

Telemecanique

Protocole Modbus Esclave

Modbus Slave Protocol

Instruction de service
Instruction sheet
Bedienungsanweisung
Istruzioni di servizio
Instrucción de servicio
04/2005



Telemecanique

Contents

- Safety Information _____ 29
- 1 - Minimum hardware and software requirements _____ 31
- 2 - Installing the protocol: Starting XBT L1000 _____ 31
- 3 - Operating principle _____ 31
- 4 - Content of the dialog table _____ 32
- 5 - Configuring the dialog table _____ 33
- 6 - Equipment symbols _____ 33
- 7 - Protocol parameters _____ 33
- 8 - Objects supported _____ 34
- 9 - Modbus Slave setup _____ 34
 - 9.1 - Addressing _____ 34
 - 9.2 - Cables _____ 35
 - 9.3 - DIAGRAMS _____ 35
- 10 - Bandwidth principle _____ 39
 - 10.1 - General operating principle _____ 39
 - 10.2 - Calculating bandwidth usage _____ 40
 - 10.3 - Tips _____ 44
- 11 - Diagnostics _____ 45
- 12 - Appendices _____ 46
 - 12.1 - Internal date and time _____ 46
 - 12.2 - Communication requests _____ 46
 - 12.3 - Calculating the Modbus Slave frame check (CRC) _____ 49

E
N
G
L
I
S
H

E
N
G
L
I
S
H

Safety Information

E
N
G
L
I
S
H

Important Information

NOTICE


Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.





The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

	DANGER
DANGER indicates an imminently hazardous situation, which, if not avoided, will result in death, serious injury, or equipment damage.	

	WARNING
WARNING indicates a potentially hazardous situation, which, if not avoided, can result in death, serious injury, or equipment damage.	

	CAUTION
CAUTION indicates a potentially hazardous situation, which, if not avoided, can result in injury or equipment damage.	

PLEASE NOTE

Electrical equipment should be serviced only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. This document is not intended as an instruction manual for untrained persons.

© 2005 Schneider Electric. All Rights Reserved.

E
N
G
L
I
S
H

1 - Minimum hardware and software requirements

The Modbus Slave protocol is available only on XBT N401(1)(2), XBT N410(2) and XBT R411 terminals, running version 4.40 or later of the XBT L1000 software.

2 - Installing the protocol: Starting XBT L1000

Two scenarios:

- The "Install Protocol" dialog box opens automatically.
- If a protocol has already been installed, you can update the previous version or install another protocol. Close all open applications in XBT L1000 then select the File/Install Protocol menu.

3 - Operating principle




The XBT is totally passive with respect to communication. The PLC reads or writes the data in the XBT memory. If the PLC does not send any data to the XBT (or does not attempt to read from the XBT memory), the values are not refreshed. After expiration of the communication time-out, if it has been configured, the values are replaced by "?" characters and a "Connecting..." system message appears. To avoid configuring the time-out, the value 0 should be entered for this parameter.

When the user presses a key, if the "Function key status" word has not been read by the PLC, the LED associated with the key flashes rapidly and pressing the key again has no effect. Once the word has been read by the PLC, the LED stops flashing and the key can be used again.

In Modbus Slave mode, the XBT terminal does not read/write PLC variables.

4 - Content of the dialog table

No.	FUNCTION	Function XBT N401(1)	Input XBT N401(2)	Input XBT N410(2)	XBT R411
1	Image of static function keys				
2	Image of system keys				
3	Image of numeric keys				
4	Communication control				
5	Set PLC clock				
6	No. of displayed page				
7	No. of last field entered				
22	No. of last alarm acknowledged				
8	Report				
9	Log filling rate				
24	Graphs plotting performed				
30	Checksum application				
31	Terminal advanced state				
32	Last recipe transferred				
10	No. of page to be processed				
11	No. of field to be entered				
12	Print command				
33	No. of recipe to be transferred				
25	Draw graph activation				
13	Write table authorization				
26	Recipe transfer not allowed				
14	Clear log/Advanced functions				
15	LED control				
16	Image of static function keys				
17	Image of system keys				
18	Image of numeric keys				
34	Communication control				
19	Set PLC clock				
20	No. of displayed page				
21	No. of last field entered				

	: Functions selected by default
	: Other available functions
	: Not available

5 - Configuring the dialog table

- Select Configuration/Dialog Table.
- Enter the table start address and the scan time.
- Construct the table by adding or deleting the functions required by your application.

Note Refer to the user’s manual for XBT N/XBT R Magelis for more detailed information about dialog table content.

