PACiS SPP MODBUS

Gateway and C264

SPP/EN MODBUS/D10

PACiS V5

Slave Protocol Profile
MODBUS

Issue A1

Schneider Electric

CONTENTS

1. INTRODUCTION

1.1 Scope of the document

This document is a chapter of PACiS MiCOM C264 and the PACiS gateway documentation binders. It describes the MODBUS slave protocols (communication with SCADA systems) implemented on PACiS MiCOM C264 and PACiS GATEWAY.

Slave MODBUS protocol implemented on PACiS MiCOM C264:

- Generic serial slave MODBUS: MODICON

Slave MODBUS protocol implemented on PACIS GATEWAY:

- Generic serial slave MODBUS: MODICON
- Generic TCP/IP slave MODBUS: MODICON

1.2 Glossary

C264	PACiS Computer C264
GTW	PACiS gateway
IED	Intelligent Electronic Device
N	Stand for Not supported In interoperability tables
S	Stand for Supported In interoperability tables
SCADA	Supervisory Control and Data Acquisition

2. INTEROPERABILITY

2.1 Network configuration (Network-specific parameter)

C264	GTW	Description
S	**S**	Point-to-point
N	N	Multiple point-to-point
S	**S**	Multipoint-party line
N	N	Multipoint-star

2.2 Physical layer (Network-specific parameter)

2.2.1 Serial Transmission speed (control and monitor direction):

C264	GTW	Description
S	**S**	300 bit/s
S	**S**	600 bit/s
S	**S**	1 200 bit/s
S	**S**	2 400 bit/s
S	**S**	4 800 bit/s
S	**S**	9 600 bit/s
S	**S**	19 200 bit/s
S	**S**	38 400 bit/s
N	N	56 000 bit/s
N	N	57 600 bit/s
N	N	64 000 bit/s

2.2.2 Network card

General Ethernet card supports.

C264	GTW	Description
N	**S**	10M
N	**S**	100M
N	N	1000M

2.3 Link layer (Network-specific parameter)

2.3.1 Link transmission procedure

MODBUS is a master/slave protocol that is used by many devices such as relays, computers or monitoring devices.

As the computer is the slave on the TBUS, this protocol is referenced as “Slave MODBUS” in the computer. So, there is one kind of exchange which is “Request/reply”: Slave computer receive a request emitted by a SCADA and responds to it.

2.3.1.1 Link Type

C264	GTW	Description
S	**S**	Serial
N	**S**	TCP

2.3.1.2 Transmission mode

C264	GTW	Description
N	N	ASCII Mode
S	**S**	RTU Mode

NOTES:

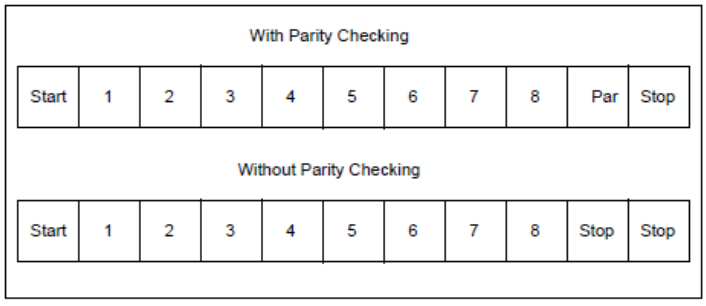
1. The format for each byte in RTU mode is:

Coding System: 8–bit binary, hexadecimal 0–9, A–F
Two hexadecimal characters contained in each 8–bit field of the message

Bits per Byte: 1 start bit
8 data bits, least significant bit sent first
1 bit for even/odd parity; no bit for no parity
1 stop bit if parity is used; 2 bits if no parity

Error Check Field: Cyclical Redundancy Check (CRC)

With RTU character framing, the bit sequence is:



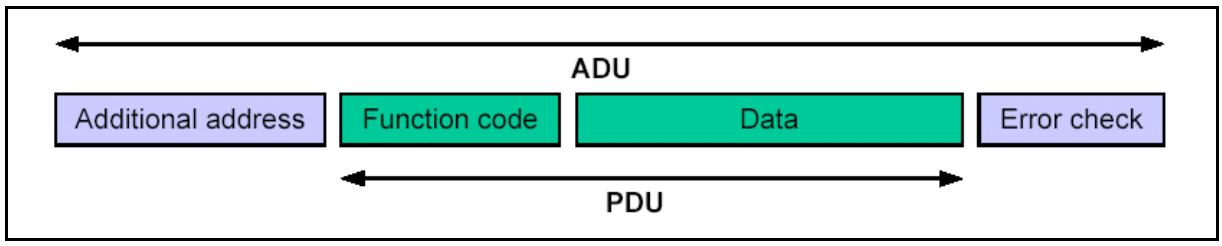
2. RTU Message frame:

In RTU mode, messages start and end with a silent interval of at least 3.5 character times (shown as T1–T2–T3–T4 in the figure below).
When the first field (the address field) is received, each device decodes it to find out if it is the addressed device.
The entire message frame must be transmitted as a continuous stream. If a silent interval of more than 1.5 character times occurs before completion of the frame, the receiving device flushes the incomplete message and assumes that the next byte will be the address field of a new message.
Similarly, if a new message begins earlier than 3.5 character times following a previous message, the receiving device will consider it a continuation of the previous message. This will set an error, as the value in the final CRC field will not be valid for the combined messages.

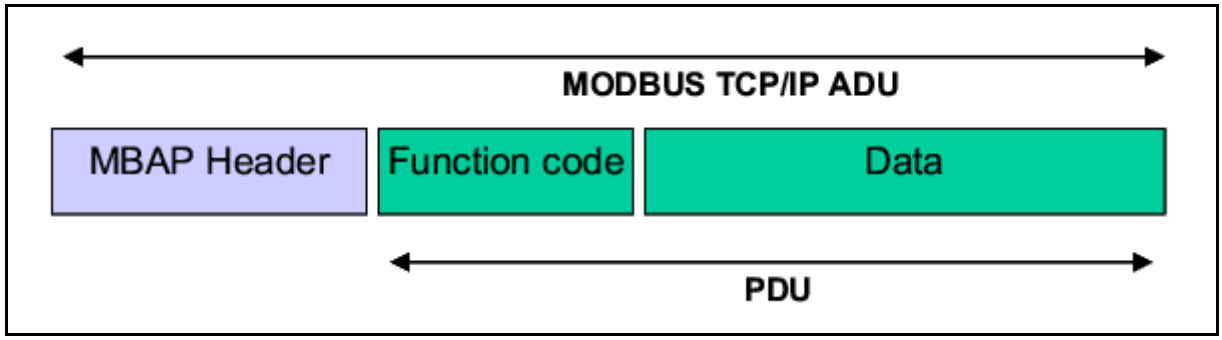
START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1–T2–T3–T4	8 BITS	8 BITS	*n* x 8 BITS	16 BITS	T1–T2–T3–T4

2.3.2 Frame Structure

2.3.2.1 Serial RS232/RS485



2.3.2.2 TCP Ethernet



PDU is identical for both serial and TCP. First field of ADU, "Additional address", is "MBAP Header" and "Error check" disappear (TCP/IP control).

MBAP (ModBus Application Protocol header) is a seven bytes header filed as follow:

Fields	Length (bytes)	Description	SCADA	GTW
Transaction Identifier	2	Identification of a MODBUS Request/Response transaction	Initialized by the SCADA	Recopied by the GTW from the received request. No check.
Protocol Identifier	2	0 = MODBUS protocol	Initialized by the SCADA	Recopied by the GTW from the received request. No check.
Length	2	Number of following bytes	Initialized by the SCADA (request)	Initialized by the GTW (response)
Unit Identifier	1	Identification of a remote slave connected on a serial line or on other buses.	Initialized by the SCADA	Recopied by the GTW from the received request. No check.

