MV Network Control
Flair 200C

MODBUS Communication
User Manual

Merlin Gerin
Modicon
Square D
Telemecanique

Schneider Electric

Contents

General

Introduction

The FLAIR 200C communication board allows the connection of MV/LV substation to a telecontrol system by using a MODBUS protocol . It includes advanced telecommunication function and manages PSTN type of transmission modems.

Application

Permanent and non permanent serial link with a telecontrol center by using MODBUS protocol.

Advantages

- type of transmission modem : RS232, GSM
- Advanced telecommunication functions
- Configuration by PC computer
- Built-in protocol analyser

Functions

Report by exception

Each alarm may be configured to be sent spontaneously to the telecontrol centre when it changes of state.
The modem is activated through HAYES frames and after PSTN link is established with the telecontrol centre, a MODBUS protocol is initiated.

Protocol analyser

The communication board includes a protocol analyser functionality (including a MODBUS frame translation) available from the PC computer connected to the communication board
This analyser allows the display of the frames which are exchanged with the telecontrol system.

Events

The communication board memorises up to the last 150 events. Each change of states is time tagged with an accuracy of 20ms.

General

Accessible data

■ **Writing of digital data**

- ❑ Transmission of 2 remote control commands relay.

■ **Reading of digital data**

- ❑ Phase and earth fault currents of the way
- ❑ Voltage absence and presence
- ❑ Equipement fault

■ **Reading of measurements**

- ❑ Voltage
- ❑ Currents : phases and earth
- ❑ Power (P, Q, S)
- ❑ Power factor
- ❑ Energy

■ **Diagnostic**

- ❑ Reading of diagnostic counters.

■ Parameter setting

- ❑ Communication
- ❑ Measurements
- ❑ Fault passage indicator

■ **others functions**

- ❑ Time synchronisation
- ❑ Identification / configuration

Characteristics

type of transmission	asynchronous serial
protocol	MODBUS slave
speed	300, 600, 1200, 2400, 4800, 9600, 19200 bauds
data format	1 start bit, 8 data bits with no parity, 1 stop bit
electrical interface	RS232 or GSM Module
type of connector	9 pin SUB-D, female
W amount on a line	4080

MODBUS data addresses and encoding

General

Addressing

A MODBUS master can access 255 storage spaces of 64K words (255 MODBUS addresses).

Transmission

■ asynchronous, 300 to 19200 bauds

■ 1 start bit, 8 data bits, 1 stop bit, no parity

■ maximum response time < 30ms.

Reply messages

■ Upon receipt of a request recognized by the equipment (read or write), transmission of the data corresponding to the MODBUS specifications.

■ Upon receipt of a request not recognized by the equipment, transmission of an exception message (type 1, 2 or 3 only).

Read zone

■ The number of words read may not exceed the size of the checked zone.

■ Some zones may only be accessed as a whole.

Remarks

■ The bit by bit write and read functions are not used in the FLAIR 200C application.

■ Values followed by the letter "h" are in hexadecimal form (e.g. 0003h).

■ In the charts describing the data exchanged between the master and the FLAIR 200C, the hatched strips in the "authorized function" columns indicate the zones that are accessible as a whole.

Terminology

■ TCD: remote control (encoded in 2 bits)

■ TSD: two-state remote indication (encoded in 2 bits)

■ TSS: single-state remote indication (encoded in 1 bit)

■ TM: telemetering (encoded in 16 bits or 32 bits)

MODBUS data addresses and encoding

Identification / configuration zone

	word address 0000h to 0001h	access mode	authorized function
Software version	0000h	read	3,4
Status	0001h	read/write	3,4,6

■ **Bit 0 to 7 of status indicates the type of the equipment.** (read only)

=94 decimal (5Eh) for FLAIR 200C Modbus

■ **Bit 15 of status indicates:**

- 0 = No events loss
- 1 = Loss of events

When the pile of event is full, the oldest event is crushed and the bit "loss event" is put at one.