6 - Equipment symbols

Since the XBT terminal is totally passive, the Modbus Slave protocol does not require equipment symbols to be declared.

7 - Protocol parameters

Select Protocol Parameters from the XBT L1000 Configuration menu (see table below).

Refer to the PLC user’s manual for details of how to configure the Modbus Slave protocol.

	RTU (8 bits)
Coding system	8-bit binary code
Number of bits per character	
- Start bit	1
- Number of data bits	8
- Parity bit	even/odd/none
- Stop bit *	1
- Speed (baud)	600/1200/2400/4800/9600/19200
Message structure	
- Message	Modbus frame
- Check	CRC 16
- End of frame	Silence for 3.5 characters
Interface types	RS485
Timeout (s)	0 s to 120 s
Slave number	Terminal address (1 to 30) Value at 0 = broadcasting Value at 31 = disconnection

(*) The configuration 'No parity + 1' stop bit is possible, without being though in conformity with the Modbus standard.

8 - Objects supported

The addressable XBT internal memory is limited to 300 words, of address 0 to 299.

	Mnemonic (syntax)	Mnemonic identifiers
Word bit	% MWi:Xj	i: (0...299) j: (0...F)
Word	% MWi	i: (0...299)
Double word	% MDi	i: (0...298)
Floating point	% MFi	i: (0...298)
String	% CHi	i: (0...299)

E
N
G
L
I
S
H

9 - Modbus Slave setup

9-1 Addressing

With the Modbus Slave protocol, the terminal behaves like a slave. It therefore answers an address between 0 and 30.

The value 0 is reserved for broadcasting. Messages sent to address 0 will be received by all equipment connected to the bus. This can be used to send identical data to all the equipment, instead of sending a message to each item of equipment.

The value 31 is synonymous with disconnection for the terminal. A terminal detects an address 31 when no cable is connected to it. For this reason, any terminal configured with this address believes itself to be disconnected and displays messages requesting reconnection.

Several types of connection are offered:

- Using an XBT Z968 cable (straight) or XBT Z9680 cable (angled): the address of the terminal is hard-wired and is worth 4
- Using an XBT Z938 cable: The terminal address is configured in the software
- Using an XBT Z908 cable and an SCA62 box: The address is "hard-wired" using the jumpers on the SCA62 box (the address will be between 1 and 30).

9-2 Cables

	Connected device	Physical link	Reference
XBT N401/N410 XBT R411	Twido	RS485	XBT Z968 (straight) (SUBD25 <-> MiniDin) XBT Z9680 (angled) (SUBD25 <-> MiniDin)
	Micro		
	Premium		
	Nano		
	SCA62		XBT Z908 (SUBD25 <-> SCA62 box)
	LU9GC3	XBT Z938 (SUBD25 <-> RJ45)	
	Quantum	RS232C	XBT Z9710 (SUBD25 <-> SUBD9)
	Momentum		XBT Z9711 (SUBD25 <-> RJ45)

ENGLISH

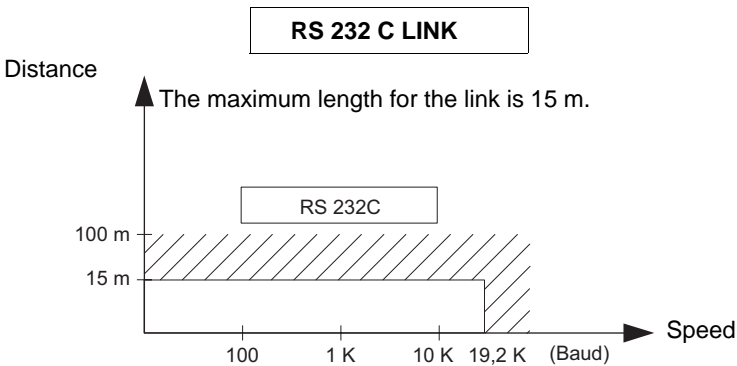
⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

