CIP Modbus Object Write Example

Quantum 140NOC77101 using
Explicit Messaging via MBP_MSTR

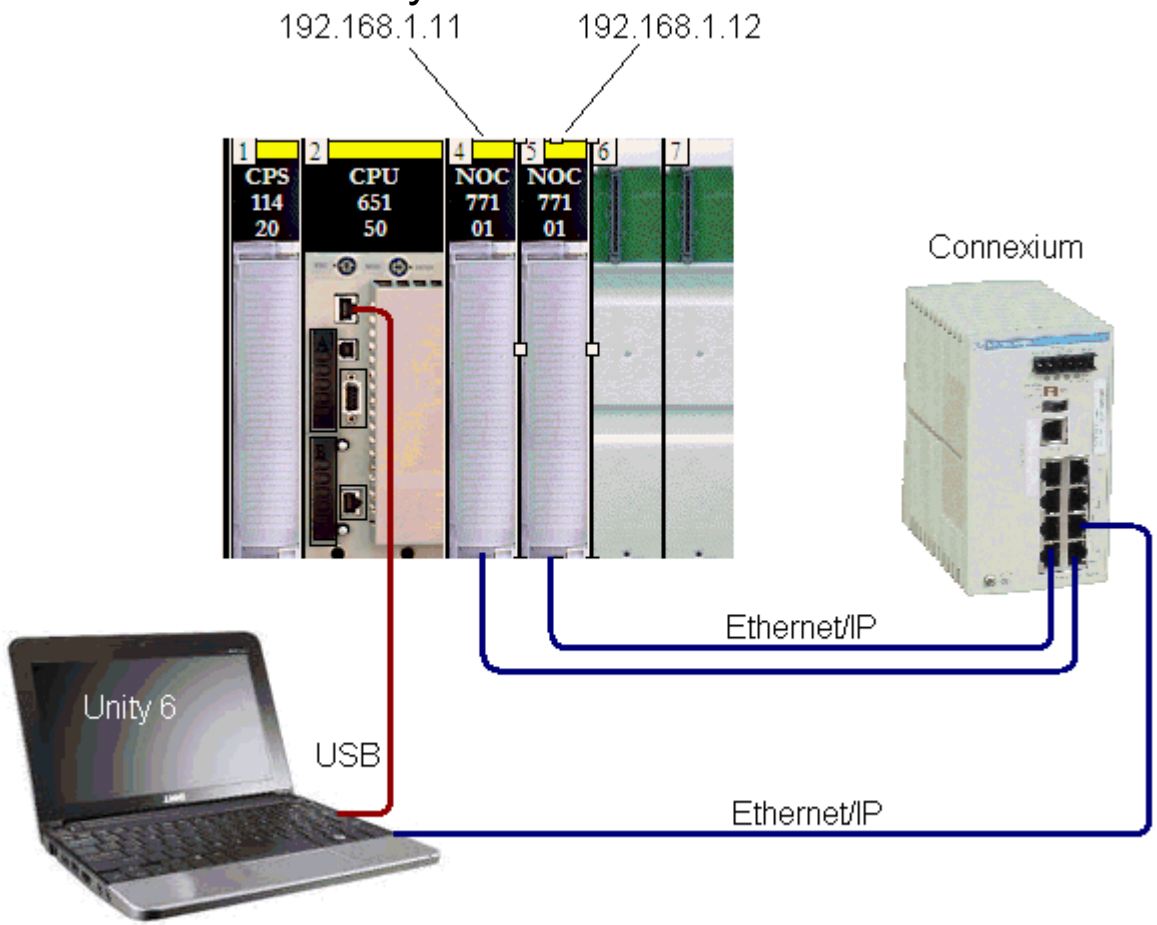
Dec 15, 2012

Version 1.0

Schneider Electric

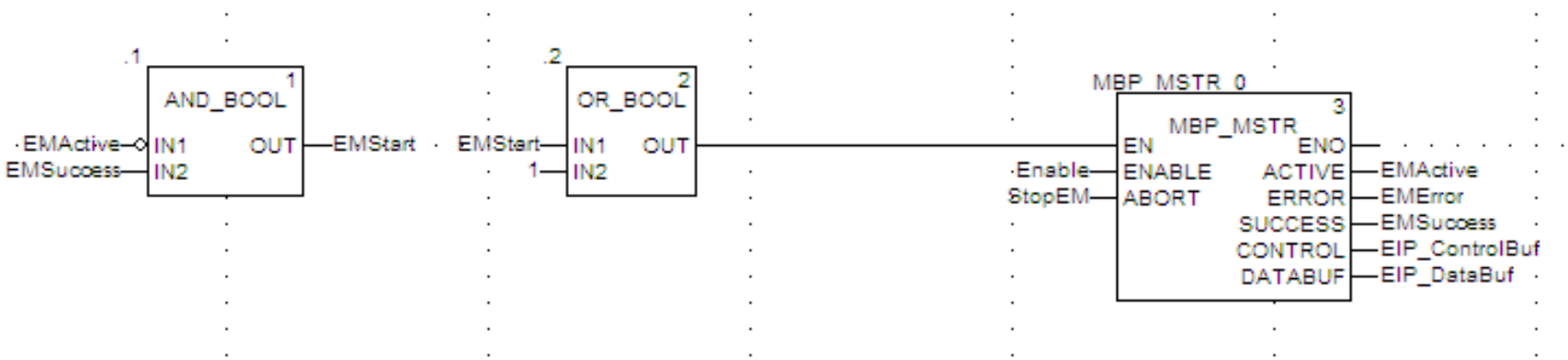
PLC Hardware Configuration

- NOC77101 (192.168.1.11) to query NOC77101 (192.168.1.12) with Explicit Messaging CIP Modbus Object WRITE.
- 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

EIP_ControlBuf

Modification | Force

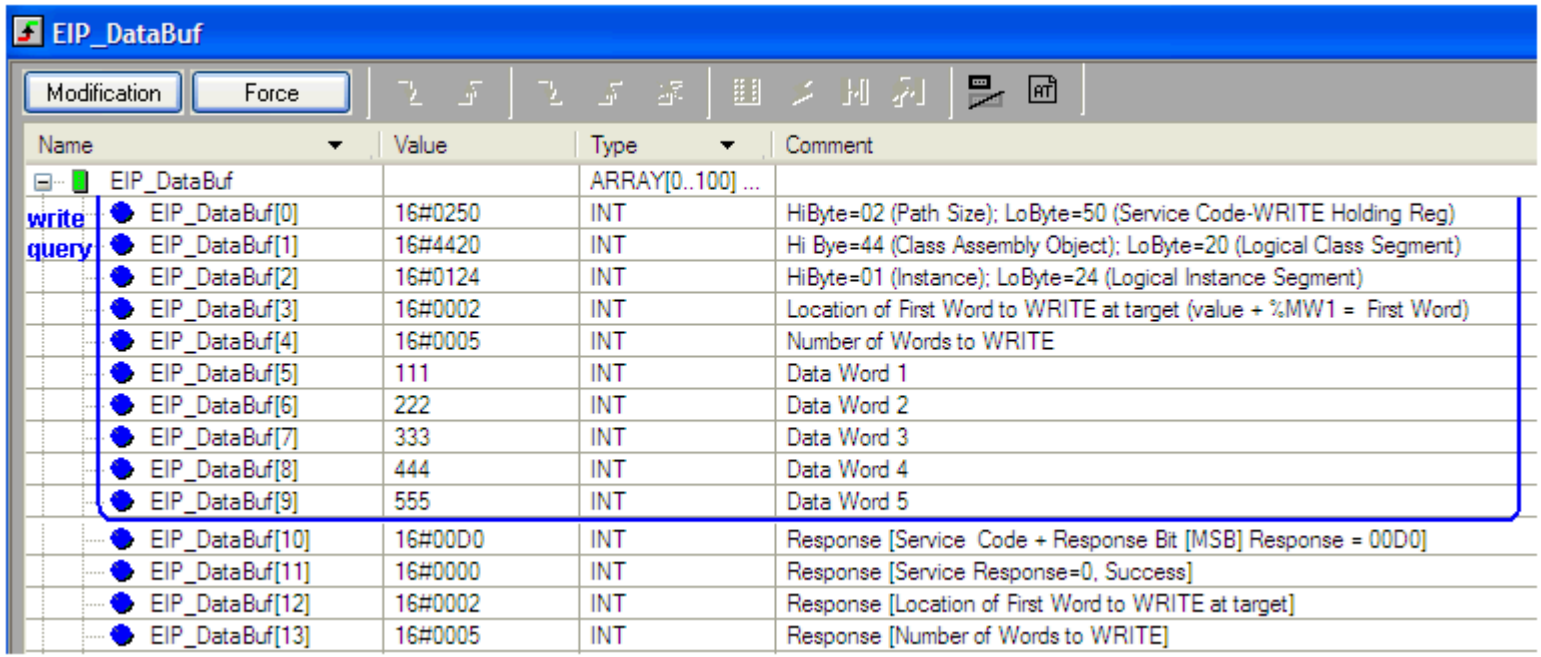
	Name	Value	Type	Comment
	EIP_ControlBuf		ARRAY[0..10] O...	
	EIP_ControlBuf[0]	16#000E	INT	HiByte=00 (unconnected); LoByte=0E (Service Code=Explicit Message)
1	EIP_ControlBuf[1]	16#0000	INT	Error Status (Read Only)
2	EIP_ControlBuf[2]	16#0014	INT	EIP_DataBuf Length (In WORDS)
	EIP_ControlBuf[3]	16#000A	INT	Response Offset in EIP_DataBuf
	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
3	EIP_ControlBuf[7]	16#0014	INT	CIP Request Length (in BYTES)
1	EIP_ControlBuf[8]	16#0000	INT	Length of Received Response (Read Only)
	EIP_ControlBuf[9]	16#0000	INT	
	EIP_ControlBuf[10]	16#0000	INT	