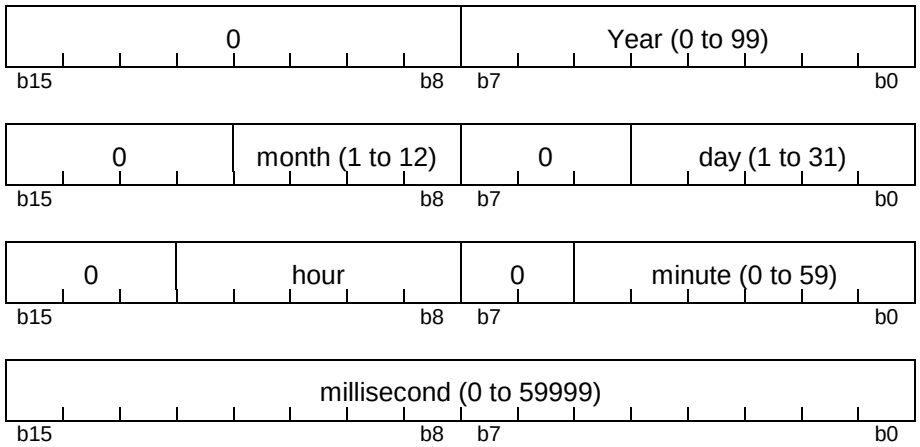
When all the pile of event is read, the bit "loss event " will be given has zero. This change of state will not cause event.

Time synchronization zone

This zone contains the internal date and time of the equipment for time-stamping of events.

The zone may only be read or written as a whole.

Binary date	word address 0002h to 0005h	access mode	authorized function
Year	0002h	read/write	3,4,16
month+day	0003h	read/write	3,4
Hours+minutes	0004h	read/write	3,4
milliseconds	0005h	read/write	3,4



MODBUS data addresses and encoding

Test zone

The test zone contains 9 words that can be read or written. It is recorded in saved RAM and is available to users to facilitate final adjustment tests.

The contents of the zone do not have any effect on the FLAIR 200C functions.

Test zone	word address	access mode	authorized function
9 words	0006h to 000Eh	read/write	1,2,3,4,5,6,16

Event zone

This zone contains the time stamp events.

Event zone	word address	access mode	authorized function
exchange word	000Fh	read/write	3,4,6,16
event 1	0010h to 0017h	read	3,4
event 2	0018h to 001Fh	read	3,4
event 3	0020h to 0027h	read	3,4
event 4	0028h to 002Fh	read	3,4

Only the exchange word may be written.
It is possible to read the exchange zone as a whole or the exchange word only.

The exchange word is used to manage a specific protocol to be sure not to lose events as a result of a MODBUS communication problem; the event table is numbered for that purpose.

The exchange word comprises 2 bytes:

- Most significant byte = exchange number which identifies each event frame. It is preset to zero when the FLAIR 200C is switched on; when it reaches its maximum value (FFh), it automatically goes back to 0. The FLAIR 200C numbers the exchanges and the master acknowledges the numbering.

- Least significant byte = number of valid events in the event zone (maximum 4).

Encoding of events

Each event is encoded with 4 words related to the event, followed by 4 words containing the event time-stamping data:

■ word 1: 0800h /2048

■ word 2: event bit address

□ 001Fh /31:
Event loss bit (set only on appearance)

□ 0310h to 031Fh: TSD 1 to 8

□ 0320h to 032Fh : code CR

□ 0330h to 034Fh : TSS 1 to 32

■ word 3: 0

■ word 4:
downward face = 0000h/0
rising face = 0001h/1

■ words 5 to 8: time-stamping with same format as date zone.

Acknowledgment of events

To inform the FLAIR 200C that it has correctly received the frame it has read, the master must :

☐ write the number of the last exchange it has received in the "exchange number" byte

☐ reset the "number of events" byte of the exchange word to zero.

After acknowledgment, the FLAIR 200C erases the events that have already been transmitted and replaces them by new ones when applicable.

Remark: until the exchange word written by the master becomes "X,0" (with X = number of the previous exchange that the master wishes to acknowledge), the exchange word in the table remains at "X, number of previous events".

If the number is equal to zero, the master is not required to acknowledge a message with no event.