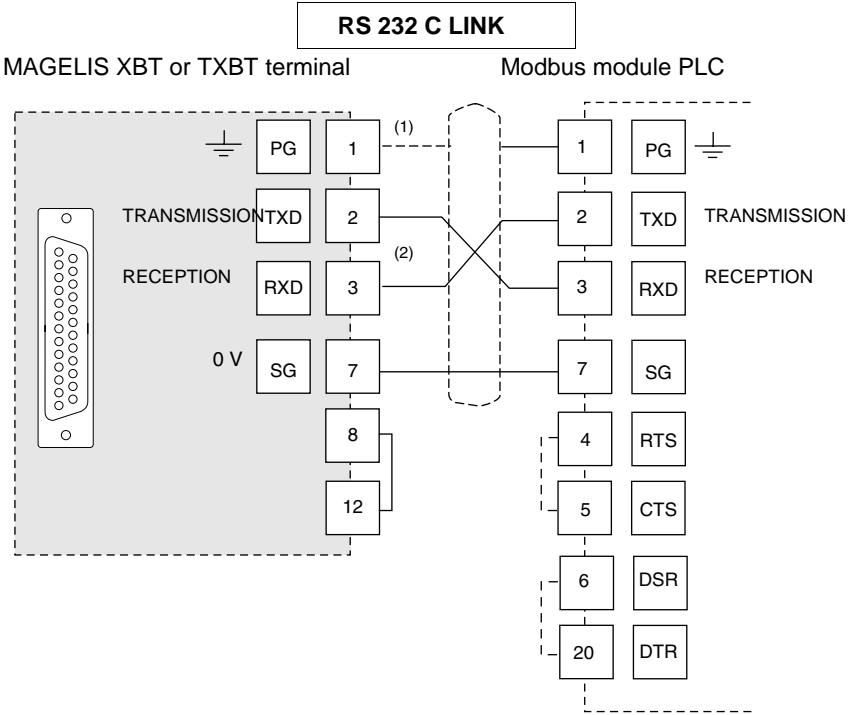
For XBT N, power-on the product before starting the master of the bus.

Failure to follow this instruction can result in death, serious injury or equipment damage.

9-3 DIAGRAMS



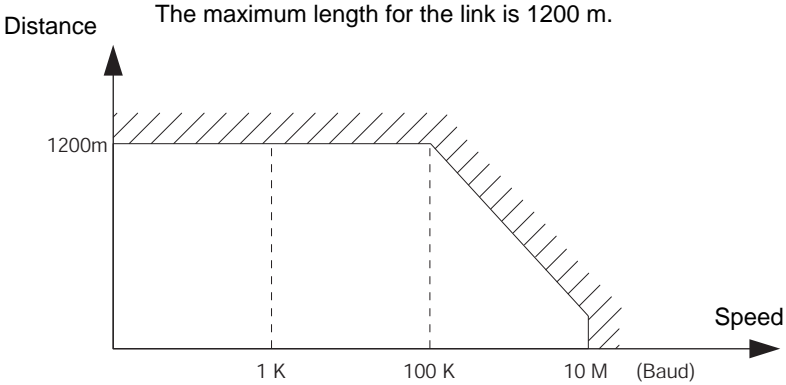
Wiring = 3 shielded wires with a minimum cross-section of 0.6 mm² (AWG22)



- (1) Connection of the shielding at both ends depends on any electrical restrictions affecting the installation.
- (2) In some configurations, it is not necessary to invert pins 2 and 3. Please refer to the documentation for the PLC being used.

RS 485 LINK

(1)



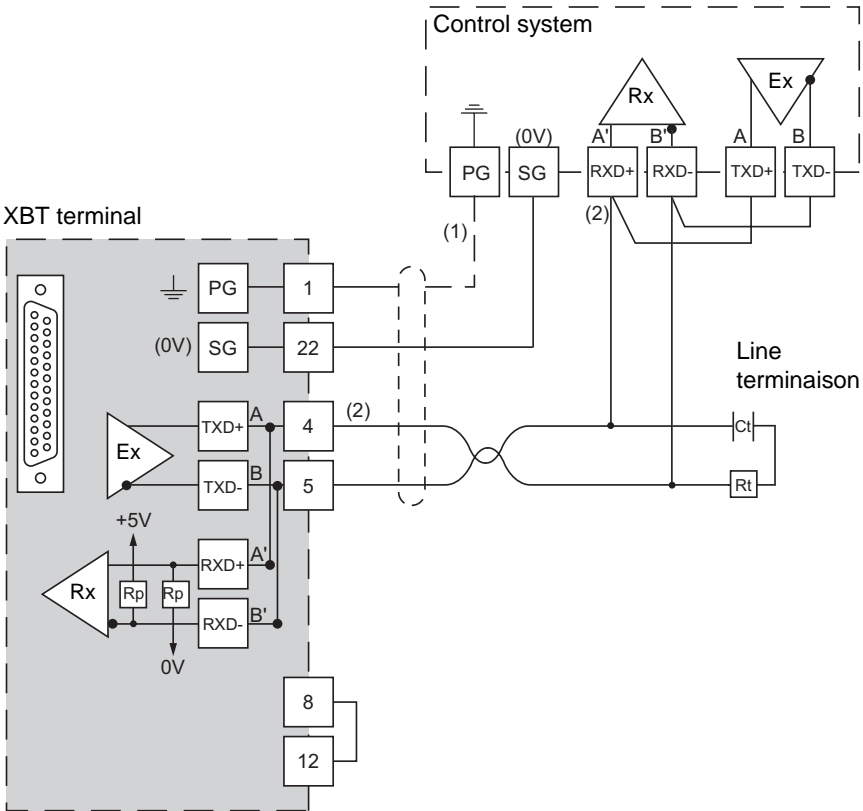
Wiring = 2 shielded twisted wires with a minimum cross-section of 0.6 mm² (AWG22)
and one 0 V wire