[1] EIP_ControlBuf[1] and EIP_ControlBuf(8) are Read Only and not configurable.

[2] EIP_ControlBuf[2] must be equal to or greater than the total EIP_DataBuf message and response length.

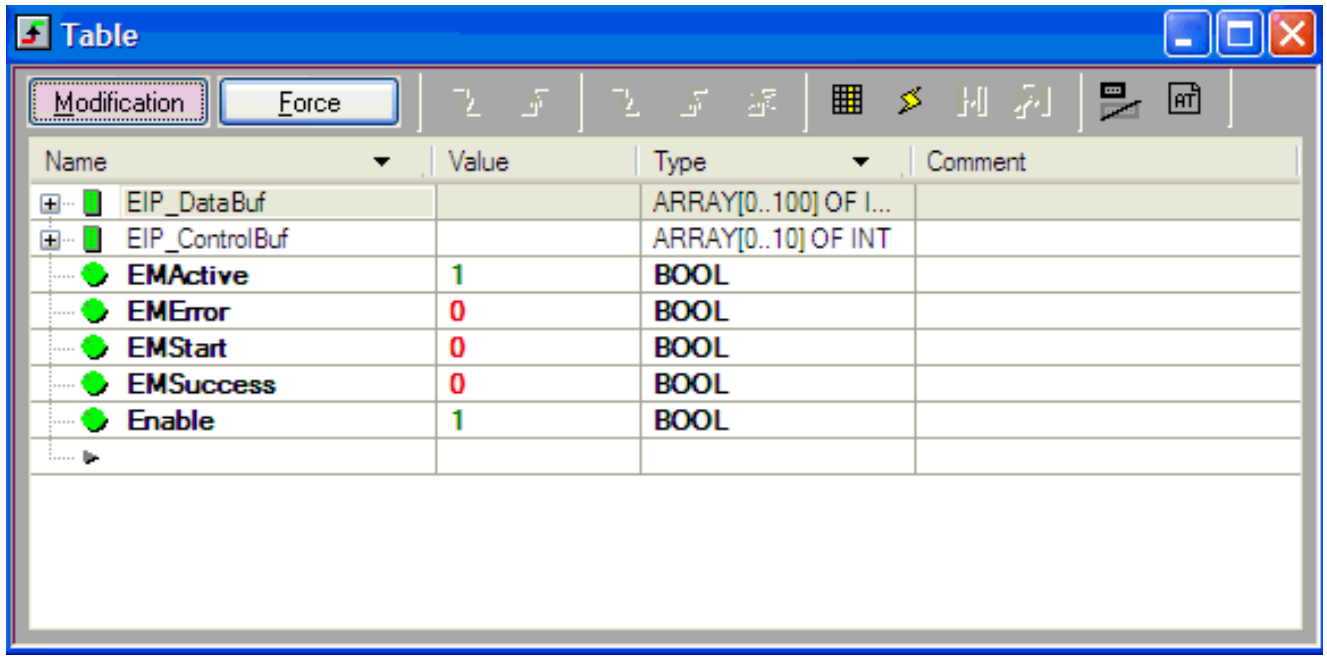
[3] EIP_ControlBuf[7] value is the total number of bytes of the CIP message (10 bytes) plus the total number of data bytes to Write.
EIP_ControlBuf[7] = (10 bytes) + (2 x (EIP_DataBuf[4])