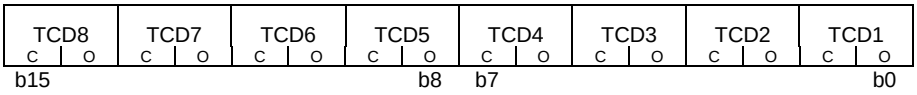
MODBUS data addresses and encoding

TC / TSD / TSS zone

TCD / TSD / TSS	word adddress	access mode	function authorized
TCD 1-8	0030h	write	1,2,3,4,5,6
TSD 1-8	0031h	read	1,2,3,4
CR	0032h	read	1,2,3,4,5,6
TSS 1-16	0033h	read	1,2,3,4
TSS 17- 32	0034h	read	1,2,3,4

Each TCD word is encoded as follows:

TCD	Single remote indications	Word bit
1	Digital output n°1	30h 0-1
2	Digital output n°2	30h 2-3
3	Preset NRJ	30h 4-5
4	Reset FPI	30h 6-7



A remote control TCD is encoded in 2 bits:

- 01 = open order
- 10 = closing order

The TCDs are assigned as follows:

- TCD 1 and 2 : digital ouput 1 and 2.

- TCD 3: Loading of the meter Energy with the value preset energy (32 Bits) by closing order.

- TCD 4: Reset Fault passage indicator by close order

Remote control orders are performed by writing a TCD word. Only one remote control order at a time may be requested.

The control order zone (TCD) may be read with bit and word read function code. As it contains no information the data is 0.

The CR code (result code) gives information on the processing of the remote control order carried out by the FLAIR 200C:

- bit 0: Remote control in progress.

- bit 1: Fault concerning the initial remote control order

- bit 2: Serious fault detected during internal check.

- bit 3: not used

- bit 4: not used.

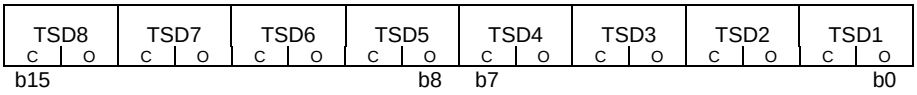
- bit 5: Failure to execute for an unknown reason.

Each change of state of one of this bit will produce a MODBUS event.

The telecontrol center system may reset this codes by writing a 0 to the relevant address.

MODBUS data addresses and encoding

Each TSD word is encoded as follows:



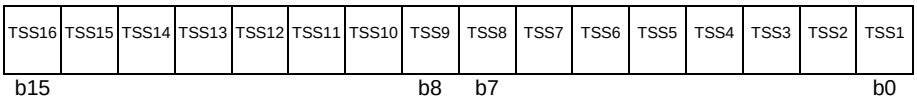
A TSD is encoded in 2 bits, F,O

- 01 = open.
- 10 = closed.
- 00 or 11 = undetermined.

The assignment of the TSD is as follows:

- TSD1: Digital ouput 1
- TSD2: Digital ouput 2
- TSD3: Preset NRJ (always to 01)
- TSD4: Reset FPI (always to 01)

Each TSS word is encoded as follows:



Single remote indications		Word bit	Single remote indications		Word bit
TSS1 :	Digital input 1.	33h 0	TSS17	Reserved	34h 0
TSS2 :	Digital input 2.	33h 1	TSS18 :	Reserved	34h 1
TSS3 :	Digital input 3.	33h 2	TSS19 :	Reserved	34h 2
TSS4 :	Digital input 4.	33h 3	TSS20 :	Reserved	34h 3
TSS5 :	Digital input 5.	33h 4	TSS21 :	Reserved	34h 4
TSS6 :	Digital input 6.	33h 5	TSS22 :	Reserved	34h 5
TSS7 :	Reserved	33h 6	TSS23 :	Earth fault	34h 6
TSS8 :	Reserved	33h 7	TSS24 :	Fug. Earth fault	34h 7
TSS9 :	Reserved	33h 8	TSS25 :	AC supply off phase 1	34h 8
TSS10 :	Reserved	33h 9	TSS26 :	Reserved	34h 9
TSS11 :	Flair 200C Fault	33h10	TSS27:	Reserved	34h10
TSS12 :	Local configuration	33h11	TSS28:	Reserved	34h11
TSS13 :	Remote configuration	33h12	TSS29:	Phase fault	34h12
TSS14 :	Configuration in progress	33h13	TSS30 :	Fast. Phase fault	34h13
TSS15 :	Configuration fault	33h14	TSS31 :	Reserved	34h14
TSS16:	Reserved	33h15	TSS32 :	Reserved	34h15