2.3.3 Frame length

2.3.3.1 Serial RS232/RS485

C264	GTW	Description
up to 256	up to 256	number of bytes in control direction
up to 256	up to 256	number of bytes in monitor direction

2.3.3.2 TCP Ethernet

C264	GTW	Description
N	up to 260	number of bytes in control direction
N	up to 260	number of bytes in monitor direction

2.4 Application layer

2.4.1 Selection of standard Modbus functions

C264	GTW	Function Code	Description
S	**S**	01	READ COIL STATUS [identical to function code 02]
S	**S**	02	READ INPUT STATUS [identical to function code 01]
S	**S**	03	READ HOLDING REGISTERS [identical to function code 04]
S	**S**	04	READ INPUT REGISTERS [identical to function code 03]
S	**S**	05	FORCE SINGLE COIL
N	N	06	PRESET SINGLE REGISTER
S*	N	07	READ EXCEPTION STATUS (*) C264 always answer with a register set to “0”
S	**S**	08	DIAGNOSTICS [only sub function 0 is supported]
N	N	09	PROGRAM 484
N	N	10	POLL 484
N	N	11	FETCH COMM. EVENT CTR.
N	N	12	FETCH COMM. EVENT LOG
N	N	13	PROGRAM CONTROLLER
N	N	14	POLL CONTROLLER
S	**S**	15	FORCE MULTIPLE COILS [identical to function code 05, one point authorized only]
N	N	16	PRESET MULTIPLE REGISTERS [identical to function code 06, one point authorized only]
N	N	17	REPORT SLAVE ID
N	N	18	PROGRAM 884/M84
N	N	19	RESET COMM. LINK
N	N	20	READ GENERAL REFERENCE
N	N	21	WRITE GENERAL REFERENCE
N	N	22	MASK WRITE 4X REGISTER
N	N	23	READ/WRITE 4X REGISTERS
N	N	24	READ FIFO QUEUE

2.4.2 Error Management

In the query-response cycle, if an error is detected by the slave, the function code of the response is modified by the slave to indicates that the response is an error response.

