Il protocollo MODBUS

Il protocollo MODBUS, proposto dalla *Compagnie de Regulation et de Controle Industriel*, è uno standard utilizzato su bus di qualsivoglia livello fisico (in corrente, 232, 485, anche su Ethernet, ecc.).
È adatto per connessioni punto-punto oppure multipunto del tipo master-slave, in modalità polling-selecting.
Dal punto di vista del protocollo, ogni slave risulta organizzato in due aree:

- **area word**, contenente tutte le grandezze numeriche, i parametri di personalizzazione (i valori misurati, i valori di soglia, i coefficienti, i time-out, ecc.);
- **area bit**, contenente tutti gli stati binari (comandi, allarmi, ingressi, ecc.).

I messaggi possibili contemplano quindi pochi codici (**tab. 1**), con l'aggiunta del messaggio di broadcasting, di indirizzo '0', di sola scrittura e senza risposta.

Tab. 1 – Alcuni codici funzione MODBUS

Funzione	Codice	Risposta
lettura n bit	1 oppure 2	bit letti
lettura n word	3 oppure 4	word lette
scrittura 1 bit	5	eco
scrittura 1 word	6	eco
scrittura n bit	15	eco header
scrittura n word	16	eco header
broadcasting	-	-

La trasmissione è asincrona, strutturata in byte e codificata in ASCII (*American Standard Code for Information Interchange*) o in binario RTU (*Remote Terminal Unit*).
In ASCII mode, il frame (**fig. 1**) inizia con il carattere due punti (3AH) e termina con i due caratteri CR (0DH) LF (0AH).

: 3AH	Indirizzo dello slave	Funzione richiesta	Dati eventuali associati alla funzione	LRC	CR 0DH	LF 0AH
1 byte	2 byte	2 byte	n byte	2 byte	1 byte	1 byte

Fig. 1. *Frame MODBUS in ASCII mode.*

Al suo interno sono possibili solo i sedici caratteri 0 ÷ 9, A ÷ F, ciascuno dei quali fornisce una cifra esadecimale di informazione, compresi i 2 byte conclusivi di controllo LRC (*Longitudinal Redundancy Check*). I due byte ASCII di LRC corrispondono al complemento a due della somma ad 8 bit dei byte a monte, escluso il due punti.
In RTU mode, il frame inizia e termina con un silenzio pari ad almeno 3,5 caratteri (**fig. 2**).

Silenzio	Indirizzo dello slave	Funzione richiesta	Dati eventuali associati alla funzione	CRC	Silenzio
4 byte time	1 byte	1 byte	n byte	2 byte	4 byte time

Fig. 2. *Struttura dei messaggi MODBUS in RTU mode.*

Nel messaggio RTU ogni byte contiene due cifre esadecimali di informazione, e il tutto termina con 2 byte di controllo CRC (*Cyclical Redundancy Check*).

ESEMPIO 1

Per inviare il valore 63H, basta un solo byte in RTU mode (63H = 0110 0011), mentre servono due byte in ASCII mode ('6'+ '3' = 36H + 33H = 0011 0110 + 0011 0011).

Le regole di scambio prevedono che lo slave risponda solo se il messaggio di interrogazione a lui diretto risulta corretto nel CRC (oppure LRC); mentre se rileva un codice errato o un indirizzo di memoria inesistente all'interno di un messaggio corretto a lui destinato, risponde con un messaggio di errore, caratterizzato dal byte di codice funzione con il bit MSB = 1, seguito dal codice dell'errore.

ESERCIZIO A

Un master MODBUS intende leggere dal periferico numero 5, le variabili contenute in 3 word, residenti a partire dall'indirizzo 4BH della sua tabella interna. Comporre i frame MODBUS di richiesta e di risposta e tradurli in modalità ASCII e RTU. Calcolare il valore da assegnare ai due byte LCR per il messaggio di trasmissione.

SOLUZIONE

Dalla **tab. 1** si ricava che il codice della funzione corrispondente alla lettura di word è 3 e, seguendo le indicazioni sulla struttura di una trama MODBUS (**fig. 1** e **2**) si compongono i due frame (**fig. 3**), ipotizzando un campo dati a piacere.

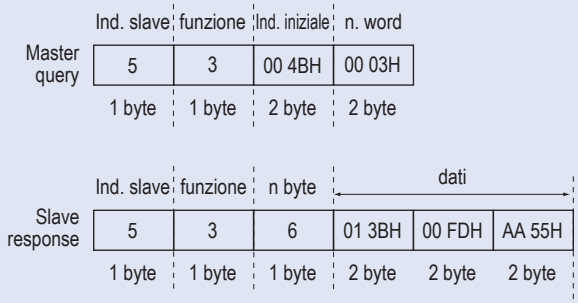

Fig. 3. *Polling MODBUS.*

Per la traduzione in formato ASCII e RTU vanno aggiunti i byte di testa e di coda necessari (**tab. 2** e **tab. 3**).