MODBUS data addresses and encoding

Telemetering zone

TM 16 bits	Units	Word address		function	
		Hexa.	decimal	mode	authorized
Phase current I1	0.1 A	0040h	64	read	3,4
Phase current I2	0.1 A	0041h	65	read	3,4
Phase current I3	0.1 A	0042h	66	read	3,4
Current I0	0.1 A	0043h	67	read	3,4
Imoyen	0.1 A	0044h	68	read	3,4
Power factory	0.001	0045h	69	read	3,4
Frequency	0.01 Hz	0046h	70	read	3,4
Reserved	-	0047h to 004Fh	71 to 79	read	3,4
TM 32 bits	Units	Word address		function	
		Hexa.	decimal	Mode	authorized
V1	0.1 V	0050h-1	80 to 81	read	3,4
P	10 W	0052h-3	82 to 83	read	3,4
Q	10 VAR	0054h-5	84 to 85	read	3,4
S	10 VA	0056h-7	86 to 87	read	3,4
NRJ	KWh	0058h-9	88 to 89	read	3,4
Reserved	-	005Ah to 005Fh	88 to 95	read	3,4

Each TM 16 bits value is a signed value encoded in 2's complement 16-bit word.
Each TM 32 bits value is a signed value encoded in 2's complement 32-bit word (LSB then MSB)

invalid or non-declared measurements are encoded with the value 8000h (-32768) (80000000h for 32-bits)

Remote parameters zone

16 parameters	Word address		access mode	function authorized
	Hexa.	decimal		
Alarms on TSS	0060h	96	Read/write	1,2,3,4,5,6
Reserved	0061h to 0065h	97 to 101	Read/write	1,2,3,4,5,6
Primary host phone number	0066h to 0069h	102 to 105	Read/write	1,2,3,4,5,6
Standby host phone number	006Ah to 006Dh	106 to 109	Read/write	1,2,3,4,5,6
SMS service center phone number	006Eh to 0071h	110 to 113	Read/write	1,2,3,4,5,6
SMS user phone number	0072h to 0075h	114 to 117	Read/write	1,2,3,4,5,6
Cyclic dial up period	0076h to 0077h	118 to 119	Read/write	1,2,3,4,5,6
Reserved	0078h to 007Fh	120 to 127	Read/write	1,2,3,4,5,6
Configuration bits	0080h	128	Read/write	1,2,3,4,5,6
Primary voltage TP	0081h	129	Read/write	1,2,3,4,5,6
Secondary voltage TP	0082h	130	Read/write	1,2,3,4,5,6
Reserved	0083h	131	Read/write	1,2,3,4,5,6
Nominal voltage	0084h	132	Read/write	1,2,3,4,5,6
Power off threshold	0085h	133	Read/write	1,2,3,4,5,6
Power on threshold	0086h	134	Read/write	1,2,3,4,5,6
Reserved	0087h	135	Read/write	1,2,3,4,5,6
Imax threshold	0088h	136	Read/write	1,2,3,4,5,6
I0 threshold	0089h	137	Read/write	1,2,3,4,5,6
Validation time	008Ah	138	Read/write	1,2,3,4,5,6
Inrush time	008Bh	139	Read/write	1,2,3,4,5,6
Reset fault time	008Ch	140	Read/write	1,2,3,4,5,6
Imax fault ack. time	008Dh	141	Read/write	1,2,3,4,5,6
Quick Imax fault ack. time	008Eh	142	Read/write	1,2,3,4,5,6
I0 fault ack. time	008Fh	143	Read/write	1,2,3,4,5,6
Voltage on ack. time	0090h	144	Read/write	1,2,3,4,5,6
Volatge off ack. time	0091h	145	Read/write	1,2,3,4,5,6
Primary curent TC	0092h	146	Read/write	1,2,3,4,5,6
Reserved	0093h	147	Read/write	1,2,3,4,5,6
Preset NRJ (LSB)	0094h	148	Read/write	1,2,3,4,5,6
Preset NRJ (MSB)	0095h	149	Read/write	1,2,3,4,5,6
Reserved	0096h to 009Fh	150 to 159	Read/write	1,2,3,4,5,6

- **A TSS Alarm is alarmed with 1 bit :**
  - 1 = Alarm is ON if the TSS is ON
  - 0 = Alarm is not used

ALARM	Single remote indications	Word	bit
1	Digital input 1.	60h	0
2	Digital input 2.	60h	1
3	Digital input 3.	60h	2
4	Digital input 4.	60h	3
5	Digital input 5.	60h	4
6	Digital input 6.	60h	5
7	Flair200C Fault	60h	6
8	Test alarm	60h	7
9	Short message system enabled	60h	8
10	reserved	60h	9
11	AC supply OFF	60h	10
12	Phase fault	60h	11
13	Earth fault	60h	12
14	Alarm message set up	60h	13
15	reserved	60h	14
16	reserved	60h	15

■ **Test alarm** : A bit is used to test the alarm mechanism : if the bit is written with "1" by the master MODBUS, an alarm signal will set off one minute later. The bit will then be set to 0 by the FLAIR 200C if the alarm is acquitted.