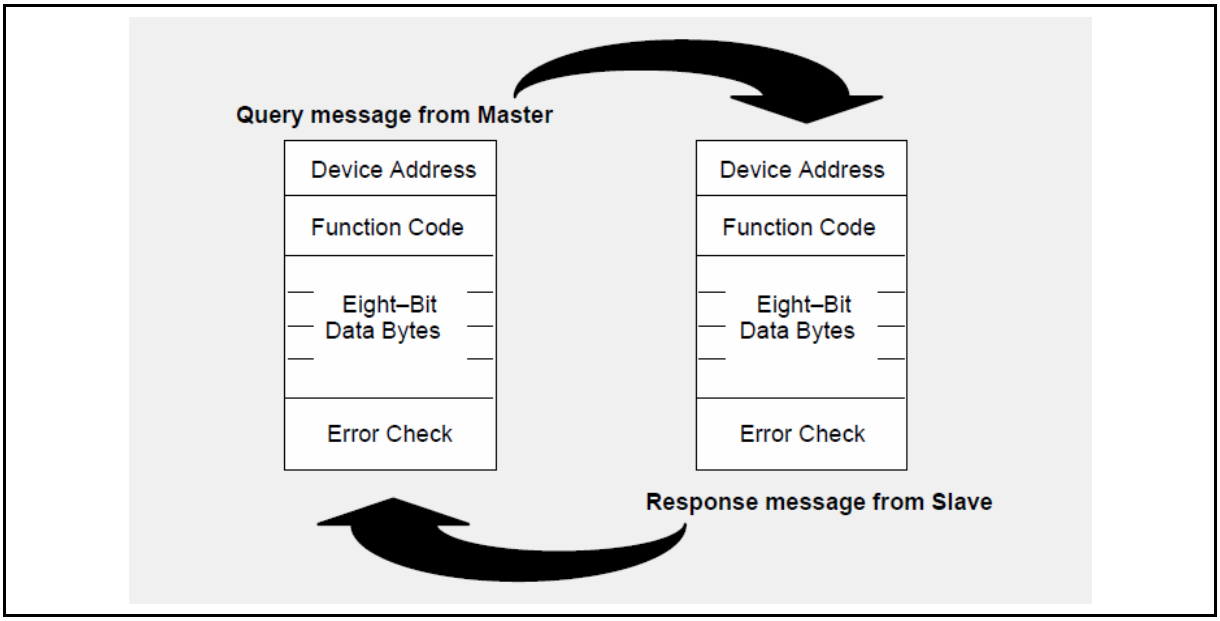


FIGURE 1: MASTER–SLAVE QUERY–RESPONSE CYCLE

The Query:

The function code in the query tells the addressed slave device what kind of action to perform. The data bytes contain any additional information that the slave will need to perform the function. The error check field provides a method for the slave to validate the integrity of the message contents.

The Response:

If the slave makes a normal response, the function code in the response is an echo of the function code in the query. The data bytes contain the data collected by the slave, such as register values or status.

If an error occurs, the function code is modified to indicate that the response is an error (exception) response, and the data bytes contain a code that describes the error. The error check field allows the master to confirm that the message contents are valid.

In an exception response, the slave sets the MSB of the function code to 1. This makes the function code value in an exception response exactly 80 hexadecimal higher than the value would be for a normal response.

Response behavior:

- If the slave device receives the query without a communication error, and can handle the query normally, it returns a normal response.
- If the slave does not receive the query due to a communication error, no response is returned. The master program will eventually process a timeout condition for the query.
- If the slave receives the query, but detects a communication error (parity, LRC, or CRC), no response is returned. The master program will eventually process a timeout condition for the query.
- If the slave receives the query without a communication error, but cannot handle it (for example, if the request is to read a non–existent coil or register), the slave will return an exception response informing the master of the nature of the error.

C264	GTW	Exception code	Meaning	Description
S	**S**	01	ILLEGAL FUNCTION	The function code received in the query is not an allowable action for the slave.
S	**S**	02	ILLEGAL DATA ADDRESS	The data address received in the query is not an allowable address for the slave.
S	**S**	03	ILLEGAL DATA VALUE	A value contained in the query data field is not an allowable value for the slave.
N	**N**	04	SLAVE DEVICE FAILURE	An unrecoverable error occurred while the slave was attempting to perform the requested action.
N	**N**	05	ACKNOWLEDGE	The slave has accepted the request and is processing it, but a long duration of time will be required to do so.
S	**N**	06	SLAVE DEVICE BUSY	The slave is engaged in processing a long–duration program command. The master should retransmit the message later when the slave is free.
S	**N**	07	NEGATIVE ACKNOWLEDGE	The slave cannot perform the program function received in the query.
N	**N**	08	MEMORY PARITY ERROR	The slave attempted to read extended memory, but detected a parity error in the memory. The master can retry the request, but service may be required on the slave device.

Exception codes 04, 05 and 08 aren't used.

Exception code 01 (ILLEGAL FUNCTION)

Exception code 01 will be sent if:

- An unsupported request is received.
- An unsupported sub-function code for Diagnostic request is received (different from 0).

Exception code 02 (ILLEGAL DATA ADDRESS)

PACiS GATEWAY:

For the PACiS GATEWAY, the exception 02 (ILLEGAL DATA ADDRESS) will be sent if:

- A read coil command, starting to an inexistent point in configuration, is received.
- A read holding command, starting to an inexistent point in configuration, is received.
- A force coil / multiple coils command, starting to an inexistent point in configuration, is received.
- A preset single / multiple register(s) command, referring to a starting inexistent point in configuration, is received.

If there is some "holes" (addresses not in configuration), these holes will be padded with 0 (i.e. value OFF).