E
N
G
L
I
S
H

(1) THE MAXIMUM LENGTH INCLUDING THE RS 485 LINK IS 1200 M, PROVIDED THAT THE EQUIPMENT CONNECTED TO THE XBT TERMINAL IS NOT SUBJECT TO MORE STRINGENT RESTRICTIONS. (REFER TO CONNECTED DEVICES INSTRUCTION SHEET)

ENGLISH

RS 485 LINK



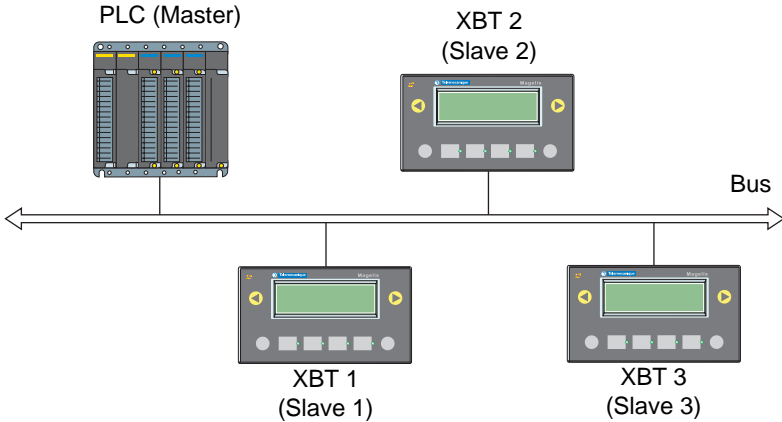
- (1) Connection of the shielding at both ends depends on any electrical restrictions affecting the installation.
- (2) Rt: Line impedance resistor (typically 110 Ω). It is recommended to install the line impedance resistor with a RC circuit ($R = 120 \Omega / 0,25 \text{ W}$ and $C = 1\text{nF} / 10 \text{ V min}$). Make sure that only one line impedance resistor is installed.

Note RP resistors are integrated into the XBT and feature 4,7 kΩ for XBT N and 100 kΩ for XBT R.

10 - Bandwidth principle

10-1 General operating principle

The Modbus Slave protocol operates in point-to-point or multidrop mode. The PLC is connected to one or more terminals.

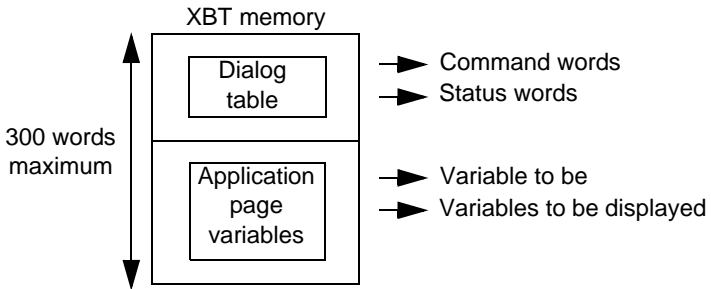


ENGLISH

Data exchanges between the terminals and the PLC are made in data-transmission cycles, during which the PLC will read and write to the XBT memory (for example, a PLC can read the values every 300 ms in the display-unit memory).

The PLC will carry out the following operations:

- Writing in the dialog table (command words)
- Reading words from the dialog table (status words)
- Writing variables (display variables)
- Reading variables (variables entered by the user)



Each request transmission by the PLC results in a certain level of bandwidth usage. Therefore, before a communication architecture can be set up, the rate of bandwidth usage must be calculated to prevent the possibility of saturation.

General reminders

- For a transmission speed of 19200 baud, the transmission time for a word is approximately 1 ms.
- A PLC sending a write request to a terminal requires:
 - 9 bytes for sending
 - 8 bytes for acknowledgment
 i.e., 17 bytes (see section a) Writing of n words initiated by the master, page 46).

- A PLC sending a read request to a terminal requires:
 - 8 bytes for sending
 - 5 bytes for acknowledgment
 i.e., 13 bytes (see section c) Reading of n output or internal words initiated by the master, page 47).