■ **Alarm message set up :** A bit is used to set up the alarm mechanism: if the bit is written with "1" by the master MODBUS, The alarm mechanism is set up. If the bit is written with "0" by the master MODBUS, no alarm neither cyclic dialup will be do by the equipment

■ **Short message system enabled** : A bit is used to set up the SMS mechanism : if the bit is written with "1" by the master MODBUS, an alarm will send a SMS.

❑ **Phone number.**

Phone number of the host computer system or SMS, used to send the alarms.

15 figures maximum encodded.

Only this figures are accepted : <0 to 9>, '+'=<A>

Zone initialized with <F..F> : Flair 200C doesn't send alarms.

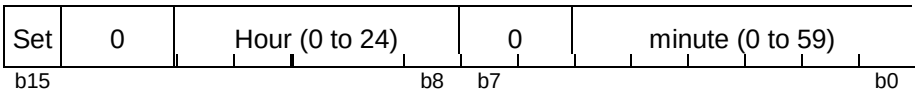
i.e. :+330476606599 encodded value :

Phone number	Word
FFFA	6Ah
3304	6Bh
7660	6Ch
6599	6Dh

❑ **Cyclic dial up period.**

The equipment may periodically dial up. This function can be used to verify that FLAIR 200C is alive and to download measurements.

■ Hour of the first dialup during the day (0076h)

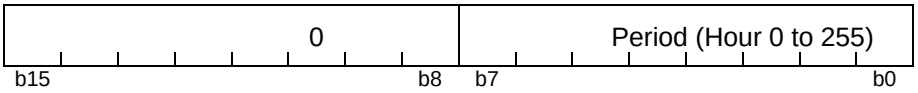


Set = 1 : Cyclic dial up mechanism is ON (only if "Alarm message set up"=1)

= 0 : Cyclic dial up mechanism is OFF

Hour and minute are the time in the day when the dial up function is started

■ Period of the dialup (0077h)



Period (number of hours) between to dial up

Each time when data is written in the this zone(76h-77h) automatic call is Re-initialize

❑ **Fault Detection parameters.**

■ **configuration bits**: bits used to configure boolean parameters:

Boolean parameter	Word	bit	Valeur autorisé
Homopolar wiring	80h	1	0, 1
Reset / power on	80h	2	0, 1
Reserved	80h	3	
U cable	80h	4-5-6	0 : U21, 3 : V1
Reserved	80h	7	
Reserved	80h	8	
Reserved	80h	9	
Active Inrush	80h	10	0.1
Reserved	80h	11	
Frequency 60hz	80h	12	0, 1
Reserved	80h	13-15	

■ **parameters**: used to configure measurements and fault passage indicator

Refer to the user's manual for the parameter definition.

Parameters	Min	Max	Incremental value	Details
Primary voltage TP	100	3200	1	NA
Secondary voltage TP	0	15	1	0 : 100 1 :110 2 :115 3 :120 4:100/sqrt(3) 5110sqrt(3) 6:115/sqrt(3) 7:120/sqrt(3) 8 : 200 9 : 210 10 : 230 11 : 240 12 200/sqrt(3) 13 210/sqrt(3) 14: 230/sqrt(3) 15: 240/sqrt(3)
Nominal voltage (V)	20	32000	1	NA
Power off threshold (%)	5	95	1	NA
Power on threshold (%)	70	120	1	NA
Résidual Volt threshold(%)	5	95	1	NA
Imax threshold (A)	40	750	1	NA
I0 threshold(A)	20	160	1	NA
Validation time(s)	1	70	1	NA
Inrush time (s)	0	70	1	NA
Reset fault Time (h)	1	12	1	NA
Imax fault ack. Time (ms)	40	800	1	NA
Quick Imax. fault ack. Time (ms)	20	800	1	NA
I0 fault ack. Time (ms)	20	800	1	NA
Voltage on ack. Time (ms)	10	18000	1	NA
Volatge off ack. Time (ms)	10	18000	1	NA
Primary current TC	50	2500	1	NA
Preset Energy (LSB) (kwh)	0	65535	1	NA
Preset Energy (MSB)	0	65535	1	NA