C264 Computer:

For the C264 Computer, the exception 02 (ILLEGAL DATA ADDRESS) will be sent if:

- A read coil command, requesting for an inexistent point in configuration, is received.
- A read holding command, requesting for an inexistent point in configuration, is received.
- A force coil / multiple coils command, referring to an inexistent point in configuration, is received.
- A preset single / multiple register(s) command, referring to an inexistent point in configuration, is received.

If the starting address is in configuration and/or if there is some “holes” (addresses not in configuration), an error with code 02 (Illegal Data Address) is transmit."

Exception code 03 (ILLEGAL DATA VALUE)

Exception code 03 will be sent if:

- An illegal value is received in force coils request (so value different from FF00h and 0000h).
- An illegal count value for multiple preset registers is received. For example, if the function 16 has a count number greater than 1.
- An illegal count value for multiple forced coils is received. For example, if the function 15 has a count number greater than 1.

Exception code 07 (NEGATIVE ACKNOWLEDGE)

Exception code 07 will be sent if:

- A read coil / input status have more than 2000 points.
- A force coil is refused because the command is incorrect or cannot be executed (equipment absent, invalid, in local...).

2.5 Data sent to SCADA

2.5.1 Analogue Inputs

MODBUS function 3 or 4 can be used to poll the Analogue Inputs.

The Analogue Inputs are represented on the MODBUS mapping by one word (2 bytes) or two words (4 bytes).

Supported measurements formats:

C264	GTW	Format	Description
S	**S**	Precision [8..16]	8 bits or 16 bits
S	**S**	NATURAL	No transformation: on 8 or 16 bits
S	**S**	UNORMALIZED	Unsigned Normalized: unsigned scaled on 8 or 16 bits
S	**S**	SNORMALIZED	Signed Normalized: signed scaled on 8 or 16 bits
S	N	Float IEEE754 ‘Little Endian’	Float value on 32 bits ‘Little Endian’.
S	N	Float IEEE754 ‘Big Endian’	Float value on 32 bits ‘Big Endian’.

Signed normalized coding:

The **signed normalized coding** is used to encode the 16 bits-registers. Analogue maximal value will be coded 7FFFh [decimal value + 32767], and minimal value will be coded 8000h [decimal value –32768]. (See note 1)

Example: In configuration the maximal value for an analogue point is +3000 and minimum value for this analogue is 0.

That means that when the analogue is received with value 0 from the system, the gateway will send to the SCADA the register with 8000h value. If this analogue is equal to the maximal value +3000, the value sent to the SCADA is 7FFFh. Calculus is linear for the coding between the min and max values.

NOTE:

For this mode, the gateway may now code the value on 8 to 16 bits [low part of the register will be used]. But, 16 bits is normally the standard to use the full scale conversion.

Global formula is:

SCVal: Scaled value to be sent to SCADA

Val: Received value to be transmitted.

Vmax: Received value corresponding to MAX value.

Vmin: Received value corresponding to MIN value.

P is the precision, P= “8” or “16”: $MAX = 2^{(P-1)} - 1$, $MIN = -2^{(P-1)}$

$$SCVal = \frac{(MAX - MIN) * Val + MIN * Vmax - MAX * Vmin}{Vmax - Vmin}$$

Unsigned normalized coding:

The **unsigned normalized coding** is used to encode the 16 bits-registers. Analogue maximal value will be coded FFFFh [decimal value + 65535], and minimal value will be coded 0000h [decimal value 0]. (See note 1)

Example: In configuration the maximal value for an analogue point is +3000 and minimum value for this analogue is 0.

That means that when the analogue is received with value 0 from the system, the gateway will send to the SCADA the register with 0h value. If this analogue is equal to the maximal value +3000, the value sent to the SCADA is FFFFh. calculus is linear for the coding between the min and max values.

NOTE:

For this mode, the gateway may now code the value on 8 to 16 bits [low part of the register will be used]. But, 16 bits is normally the standard to use the full scale conversion.