One word = 2 bytes. Therefore, for example, sending one write word requires:
17 + 2 = 19 bytes

ENGLISH

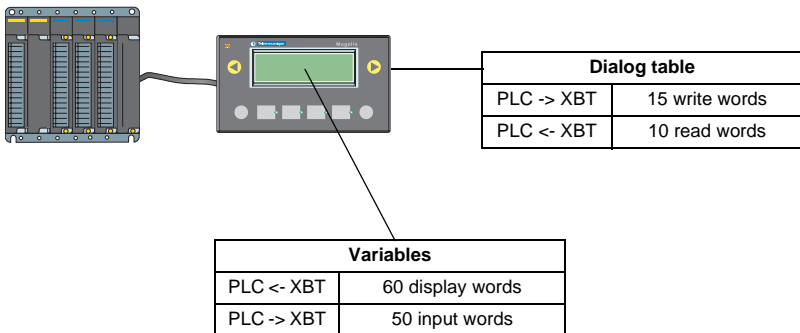
10-2 Calculating bandwidth usage

The bandwidth specifies the quantity of data, which can circulate on the network per second. This depends on several parameters, such as the transmission speed and the number of items of equipment connected to the network. To find out how much of the bandwidth is used, calculate the time it takes to send the data during each cycle. To do this, convert the data rate (in bps) into the time during which the bandwidth is occupied.

Example of calculating bandwidth usage in point-to-point mode

Hypothesis:

Say a terminal is connected to a PLC in point-to-point mode.



The **dialog table** contains 25 words, with a cycle of 300 ms (terminal default value).

Write request:	15 words	PLC -> XBT
Read request:	10 words	PLC <- XBT

Writing and displaying variables: 60 words refreshed every 300 ms. Of these 60 words, 50 can be modified by the PLC.

Display:	60 words	PLC <- XBT
Write:	50 words	PLC -> XBT

Calculating how much of the bandwidth is used by the dialog table

We will apply the following formula: *No. of word bytes + send bytes + acknowledgment bytes*

Say in our example:

$30 + 9 + 8 = 47$ i.e., **47 bytes** for the write request

$20 + 8 + 5 = 33$ i.e., **33 bytes** for the read request

A word is assumed to be sent in 1 ms (at a speed of 19200 baud). Knowing that one word = 2 bytes, we get:

$(47 + 33)/2 = 40$ i.e., a transmission time of approximately **40 ms** for the dialog table.



The dialog table will therefore consume approximately 13% of the bandwidth.

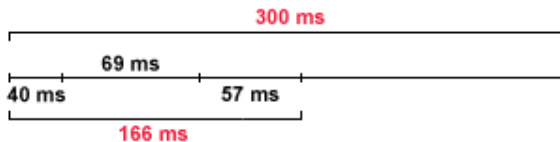
Calculating how much of the bandwidth is used by the variables

To display the terminal variables, we will have bandwidth usage of:

$60 \text{ words} = 120 \text{ bytes} + 9 \text{ bytes} + 8 \text{ bytes} = 137 \text{ bytes}$ i.e., a transmission time of approximately: **69 ms**

To write the terminal variables, we will have bandwidth usage of:

$50 \text{ words} = 100 \text{ bytes} + 8 \text{ bytes} + 5 \text{ bytes} = 113 \text{ bytes}$ i.e., a transmission time of approximately: **57 ms**

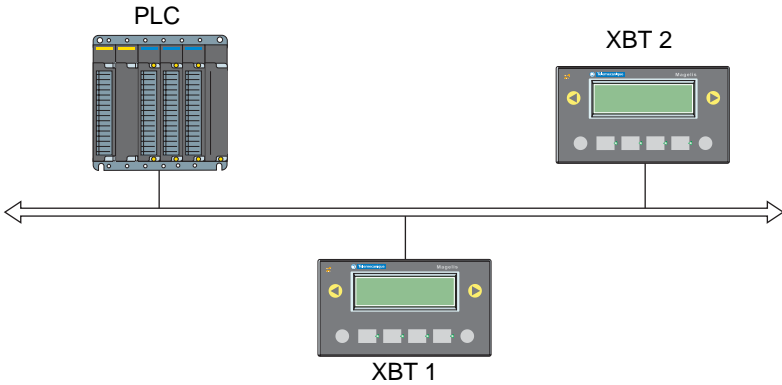


We will have a total consumption of **166 ms** (40 + 69 + 57) of the bandwidth 300 ms (i.e., approximately **55%** of the bandwidth).