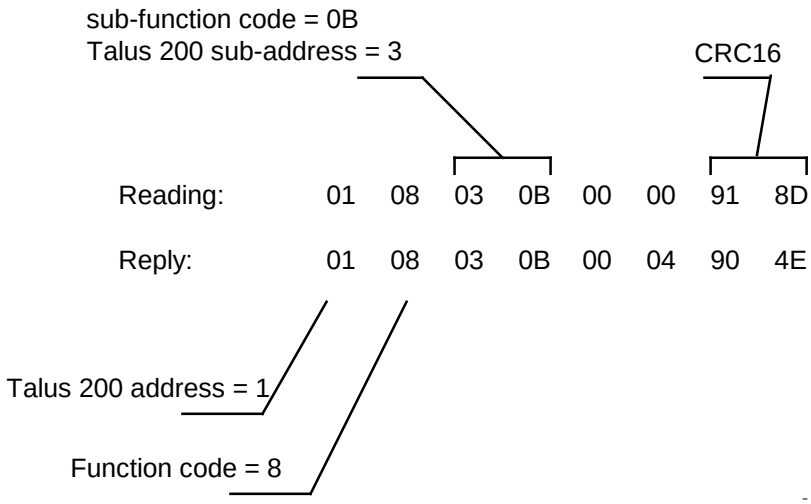
MODBUS data addresses and encoding

Diagnostic counter reading

The sub-function codes recognized by the FLAIR 200C are:

- 0000h: FLAIR 200C returns an echo of the request.
- 000Ah: diagnostic count reset.
- 000Bh: reading of the number of frames received with no CRC errors (CPT1).
- 000Ch: reading of the number frames received with CRC errors (CPT2).
- 000Dh: reading of the number of exception replies (CPT3).
- 000Eh: reading of the number of frames addressed to the station (CPT4).
- 000Fh: reading of broadcast requests received (CPT5).

The most significant bit of the sub-function code should be assigned with the sub-address of the FLAIR 200C to be accessed.



Report by exception with a modem

When an indication configured as an alarm changes of state, FLAIR 200C initiates an alarm cycle by dialling-up the main phone number after the ‘’dial-up delay time / first attempt’’.

Two cases can occure:

1 - The telecontrol center system doesn’t answer:

FLAIR 200C dial-up again the ‘’main’’ phone number after the ‘’dial-up delay time / second attempt’’ and eventually try again after the ‘’dial-up delay time / third attempt’’.

2 - The telecontrol center system answer :

The telecontrol center system send a broadcast message (Slave address = 0) and the function code = 0.

FLAIR 200C send back an exception message with its address, function code 0 with most significant bit set to 1 and the exception code = 0.

The telecontrol center system can then initiate a standard MODBUS Master/Slave communuication.

Example of an alarm followed by TS reading (Address=1)
(Frame displayed with the MODBUS analyser function of the COMMS card)

```
98/06/12 11:18:06.20 Alarm 1, delay = 1s...
98/06/12 11:18:08.22 Call in progress... "122"
98/06/12 11:18:30.48 Connected, calling mode "CONNECT 9600"
98/06/12 11:18:33.80 address     <  00 00 01 B0
98/06/12 11:18:33.80 ADDRESS     >> 01 80 00 40 03
98/06/12 11:18:44.84 read  ts    <  01 03 00 34 00 08 04 F2
98/06/12 11:18:44.84 READ  TS    >> 01 03 10 00 9A 00 00 00 04
00
                                    00 00 00 00 40 00 00 00 00
     EA CD
```

MODBUS is a master - slave protocol.

It is used to read or write one or more words (16 bits), as well as diagnostic counters.

Functions available:

- **1**: read n output bits.
- **2**: read n input bits.
- **3**: read n output words.
- **4**: read n input words.
- **5**: write a bit.
- **6**: write a word.
- **8**: read diagnostic counters.
- **16**: write several words.

Exchanges are carried out at the master's initiative and comprise a request from the master followed by the reply from the slave. The master's requests are addressed to a slave identified by its number in the first byte of the frame or else addressed to all the slaves (broadcast).

Broadcast commands are necessarily write commands. No reply is transmitted by the slaves.