Global formula is:

SCVal: Scaled value to be sent to SCADA

Val: Received value to be transmitted.

Vmax: Received value corresponding to MAX value.

Vmin: Received value corresponding to MIN value.

P is the precision, P= “8” or “16”: $MAX = 2^{P} - 1$, $MIN = 0$.

$$SCVal = \frac{MAX * Val - MAX * Vmin}{Vmax - Vmin}$$

Natural coding:

The **natural coding** is used to encode data without any calculation. That’s means that integer value will be send.

Example: if the gateway receives the value 10.xxxx, the value 0Ah will be set in the appropriate register. The gateway receives the value –10. xxxx the value FFF6h will be coded.

In the last example, the SCADA needs to know that FFF6h is value –10, and not 65525 decimal, by checking analogue min and max value for example.

2.5.2 Tap Position

MODBUS function 3 and 4 can be used to poll tap position.

Tap position are managed like Analogue inputs, see §2.5.1 “Analogue Inputs“for details.

2.5.3 Counters

MODBUS function 3 or 4 can be used to poll the counters (CT).

The counters are represented on the MODBUS mapping by one word (2 bytes) or two words (4 bytes).

One or more counters can be polled at a time.

Four counters formats are available:

C264	GTW	Format	Description
S	**S**	NATURAL	Natural: Unsigned value on 16 bits (between 0 and + 65535)
S	**S**	UNORMALIZED	Unsigned Normalized: values on 16 bits from 0 to (2 exp Accuracy)
S	**N**	Float IEEE754 'Little Endian'	Float value on 32 bits 'Little Endian'.
S	**N**	Float IEEE754 'Big Endian'	Float value on 32 bits 'Big Endian'.

For format details see §2.5.1 "Analogue Inputs".

2.5.4 Digital Inputs

MODBUS function 1 (read coil) or 2 (read status) can be used to poll the Digital Inputs.

- The Digital Inputs are represented on the MODBUS mapping by one bit for single DI.
- The Digital Inputs are represented on the MODBUS mapping by 1 or 2 bits for double DI.

C264	GTW	Mapping
S	**S**	1 bit
S	**N**	2 bits

Coils or Status Digital Inputs have no qualities and no time tags.

One or more Digital Inputs can be polled at a time. If the returned coil quantity is not a multiple of eight; the remaining bits in the final byte will be padded with zeros (toward the high order end of the byte). The Byte Count Field specifies the quantity of complete bytes of data.

Refer to *§2.4.2 "Error Management"* for exception management details.

2.5.5 Disturbance files

Disturbance files are not treated.

2.5.6 Sequence of Events File (SOE)

Transfer of Sequence of Events File is not supported by MODBUS Standard.

2.6 Data received from SCADA

2.6.1 Commands

C264	GTW	Function	Description
S	**S**	5	Force single coil.
N	**S**	15	Force multiple coil but Only one coil change is allowed.

MODBUS function 5 (FORCE SINGLE COIL) or 15 (FORCE MULTIPLE COILS) can be used to send Commands.

Single and double point's commands are managed by the computer.

Only one Command can be sent at a time i.e. using function 15 only one coil change is allowed.

Refer to *§2.4.2 "Error Management"* for exception management details.

2.6.2 Setpoints

MODBUS function 6 (PRESET SINGLE REGISTER) or 16 (PRESET MULTIPLE REGISTERS) can be used to reply to Setpoints SCADA's request.

- If SCADA uses function 6, only one Setpoint (Signed value on 16 bits) can be sent at a time.
- If SCADA uses function 16, a restriction allowed presetting only one Setpoint at the same time.

Refer to §2.4.2 "Error Management" for exception management details.

Supported setpoints formats:

C264	GTW	Format	Description
S	**S**	NATURAL	Signed value on 16 bits (between -32768 and + 32767) (no scaling is done).
S	**N**	Float IEEE754 'Little Endian'	Float value on 32 bits 'Little Endian'.
S	**N**	Float IEEE754 'Big Endian'	Float value on 32 bits 'Big Endian'.