EIP_DataBuf
CIP Request



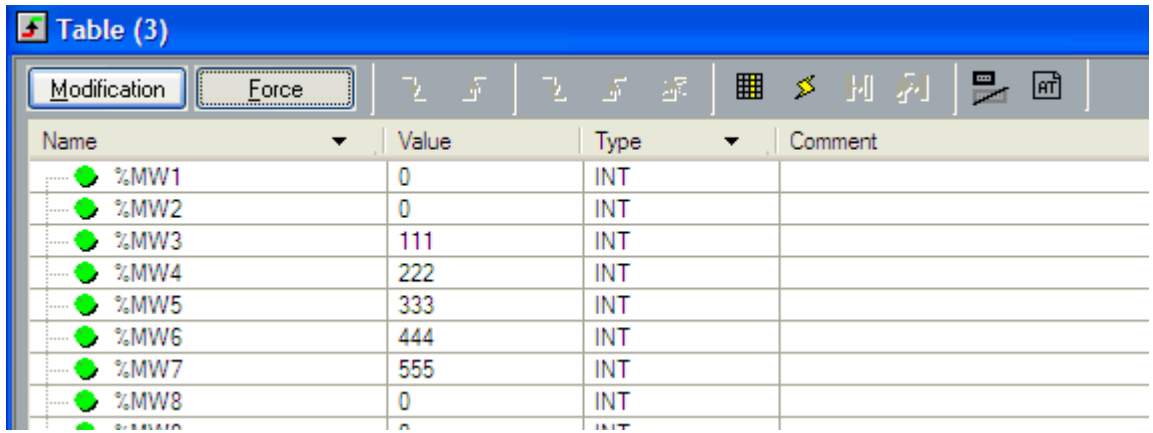
Control and Status Variables

- 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.