Structure of frames exchanged

All the frames exchanged (request and reply) have the same structure:

Slave number	function code	data zone	check zone CRC16

Each message or frame contains 4 types of information:

- slave number (1 byte): it specifies the receiving equipment (0 to FFh). If it is equal to zero, the request concerns all the slaves (broadcast) and there is no reply message.
- function code (1 byte): it is used to select a command (read, write...) and check that the reply is correct.
- data zone (n bytes): it contains the parameters linked to the function.
- check zone (2 bytes): it is used to detect transmission errors.

Please note that words (2 bytes = 16 bits) are always written as high-order bits to low-order bits, with the exception of the CRC16 which is written as least significant bit, most significant bit.

Appendix

Synchronization of exchanges

Any character that is received after a silence of more than 3 characters is considered as the beginning of a frame. A silence in the line equal to at least 3 characters should be respected between two frames.

Example: at 9600 bauds, the time is equal to approximately 3 milliseconds.

Checking of messages received by the slave

When the slave receives a frame, it checks the following, in order: CRC16, slave number, function code and function parameters.

■ If the CRC16 or the slave number are incorrect, the slave does not reply.

■ If the CRC16 and the slave number are correct, but the function code or parameters are not valid, the slave transmits an exception reply.

■ If the CRC16, slave number, function code and parameters are correct, the slave replies to the master's request.

Exception reply transmitted by the slave

Slave number	function code received with MSB set to 1	Exception code 01 unknown function code 02 incorrect address 03 incorrect data	CRC16
1 byte	1 byte	1 byte	2 bytes

Appendix

Read N bits: functions n°1 and 2

Function 1: read output bits.
Function 2: read input bits.

Request

Slave number	1 or 2	address of 1st bit (MSB+LSB)	number of bits	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

Reply

Slave number	1 or 2	number of bytes read	1st byte read		last byte read	CRC16
1 byte	1 byte	1 byte	2 bytes	N bytes	2 bytes	2 bytes

Example

Reading of 16 bits, bit address 300h of slave n°1
Request: `01 01 03 00 00 10 36 42`
Reply:`01 01 02 00 00 B9 FC`

Read N words: functions n°3 and 4

The number of words to be read should **be less than or equal to 125.**

Function 3: read output words.
Function 4: read input words.

Request

Slave number	3 or 4	address of 1st word (MSB+LSB)	number of words (MSB+LSB)	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

Reply

Slave number	3 or 4	number of bytes read	1st word read (MSB+LSB)		last word read (MSB+LSB)	CRC16
1 byte	1 byte	1 bytes	2 bytes		2 bytes	2 bytes

Example

Reading of words 40h to 43h of slave n°1,
Request: `01 03 00 40 00 04 45 DD`
Reply:`01 03 08 00 00 80 00 80 00 80 00 C2 18`

Appendix

Write a bit: function n°5

Request

Slave number	5	address of bit (MSB+LSB)	bit value	0	CRC16
1 byte	1 byte	2 bytes	1 byte	1 byte	2 bytes

Reply

The reply is an echo of the request indicating that the slave has acknowledged the value contained in the request.

Slave number	5	address of bit (MSB+LSB)	bit value	0	CRC16
1 byte	1 byte	2 bytes	1 byte	1 byte	2 bytes

Example

Writing of bit to 1, bit address 301h of slave n°1,
Request: `01 05 03 01 FF 00 D6 8E`
Reply:`01 05 03 01 FF 00 D6 8E`

Write a word: function n°6

Request

Slave number	6	address of word (MSB+LSB)	value of word (MSB+LSB)	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

Reply

The reply is an echo of the request indicating that the slave has acknowledged the value contained in the request.

Slave number	6	address of word (MSB+LSB)	value of word (MSB+LSB)	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

Example

Writing of word 30h of slave n°1, at the value 0001h
Request: `01 06 00 30 00 01 48 05`
Reply:`01 06 00 30 00 01 48 05`

Read diagnostic counters: function n°8

Each slave is assigned diagnostic counters. There are 5 counters in all per slave. The counters are 16-bit words. When they reach FFFFh, they go back to 0000h.
When a request is sent by the master, the most significant byte in the sub-function code is assigned by the FLAIR 200C equipment offset to access and the data are at 0000h.
When the slave sends a reply, the data contain the value of the counter concerned.