At a speed of 9600 baud, the bandwidth consumption will double. Consumption will therefore be **332 ms** rather than **166 ms**. The bandwidth is then saturated (**332 ms** for **300 ms** maximum).

Example of calculating bandwidth usage in multidrop mode

We want to set up an architecture comprising one PLC and two terminals.



The two **dialog tables** are made up as follows:

First dialog table (XBT 1)

- Write request:** 5 words PLC -> XBT
- Read request:** 5 words PLC <- XBT

Second dialog table (XBT 2)

- Write request:** 10 words PLC -> XBT
- Read request:** 10 words PLC <- XBT

Writing and displaying variables with the XBT 1 terminal: 10 words refreshed every 300 ms. Of these 10 words, 5 can be modified by the PLC.

Variables (XBT 1)

- Display:** 10 words PLC <- XBT
- Write:** 5 words PLC -> XBT

ENGLISH

Writing and displaying variables with the XBT 2 terminal: 30 words refreshed every 300 ms. Of these 30 words, 20 can be modified by the PLC.

Variables (XBT 2)

Display: 30 words PLC <- XBT

Write: 20 words PLC -> XBT

Calculating how much of the bandwidth is used by the dialog tables

XBT 1 terminal dialog table

$(10 + 9 + 8) + (10 + 8 + 5) = 50$ bytes

The transmission time will be approximately 25 ms for this dialog table.

XBT 2 terminal dialog table

$(20 + 9 + 8) + (20 + 8 + 5) = 70$ bytes

The transmission time will be approximately 35 ms for this dialog table.

Calculating how much of the bandwidth is used by the variables

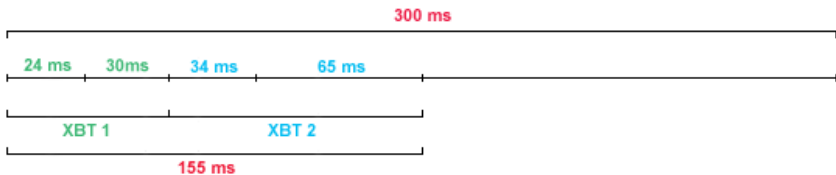
XBT 1 terminal variables (display and write)

$(20 + 9 + 8) + (10 + 8 + 5) = 60$ bytes i.e., a transmission time of approximately 30 ms.

XBT 2 terminal variables (display and write)

$(60 + 9 + 8) + (40 + 8 + 5) = 130$ bytes i.e., a transmission time of approximately 65 ms.

The bandwidth consumption can be represented as follows:



We have a total consumption of 155 ms (25 +35 + 30 + 65) of the bandwidth 300 ms (i.e., approximately 52% of the bandwidth).

As in the example in point-to-point mode, we see that if we reduce the speed to 9600 baud, the bandwidth is saturated (310 ms for 300 ms maximum).

10-3 Tips

The previous examples demonstrate that:

- The more terminals are added, the less bandwidth remains
- The more values there are to display, the higher the bandwidth consumption by the read operation

There are therefore a number of possibilities for freeing up the bandwidth:

- Increase the transmission speed (depends on the quality of the network and the connected equipment)
- Reduce the number of words in the dialog table
- Reduce the number of words needing to be read or written by the PLC
- Reduce the refresh speed for the display
- Reduce the cycle speed of the dialog table

11 - Diagnostics

Behavior in the event of an error

- Display of "??????..." in the event of a transmission error: format/parity/CRC/no response or exception response
- **CPT 1:** Counter for messages received by the terminal, whether or not they are relevant.
- **CPT 2:** Counter for messages received with a CRC error.
- **CPT 3:** Counter for error messages returned by the terminal.
- **CPT 4:** Counter for correct messages received by the terminal.
- **CPT 5:** Counter for distribution messages received by the terminal.
- **CPT 6:** Always at 0.
- **CPT 7:** Counter for messages not processed because the terminal was busy.
- **CPT 8:** Counter for messages received with parity errors, format errors, etc.

NOTE For modules:

- **Which are not 100% Modbus-compatible**
 - **Which do not accept 125 write words and 123 read words**
- it is essential that the length of pages of consecutive words does not exceed that accepted by the module on your PLC.**

Examples: Telemecanique SCM22 accepts a maximum of 120 words,
Telemecanique SCG116 accepts a maximum of 14 words.

12 - Appendices

12-1 Internal date and time

In order to access the date and time in the terminals, it is possible to define alphanumeric fields addressed on internal variables in XBT L1000.