2.7 Limits and Performance

The device address field of a message frame contains eight bits. Valid slave device addresses in queries are in the range of 0 to 247 (address 0 is reserved for broadcast operations).

Up to two Slave protocols can be configured on a PACiS MiCOM C264 computer.

Up to 6 Slave protocols can be configured on a PACiS GATEWAY

2.8 Protocol Configuration

PACiS Configuration tool permits to define:

- Network attributes
- DI attributes
- AI attributes
- DO attributes
- AO attributes

2.8.1 Network attributes

C264	GTW	Parameter	Parameter Choice	Values
S	**S**	Comm. interface	Serial port	Port number
N	**S**	parity		none/odd/even
N	**S**	Comm. interface	MODBUS TCP/IP	
N	**S**	TCP/IP address		X.X.X.X
N	**S**	IP port number		502 [1..65535]
S	**S**	link address		1 [1..255]
S	**N**	inter frame duration		3 [1..50] ms If a response consists of several frames, the second frame should be received or transmitted within this time (in mini-seconds).

2.8.2 Digital Inputs attributes

Double Points Status (DPS) and Single Points Status (SPS) are made available.

Multi Points Status (MPS) are also made available for transmission to SCADA on the PACIS Gateway.

DPS attributes:

C264	GTW	Parameter	Parameter Choice	Values
S	**N**	Double address usage		Yes / No
S	**S**	Mono addressing	Object address - register	1 [0..65535]
S	**N**	Double addressing	Open state address - register	1 [0..65535]
S	**N**	Double addressing	Closed state address - register	1 [0..65535]

SPS attributes:

C264	GTW	Parameter	Parameter Choice	Values
S	**S**	Object address - register		1 [0..65535]
N	**S**	Inversion	Object address - register	No / Yes

MPS attributes:

C264	GTW	Parameter	Parameter Choice	Values
N	**S**	State_0 to State_15 register address		1 [0..65535]

2.8.3 Analogue Inputs attributes

The protocol supports two different analogue input signals: Measurements values (MV) and counters (CT).

MV:

C264	GTW	Parameter	Parameter Choice	Values
S	**S**	Object address - register		1 [0..65535]
S	**S**	Format	Natural	
S	**S**	Format	Unsigned normalized	
S	**S**	Format	Signed normalized	
S	**N**	Format	Real IEEE754 - little endian	
S	**N**	Format	Real IEEE754 - big endian	
S	**S**	Precision		[8..16]
N	**S**	minimum value		
N	**S**	maximum value		

CT:

C264	GTW	Parameter	Parameter Choice	Values
S	**S**	Object address - register		1 [0..65535]
S	**S**	Format	Natural	
S	**S**	Format	Unsigned normalized	
S	**N**	Format	Real IEEE754 - little endian	
S	**N**	Format	Real IEEE754 - big endian	

2.8.4 Digital Outputs attributes

Double Points Control (DPC) and Single Points Control (SPC) are made available.

C264	GTW	Parameter	Parameter Choice	Values
S	**S**	Object address - register		1 [0..65535]

2.8.5 Analogue Outputs attributes

Setpoints are made available as analogue output attributes:

C264	GTW	Parameter	Parameter Choice	Values
S	**N**	Object address - register		1 [0..65535]
S	**N**	Format	Signed 16 bits	
S	**N**	Format	Real IEEE754 - little endian	
S	**N**	Format	Real IEEE754 - big endian	

Customer Care Centre

http://www.schneider-electric.com/CCC

Schneider Electric
35 rue Joseph Monier
92506 Rueil-Malmaison
FRANCE

Phone: +33 (0) 1 41 29 70 00
Fax: +33 (0) 1 41 29 71 00

www.schneider-electric.com

Publication: SPP/EN MODBUS/D10

Publishing: Schneider Electric
06/2013