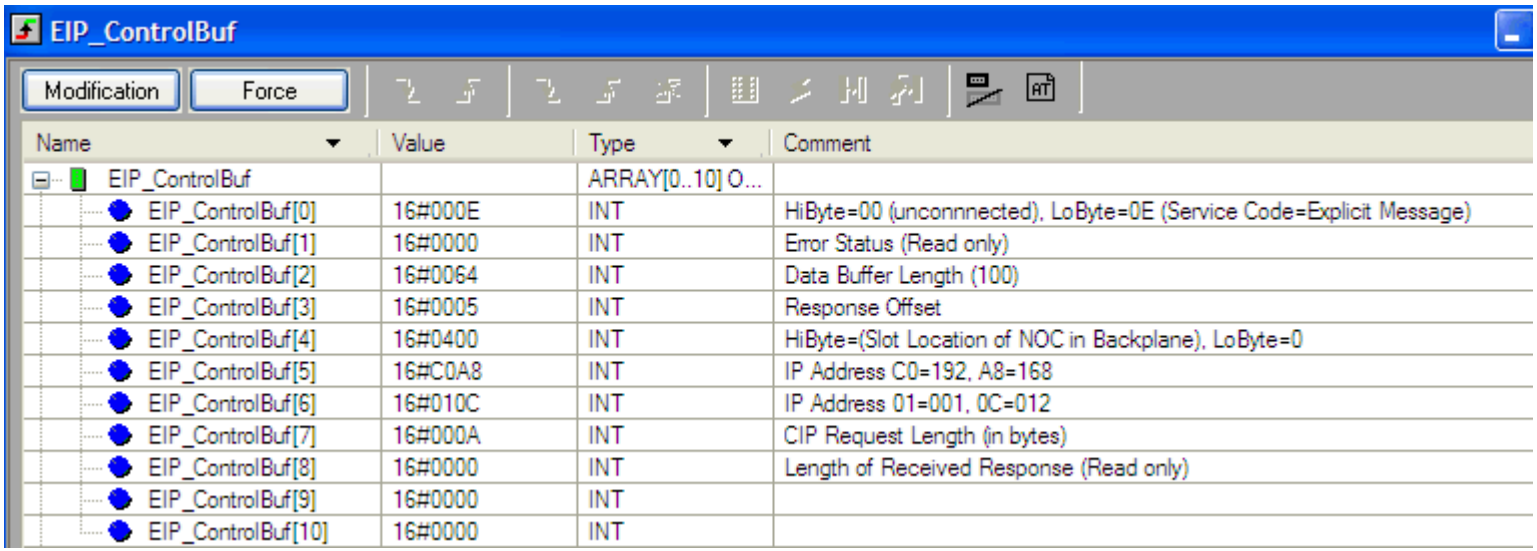


Unity Program

- Note to add the ‘Pin negation’ on the AND_BOOL IN1 input.



EIP_ControlBuf
CIP Request



Name	Value	Type	Comment
EIP_ControlBuf		ARRAY[0..10] O...	
EIP_ControlBuf[0]	16#000E	INT	HiByte=00 (unconnnected), LoByte=0E (Service Code=Explicit Message)
EIP_ControlBuf[1]	16#0000	INT	Error Status (Read only)
EIP_ControlBuf[2]	16#0064	INT	Data Buffer Length (100)
EIP_ControlBuf[3]	16#0005	INT	Response Offset
EIP_ControlBuf[4]	16#0400	INT	HiByte=(Slot Location of NOC in Backplane), LoByte=0
EIP_ControlBuf[5]	16#C0A8	INT	IP Address C0=192, A8=168
EIP_ControlBuf[6]	16#010C	INT	IP Address 01=001, 0C=012
EIP_ControlBuf[7]	16#000A	INT	CIP Request Length (in bytes)
EIP_ControlBuf[8]	16#0000	INT	Length of Received Response (Read only)
EIP_ControlBuf[9]	16#0000	INT	
EIP_ControlBuf[10]	16#0000	INT	

- EIP_ControlBuf(1) and EIP_ControlBuf(8) are Read Only and written by the PLC.
- EIP_ControlBuf(8), Length of Received Response, will toggle between 0 and E (hex) when it is operational.