Tab. 2 – Interrogazione

Field name		Caratteri ASCII		RTU
Header			:	
Indirizzo slave	5	0	5	05H
Funzione	3	0	3	03H
Indirizzo iniziale Hi	00H	0	0	00H
Indirizzo iniziale Lo	4BH	4	B	4BH
N. di word Hi	00H	0	0	00H
N. di word Lo	03H	0	3	03H
Error check (16 bit)		LRC		CRC
Trailer		CR	LF	
N. totale di byte		17		8

Tab. 3 – Risposta

Field name		Caratteri ASCII		RTU
Header			:	
Indirizzo slave	5	0	5	05H
Funzione	3	0	3	03H
N. byte	6	0	6	06H
Dato 1 Hi	01H	0	1	01H
Dato 1 Lo	3BH	3	B	3BH
Dato 2 Hi	00H	0	0	00H
Dato 2 Lo	FDH	F	D	FDH
Dato 3 Hi	AAH	A	A	AAH
Dato 3 Lo	55H	5	5	55H
Error check (16 bit)		LRC		CRC
Trailer		CR	LF	
N. totale di byte		23		11

I due byte ASCII di LRC corrispondono al complemento a due della somma a 8 bit dei byte a monte, escluso il due punti; nel frame di interrogazione la somma dei valori esadecimali dei caratteri a monte, con "B" = 42H, vale:

30H + 35H + 30H + … + 33H = 261H

Trascurando i trabocchi, rimane 61H, che in binario corrisponde a 0110 0001.
Il complemento a due è 1001 1111 = 9FH, pertanto i due caratteri LRC valgono rispettivamente '9' e 'F'.

ESERCIZIO B

Interpretare il seguente frame MODBUS di interrogazionein formato RTU, sapendo che FF 00H significa forzare alto e 00 00H forzare basso:

13H 05H 0025H FF00H CRC

SOLUZIONE

Trattandosi del codice funzione 5, il master intende forzare alto il bit di indirizzo 0025H del periferico numero 19 (13H).

ESERCIZIO 1

Un master MODBUS intende leggere dal periferico numero 9, le variabili contenute in 2 word, residenti a partire dall'indirizzo 1A 3EH della sua tabella interna. Comporre i frame MODBUS di richiesta e di risposta e tradurli in modalità ASCII e RTU, supponendo tutti i dati di valore AA 55H. Calcolare il valore da assegnare ai due byte LCR per il messaggio di trasmissione.

[Ris.: tab. 4 e tab. 5; LRC = '8' + '8']

Tab. 4 – Interrogazione

Field name		Caratteri ASCII		RTU
Header			:	
Indirizzo slave	9	0	9	09H
Funzione	3	0	3	03H
Indirizzo iniziale Hi	1AH	1	A	1AH
Indirizzo iniziale Lo	3EH	3	E	3EH
N. di word Hi	00H	0	0	00H
N. di word Lo	02H	0	2	02H
Error check (16 bit)		LRC		CRC
Trailer		CR	LF	
n. totale di byte		17		8

Tab. 5 – Risposta

Field name		Caratteri ASCII		RTU
Header			:	
Indirizzo slave	9	0	9	09H
Funzione	3	0	3	03H
N. byte	4	0	4	04H
Dato 1 Hi	AAH	A	A	AAH
Dato 1 Lo	55H	5	5	55H
Dato 2 Hi	AAH	A	A	AAH
Dato 2 Lo	55H	5	5	55H
Error check (16 bit)		LRC		CRC
Trailer		CR	LF	
n. totale di byte		19		9

ESERCIZIO 2

Interpretare il seguente frame MODBUS di interrogazione in formato RTU:

13H 01H 0015H 0022H CRC

Indicare la composizione del frame RTU di risposta, ipotizzando tutti i bit alti.

[Ris.: legge 34 bit (22H) dallo slave n. 19, a partire dall'indirizzo 21 (15H) al 53; 13H 01H 05H FFH FFHFFHFFH 02H CRC]

ESERCIZIO 3

Interpretare il seguente frame MODBUS di interrogazione in formato RTU, sapendo che FF 00H significa forzare alto e 00 00H forzare basso:

32H 05H 004EH 0000H CRC

[Ris.: forza a zero il bit di indirizzo 00 4EH dello slave n. 50]

ESERCIZIO 4

Interpretare il seguente frame MODBUS di interrogazione in formato RTU:

13H 06H 0001H 005AH CRC

[Ris.: forza la word di indirizzo 1 dello slave n. 19 al valore 005AH]

ESERCIZIO 5

Interpretare il seguente frame MODBUS di interrogazione in formato RTU, sapendo che 1 significa forzare alto, 0 forzare basso e che 02H corrisponde al numero di byte dei dati:

15H 0FH 001BH 000CH 02H FFH 0FH CRC

[Ris.: forza alti 12 bit (0CH) a partire dall'indirizzo 37 dello slave n. 21]

ESERCIZIO 6

Interpretare il seguente frame MODBUS di interrogazione in formato RTU, sapendo che 1 significa forzare alto, 0 forzare basso e che 04H corrisponde al numero di byte dei dati:

18H 10H 0001H 0002H 04H FFFFH FFFFH CRC

[Ris.: forza alte due word (codice 16) a partire dall'indirizzo 1 dello slave n. 24]