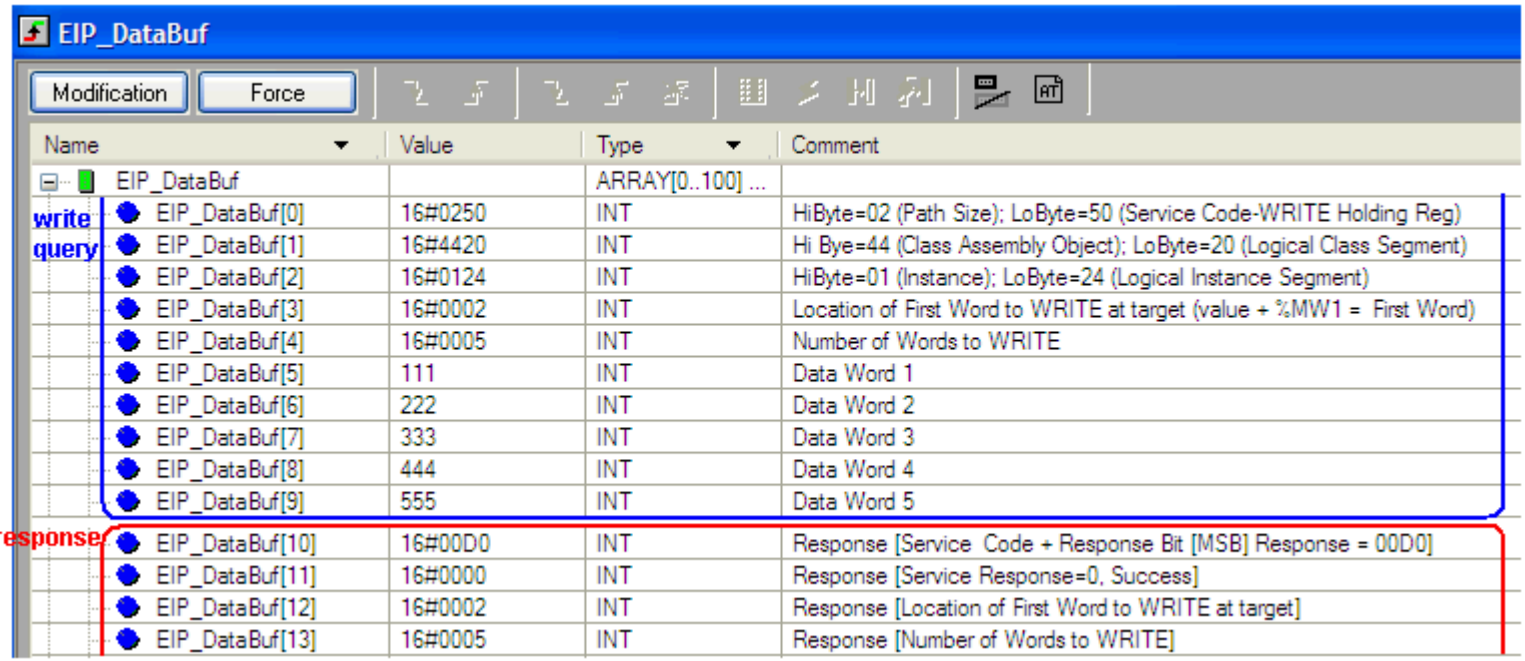


To view where the data is written in the PLC

- The data can be changed manually in the EIP_DataBuf words [5] through [9] to observe the data changes in the PLC in %MW3 through %MW7.



