



www.eneren.it
info@eneren.it

Software R_E

Comunicazione seriale RS485

INFORMAZIONI GENERICHE PER COMUNICAZIONE SERIALE RS485

IL PROTOCOLLO MODBUS

Il protocollo MODBUS definisce il formato e la modalità di comunicazione tra un "master" che gestisce il sistema e uno o più "slave" che rispondono alle interrogazioni del master.

Il protocollo definisce come il master e gli slave stabiliscono ed interrompono la comunicazione, come trasmettitore e ricevitore devono essere identificati, come i messaggi devono venire scambiati e come gli errori rilevati.

Si possono connettere un master e fino a 247 slave su una linea comune, occorre notare che questo è un limite logico del protocollo, l'interfaccia fisica può peraltro limitare ulteriormente il numero di dispositivi, per esempio l'interfaccia standard RS-485 prevede un massimo di 31 slave connessi alla linea.

Sostituendo l'ultimo elemento della linea con un apposito "bridge o ripetitore", si possono connettere altri 31 slave e così via sino al raggiungimento del numero massimo logico di dispositivi applicati.

Solo il master può iniziare una transazione.

Una transazione può avere il formato domanda/risposta diretta ad un singolo slave o broadcast in cui il messaggio viene inviato a tutti i dispositivi sulla linea che non danno risposta.

Una transazione è composta da una struttura singola domanda/singola risposta o una struttura singolo messaggio broadcast/nessuna risposta.

Alcune caratteristiche del protocollo sono definite e sono:

- Baud rate / velocità
- lunghezza dati
- parità
- numero di stop bit

FORMATO DEI MESSAGGI

Per poter comunicare tra due dispositivi, il messaggio deve essere contenuto in un "involucro"

L'involucro lascia il trasmettitore attraverso una "porta" ed è "portato" lungo la linea fino ad una analoga "porta" sul ricevitore.

MODBUS stabilisce il formato di questo involucro che, tanto per il master che per lo slave. Comprende:

- L'indirizzo del dispositivo con cui il master ha stabilito la transazione (l'indirizzo 0 corrisponde ad un messaggio broadcast inviato a tutti i dispositivi slave)
- Il codice della funzione che deve essere o è stata eseguita
- I dati che devono essere scambiati
- Il controllo d'errore composto secondo l'algoritmo CRC16

Se un dispositivo individua un errore nel messaggio ricevuto (di formato, di parità o nel CRC16) il messaggio viene considerato non valido e scartato, uno slave che rilevi un errore nel messaggio quindi non eseguirà l'azione e non risponderà alla domanda, così come se l'indirizzo non corrisponde ad un dispositivo in linea.

L'INDIRIZZO

Come sopra menzionato, le transazioni MODBUS coinvolgono sempre il master, che gestisce la linea, e uno slave per volta (tranne nel caso di messaggi broadcast).

Per identificare il destinatario del messaggio viene trasmesso come primo carattere un byte che contiene l'indirizzo numerico del dispositivo slave selezionato.

Ciascuno degli slave quindi avrà assegnato un diverso numero di indirizzo che lo identifica univocamente.

Gli indirizzi ammissibili sono quelli da 1 a 247, mentre l'indirizzo 0, che non può essere assegnato ad uno slave, posto in testa al messaggio trasmesso dal master indica che questo è "broadcast", cioè diretto a tutti gli slave contemporaneamente.

Possono essere trasmessi come broadcast solo messaggi che non richiedano risposta per espletare la loro funzione, quindi solo le assegnazioni.

CODICI FUNZIONI

- 01 - Read coil status
- 02 - Read input status
- 03 - Read holding registers
- 04 - Read input registers
- 05 - Force single coil
- 06 - Preset single register
- 15 - Force multiple coils
- 16 - Preset multiple registers

IL CRC16

Gli ultimi due caratteri del messaggio contengono il codice di ridondanza ciclica (Cyclic Redundancy Check) calcolato secondo l'algoritmo CRC16.

Per il calcolo di questi due caratteri il messaggio (indirizzo, codice funzione e dati scartando i bit di start, stop e l'eventuale parità) viene considerato come un unico numero binario continuo di cui il bit più significativo (MSB) viene trasmesso prima.

Il messaggio viene innanzitutto moltiplicato per 216 (spostato a sinistra di 16 bit) e poi diviso per $2^{16+215+22+1}$ espresso come numero binario (1100000000000101).

Il quoziente intero viene poi scartato e il resto a 16 bit (inizializzato a FFFFh all'inizio per evitare il caso di un messaggio di soli zeri) viene aggiunto di seguito al messaggio trasmesso.

Il messaggio risultante, quando diviso dal dispositivo ricevente per lo stesso polinomio ($2^{16+215+22+1}$) deve dare zero come resto se non sono intervenuti errori (il dispositivo ricevente ricalcola il CRC).

Di fatto, dato che il dispositivo che serializza i dati da trasmettere (UART) trasmette prima il bit meno significativo (LSB) anziché il MSB come dovrebbe essere per il calcolo del CRC, questo viene effettuato invertendo il polinomio.

Inoltre, dato che il MSB del polinomio influenza solo il quoziente e non il resto, questo viene eliminato rendendolo quindi 1010000000000001.