XBT N/R display unit

XBT device
% MWi type variable
Symbol: Date - ASCII, i = 50000, Time - ASCII, i = 50001
Format type: String
Length: 8 or 10
Format: ASCII

E
N
G
L
I
S
H

12-2 Communication requests

The function code is in hexadecimal format.

a) Writing of n words initiated by the master

Request from master

Slave no.	Function code 10	Address of 1st word		Number of words		Number of bytes	Value of words to be written	Check
		Hi	Lo	Hi	Lo			
1 byte	1 byte	2 bytes		2 bytes		1 byte	n bytes	2 bytes

- Address of 1st word: Same addressing field as for the read request
- Number of words: [see note, page 45](#)
- Number of bytes: Twice the number of words
- Value of words to be written: 'H'0000' to 'H'FFFF'

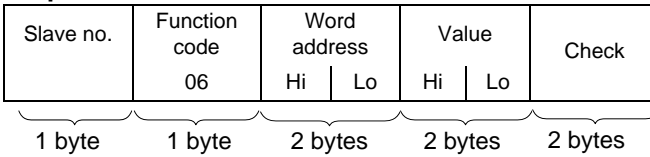
Response from slave

Slave no.	Function code 10	Address of 1st word written		Number of words written		Check
		Hi	Lo	Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		2 bytes

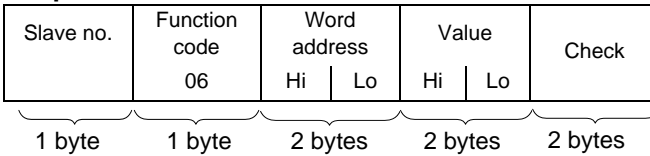
- Slave no: Same as request
- Address of first word written: Same as request
- Number of words written: Same as request

b) Writing of 1 output or internal word initiated by the master

Request from master

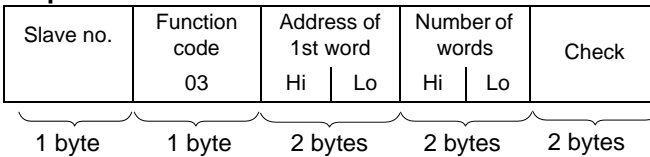


Response from slave



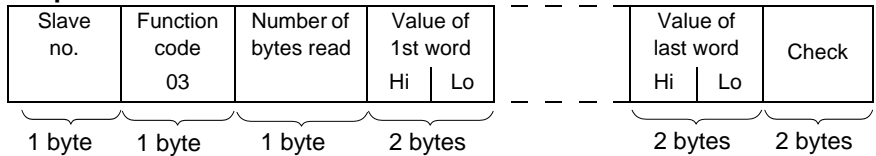
c) Reading of n output or internal words initiated by the master

Request from master



- Address of first word: corresponds to the address of the first word to be read in the slave.
- Number of words: [see note, page 45](#)

Response from slave



- Slave no: Same as request
- Number of bytes read: Twice the number of words read, then one word is on two bytes.
- Value of words read: H'0000' to H'FFFF'

d) Reading and resetting counters initiated by the master

Question

Slave no.	Function code 08	Sub-function 00xx	Data (d) 0000	Check	
1 byte	1 byte	2 bytes		2 bytes	

- One sub-function code for each function
 - Reading counter 1: 0x000B
 - Reading counter 2: 0x000C
 - ...
 - Reading counter 8: 0x0012
 - Counter reset : 0x000A

Response

Slave no.	Function code 08	Sub-function 00xx	Data (d)	Check	
1 byte	1 byte	2 bytes		2 bytes	

e) Functions supported

		Sub-function		Type of functions
Hex	Dec	Hex	Dec	
03	03	-	-	Reading of n output or internal words initiated by the master
06	06	-	-	Writing 1 output or internal word
08	08	00xx	00xx	Reading and resetting counters initiated by the master
10	16	-	-	Writing of n words initiated by the master
2B	43	0E	14	Read Device Identification

ENGLISH

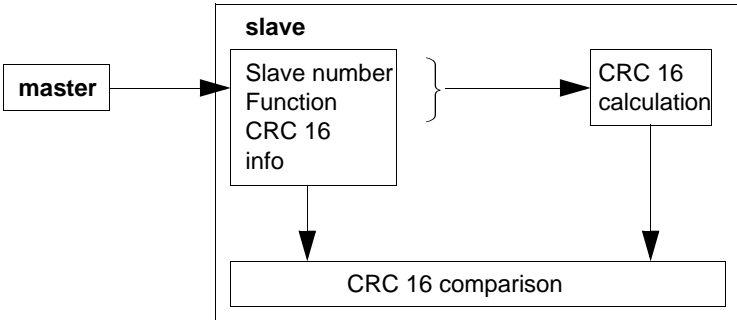
12-3 Calculating the Modbus Slave frame check (CRC)

When the master sends a request having indicated:

- The slave number
- The function code
- The function parameters

It calculates the CRC and sends it as a control word (CRC 16).