Request / reply

Slave number	8	sub-function code (MSB+LSB)	data (MSB+LSB)	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

	sub-function code	data
the slave should send the echo of the request	xx00	XXXX
resetting of diagnostic counters	xx0A	0000
reading of total number:		
of frames received with no CRC errors (CPT1)	xx0B	XXXX
of frames received with CRC errors (CPT2)	xx0C	XXXX
of the number of exception replies (CPT3)	xx0D	XXXX
of frames addressed to the station (CPT4) (excluding broadcast)	xx0E	XXXX
of broadcast requests received and correctly executed (CPT5)	xx0F	XXXX

Sub-function n°0 is used to test transmission. The slave sends back the echo of the data received.

Examples

Resetting of counters for slave n°1,
Request: `01 08 00 0A 00 00 C0 09`
Reply:`01 08 00 0A 00 00 C0 09`

Reading of broadcast requests received (CPT5) for slave n°1, offset 3 (300h in storage space)
Request: `01 08 03 0F 00 00 D0 4C`
Reply:`01 08 03 0F 00 05 10 4F`

Write N consecutive words: function n°16

The number of words to be written is between 1 and 123 and the number of bytes is between 2 and 246.
Words are written in increasing order of addresses.

Request

Slave number	10h	address of 1st word to write	number of words to write	number of bytes to write	values of words to write	CRC16
1 byte	1 byte	2 bytes	2 bytes	1 byte	N bytes	2 bytes

Reply

Slave number	10h	address of 1st word written (MSB+LSB)	number of words written (MSB+LSB)	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes

Example

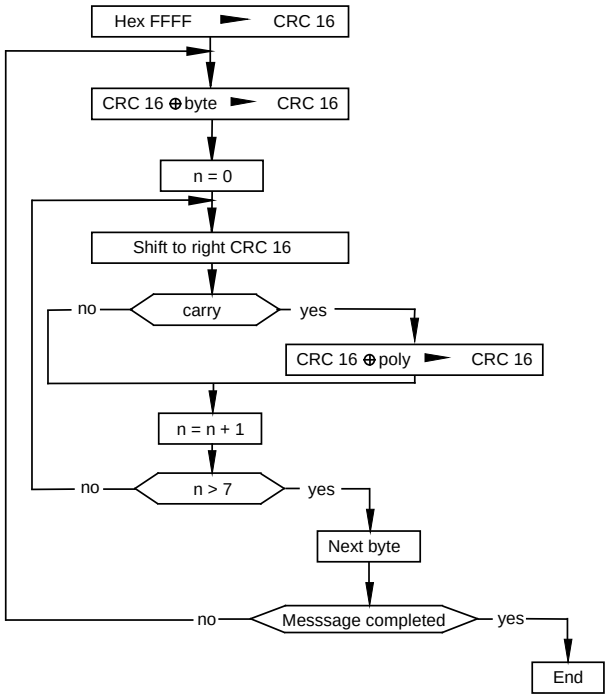
Writing of words 0302h to 0305h of slave n°1, (addresses 02h to 05h) with the values 0060h, 0A10h, 0B33h, 1662h

Request: `01 10 03 02 00 04 08 00 60 0A 10 0B 33 16 62 96 B3`

Reply: `01 10 03 02 00 04 60 4E`

Appendix

CRC 16 calculation algorithm



n = number of bits of data
poly= CRC16=1010 0000 0000 0001 calculation polynomial

Write CRC 16 calculation in C language

Calculates and gives the CRC16 in the "buf" zone with length "len".

- *buf: pointer of buffer on which the calculations are performed.
- len: length of buffer.

```
unsigned crc16(char *buf, int len)
    {
    #define POLY  0xA001
    char i;
    unsigned crc;

    for (crc = 0xFFFF; len != 0; len --)
        {
        crc ^= *buf ++;
        for (i = 0; i < 8; i ++)
            {
            if (crc & 0x0001)
                crc = (crc >> 1) ^ POLY;
            else
                crc >>= 1;
            }
        }
    return (crc);
    }
```

Schneider Electric SA

Postal address
F-38050 Grenoble Cedex 9
Tel.: +33 (0)4 86 58 60 60
Telex: merge 320842 F
http:\\www.schneider-electric.com

Rcs nanterre B 954 503 439

Published by: Schneider Electric SA
Design and layout by: PIPET
Printed by: Hewlett Packard

NT00079-01 FLAIR 200C Modbus communication - Edition 1 : 07/2005