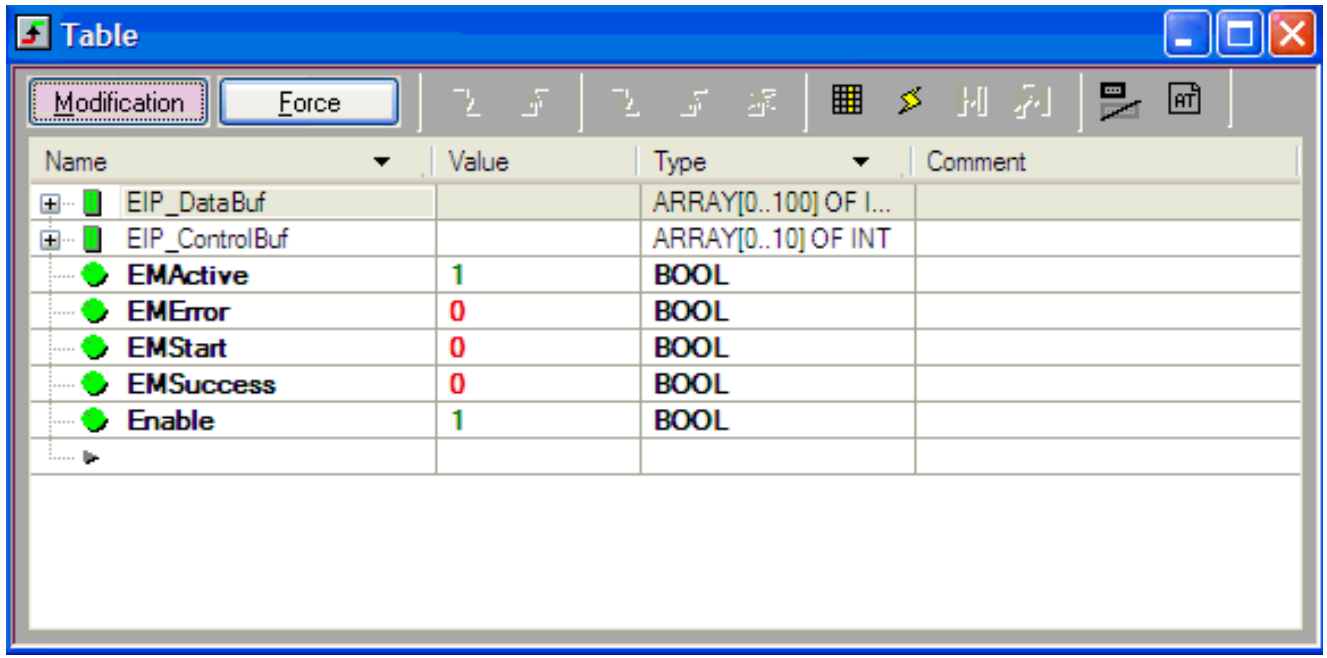
EIP_DataBuf
CIP Request

Modification | Force

Name	Value	Type	Comment
EIP_DataBuf		ARRAY[0..100] ...	
EIP_DataBuf[0]	16#024E	INT	HiByte=02 (Path Size); LoByte=4E (Service Code-Read Holding Reg)
EIP_DataBuf[1]	16#4420	INT	Hi Bye=44 (Class Assembly Object); LoByte=20 (Logical Class Segment)
EIP_DataBuf[2]	16#0124	INT	HiByte=01 (Instance); LoByte=24 (Logical Instance Segment)
EIP_DataBuf[3]	16#0002	INT	First Word to be Read (value + %MW1 = First Word)
EIP_DataBuf[4]	16#0005	INT	Number of Words to Read
EIP_DataBuf[5]	16#0000	INT	[Service Code + Response Bit [MSB]) Response = CE (Read Only)
EIP_DataBuf[6]	16#0000	INT	[Service Response=0, Success] (Read Only)
EIP_DataBuf[7]	0	INT	Response Word 1
EIP_DataBuf[8]	0	INT	Response Word 2
EIP_DataBuf[9]	0	INT	Response Word 3
EIP_DataBuf[10]	0	INT	Response Word 4
EIP_DataBuf[11]	0	INT	Response Word 5

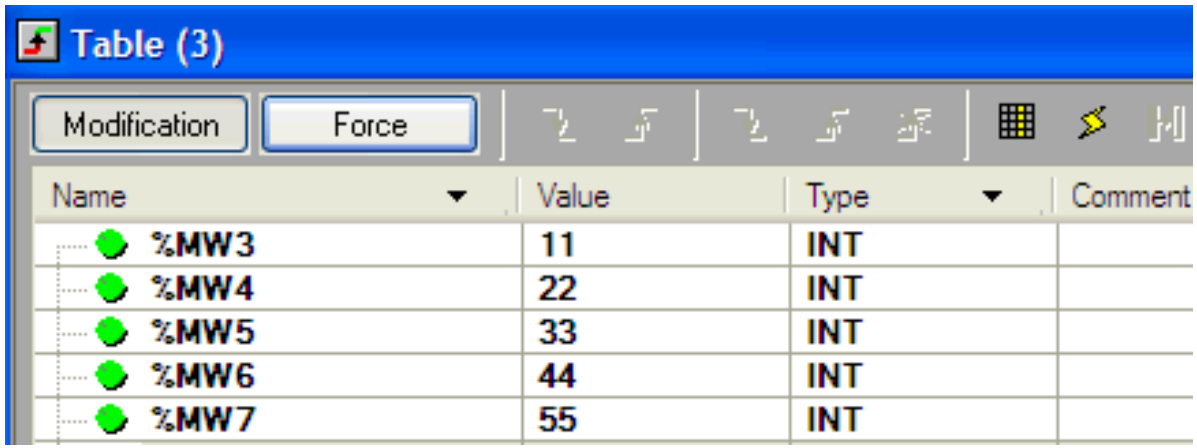
Control and Status Variables

- Set Enable to a value of 1 to start the messaging.
- In a successful implementation, EMActive, EMStart, and EMSuccess will flash between 0 and 1.