When the slave receives the request message, it stores it, calculates the CRC and compares it to the CRC 16 received.



ENGLISH

If the message received is incorrect (CRC 16s do not match), the slave does not respond.

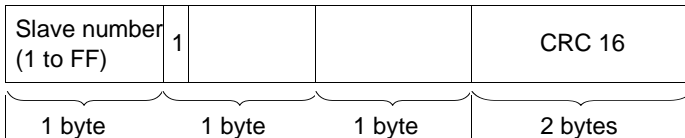
If the message received is correct but the slave cannot process it (incorrect address, incorrect data, etc.), it returns an exception response.

Content of an exception response

Exception code

1. Unknown function code*
2. Incorrect address*
3. Incorrect data error*
4. PLC not ready
5. Acknowledgment
7. Non-acknowledgment
8. Write error
9. Zone overlap

Function code received and most significant bit at 1



Example

request:

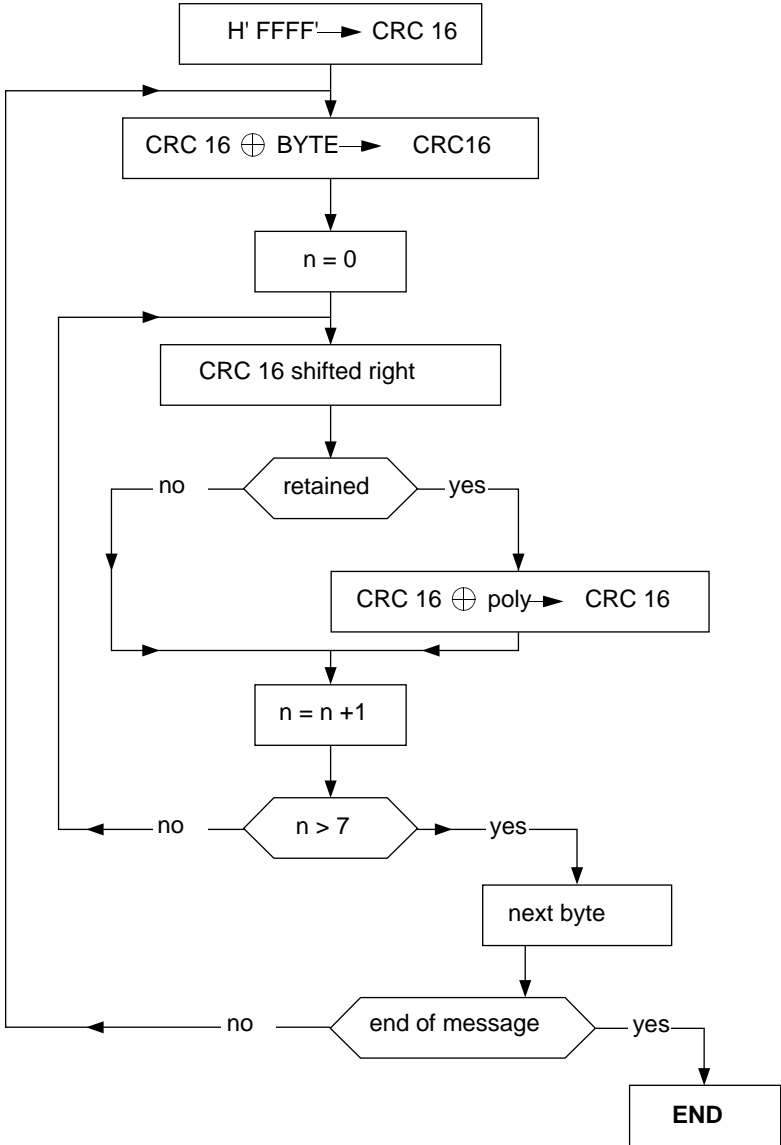
1	9	0	0	0	0	CRC 16
---	---	---	---	---	---	--------

response:

1	89 _H	1	CRC 16
---	-----------------	---	--------

(*) The slave XBT manages these codes only.

Algorithm for calculating CRC 16



⊕ = exclusive OR

n = number of information bits

poly = polynomial for calculating CRC 16 = 1010 0000 0000 0001
(generating polynomial = 1 + X² + X¹⁵ + X¹⁶).

In CRC 16, the 1st byte sent is the least significant byte.

ENGLISH

NOTES:

E
N
G
L
I
S
H