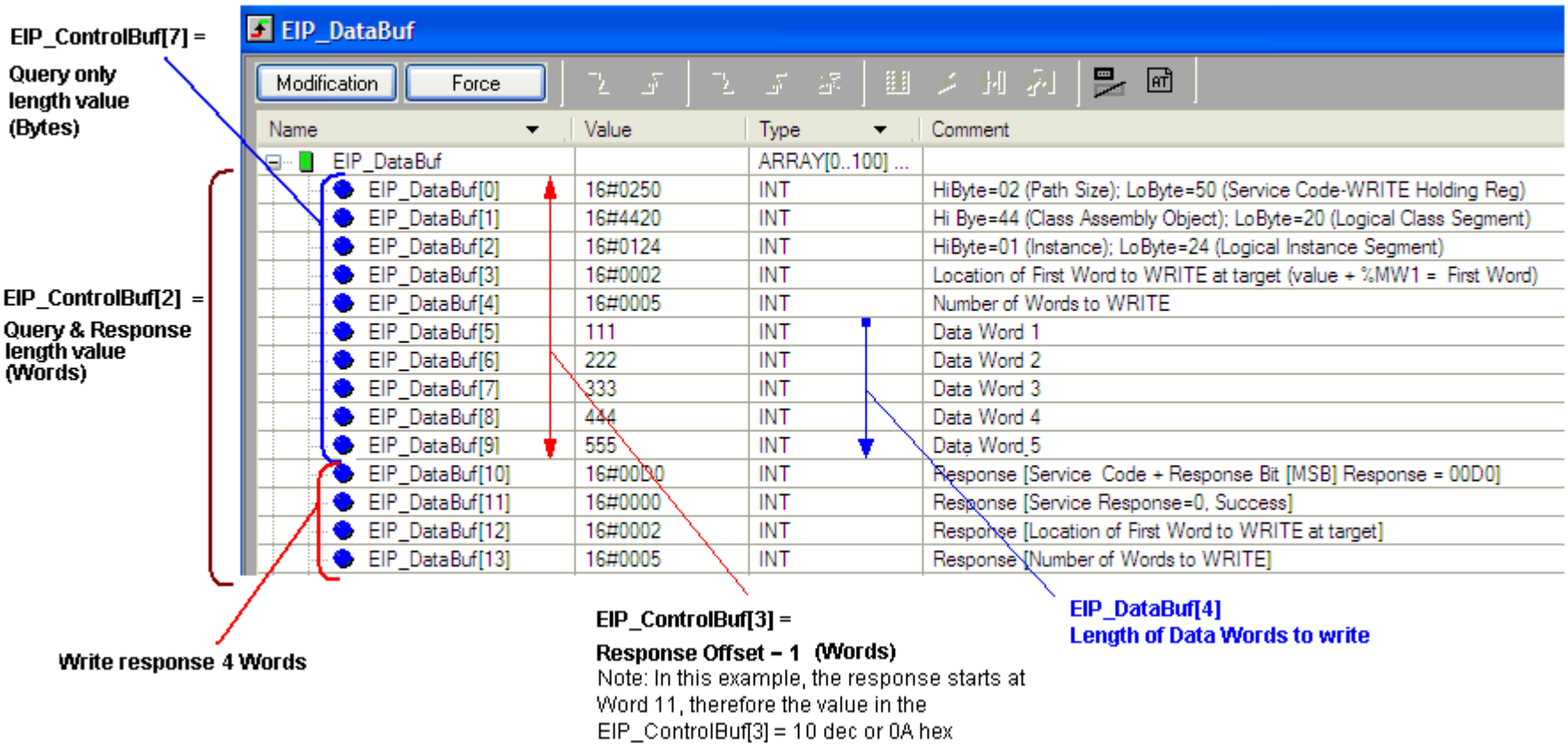
EIP_DataBuf
CIP Response



Name	Value	Type	Comment
EIP_DataBuf		ARRAY[0..100] ...	
EIP_DataBuf[0]	16#0250	INT	HiByte=02 (Path Size); LoByte=50 (Service Code-WRITE 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	Location of First Word to WRITE at target (value + %MW1 = First Word)
EIP_DataBuf[4]	16#0005	INT	Number of Words to WRITE
EIP_DataBuf[5]	111	INT	Data Word 1
EIP_DataBuf[6]	222	INT	Data Word 2
EIP_DataBuf[7]	333	INT	Data Word 3
EIP_DataBuf[8]	444	INT	Data Word 4
EIP_DataBuf[9]	555	INT	Data Word 5
EIP_DataBuf[10]	16#00D0	INT	Response [Service Code + Response Bit [MSB] Response = 00D0]
EIP_DataBuf[11]	16#0000	INT	Response [Service Response=0, Success]
EIP_DataBuf[12]	16#0002	INT	Response [Location of First Word to WRITE at target]
EIP_DataBuf[13]	16#0005	INT	Response [Number of Words to WRITE]

- The message response is located in the EIP_DataBuf array beginning at EIP_DataBuf[10] as indicated in the area highlighted in red. The location of the 'Response' is determined by the 'offset value + 1' in the EIP_ControlBuf[3], which must be larger than the write query length.

EIP_DataBuf, EIP_ControlBuf Notes



EIP_DataBuf

Modification | Force

Name	Value	Type	Comment
EIP_DataBuf		ARRAY[0..100] ...	
EIP_DataBuf[0]	16#0250	INT	HiByte=02 (Path Size); LoByte=50 (Service Code-WRITE 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	Location of First Word to WRITE at target (value + %MW1 = First Word)
EIP_DataBuf[4]	16#0005	INT	Number of Words to WRITE
EIP_DataBuf[5]	111	INT	Data Word 1
EIP_DataBuf[6]	222	INT	Data Word 2
EIP_DataBuf[7]	333	INT	Data Word 3
EIP_DataBuf[8]	444	INT	Data Word 4
EIP_DataBuf[9]	555	INT	Data Word 5
EIP_DataBuf[10]	16#00D0	INT	Response [Service Code + Response Bit [MSB] Response = 00D0]
EIP_DataBuf[11]	16#0000	INT	Response [Service Response=0, Success]
EIP_DataBuf[12]	16#0002	INT	Response [Location of First Word to WRITE at target]
EIP_DataBuf[13]	16#0005	INT	Response [Number of Words to WRITE]