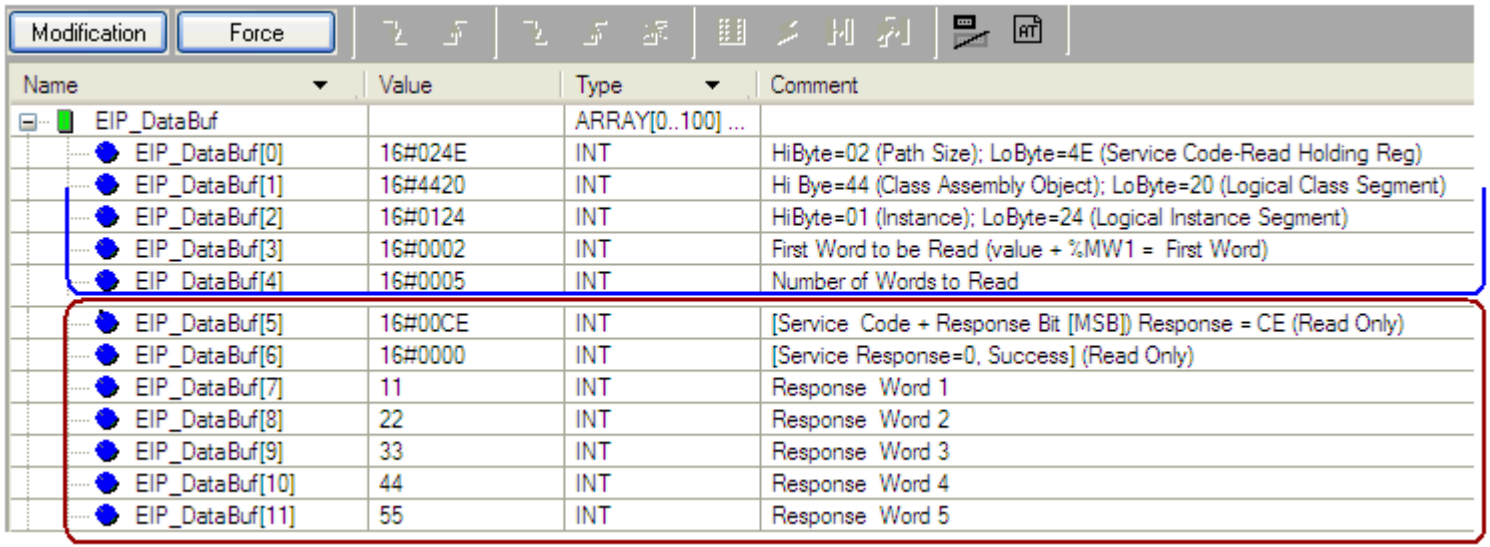
Data in PLC to be Read

- This data can be changed manually in the PLC to observe the data changing in the response.



EIP_DataBuf
CIP Response

- The message response is located in the EIP_DataBuf array beginning at EIP_DataBuf(5) as indicated in the area highlighted in red.
- The area highlighted in blue in the EIP_DataBuf array contains part of the query message previously entered.



Name	Value	Type	Comment
EIP_DataBuf		ARRAY[0..100] ...	
EIP_DataBuf[0]	16#024E	INT	HiByte=02 (Path Size); LoByte=4E (Service Code-Read Holding Reg)
EIP_DataBuf[1]	16#4420	INT	Hi Bye=44 (Class Assembly Object); LoByte=20 (Logical Class Segment)
EIP_DataBuf[2]	16#0124	INT	HiByte=01 (Instance); LoByte=24 (Logical Instance Segment)
EIP_DataBuf[3]	16#0002	INT	First Word to be Read (value + %MW1 = First Word)
EIP_DataBuf[4]	16#0005	INT	Number of Words to Read
EIP_DataBuf[5]	16#00CE	INT	[Service Code + Response Bit [MSB]) Response = CE (Read Only)
EIP_DataBuf[6]	16#0000	INT	[Service Response=0, Success] (Read Only)
EIP_DataBuf[7]	11	INT	Response Word 1
EIP_DataBuf[8]	22	INT	Response Word 2
EIP_DataBuf[9]	33	INT	Response Word 3
EIP_DataBuf[10]	44	INT	Response Word 4
EIP_DataBuf[11]	55	INT	Response Word 5