La procedura passo-passo per il calcolo del CRC16 è la seguente:

1. Caricare un registro a 16 bit con FFFFh (tutti i bit a 1).
2. Fare l'OR esclusivo del primo carattere con il byte superiore del registro, porre il risultato nel registro.
3. Spostare il registro a destra di un bit.
4. Se il bit uscito a destra dal registro (flag) è un 1, fare l'OR esclusivo del polinomio generatore 1010000000000001 con il registro.
5. Ripetere per 8 volte i passi 3 e 4.
6. Fare l'OR esclusivo del carattere successivo con il byte superiore del registro, porre il risultato nel registro.
7. Ripetere i passi da 3 a 6 per tutti i caratteri del messaggio.
8. Il contenuto del registro a 16 bit è il codice di ridondanza CRC che deve essere aggiunto al messaggio

SINCRONIZZAZIONE DEI MESSAGGI

La sincronizzazione del messaggio tra trasmettitore e ricevitore viene ottenuta interponendo una pausa tra i messaggi pari ad almeno 3,5 volte il tempo di un carattere.

Se il dispositivo ricevente non riceve per un tempo di 3,5 caratteri, ritiene completato il messaggio precedente e considera che il successivo byte ricevuto sarà il primo di un nuovo messaggio e quindi un indirizzo.

TUTTE LE FUNZIONI

Viene riportata di seguito la descrizione dettagliata delle funzioni MODBUS più utilizzate.

READ COIL STATUS (01)

Questa funzione permette di richiedere lo stato ON o OFF di variabili logiche binarie. Il modo broadcast non è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (01) il messaggio contiene l'indirizzo di partenza (starting Address) espresso su due byte e il numero di bit da leggere anch'esso su due byte.

La numerazione degli indirizzi parte da zero (bit1 = 0).

Esempio: Richiesta di lettura dallo slave 17 del bit dal 0004 al 0015.

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA bit # HI	DATA bit # LO	CRC HI	CRC LO
11	01	00	03	00	0C	CE	9F

Risposta

Oltre all'indirizzo dello slave e al codice funzione (01) il messaggio comprende un carattere che contiene il numero di byte di dati e i caratteri contenenti i dati.

I dati sono impaccati, così che un byte contiene lo stato di 8 bit, il bit meno significativo del primo byte contiene il bit corrispondente allo starting Address e così via.

Se il numero di bit da leggere non è multiplo di 8, l'ultimo carattere è completato con zeri nei bit più significativi.

Esempio: Risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA byte count	DATA bit 04..11	DATA bit 12..15	CRC HI	CRC LO
11	01	02	CD	0B	6D	68

READ INPUT STATUS (02)

Questa funzione è operativamente identica alla precedente.

READ HOLDING REGISTERS (03)

Questa funzione permette di richiedere il valore di registri a 16 bit (word) contenenti variabili numeriche. Il modo broadcast non è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (03) il messaggio contiene l'indirizzo di partenza (starting Address) espresso su due byte e il numero di word da leggere anch'esso su due byte.

Il numero massimo di word che possono essere lette è 125.

La numerazione degli indirizzi parte da zero (word1= 0).

Esempio: Richiesta di lettura dallo slave 25 dei registri da 069 a 071.

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA bit # HI	DATA bit # LO	CRC HI	CRC LO
19	03	00	44	00	03	46	06

Risposta

Oltre all'indirizzo dello slave e al codice funzione (03) il messaggio comprende un carattere che contiene il numero di byte di dati e i caratteri contenenti i dati.

I registri richiedono due byte ciascuno, il primo dei quali contiene la parte più significativa.

Esempio: Risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA byte count	DATA byte 69 HI	DATA byte 69 LO	DATA byte 70 HI	DATA byte 70 LO	DATA byte 71 HI	DATA byte 71 LO	CRC HI	CRC LO
19	03	06	02	2B	00	00	00	64	AF	7A

READ INPUT REGISTERS (04)

Questa funzione è operativamente identica alla precedente.

FORCE SINGLE COIL (05)

Questa funzione permette di forzare lo stato di una singola variabile binaria ON o OFF. Il modo broadcast è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (05) il messaggio contiene l'indirizzo della variabile da forzare su due byte e due caratteri di cui il primo è posto a FFh (255) per forzare lo stato ON e 00h per forzare OFF, il secondo è posto a zero in ogni caso. La numerazione degli indirizzi parte da zero (bit1 = 0).

Esempio: Richiesta di forzare ON sullo slave 47 il bit 4.

ADDR	FUNC	DATA bit HI	DATA bit LO	DATA ON / OFF	DATA (zero)	CRC HI	CRC LO
2F	05	00	03	FF	00	7A	74

Risposta

La risposta consiste nel ritrasmettere il messaggio ricevuto dopo che la variabile è stata modificata.

Esempio: risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA bit HI	DATA bit LO	DATA ON / OFF	DATA (zero)	CRC HI	CRC LO
2F	05	00	03	FF	00	7A	74

PRESET SINGLE REGISTER (06)

Questa funzione permette di impostare il valore di un singolo registro a 16 bit. Il modo broadcast è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (06) il messaggio contiene l'indirizzo della variabile espresso su due byte e il valore che deve essere assegnato.

La numerazione degli indirizzi parte da zero (word1 = 0).

Esempio: Richiesta di forzare 928 sullo slave 35 all'indirizzo 26.

ADDR	FUNC	DATA bit # HI	DATA bit # LO	DATA Word HI	DATA Word LO	CRC HI	CRC LO
23	06	00	19	03	A0	5E	07

Risposta

La risposta consiste nel ritrasmettere il messaggio ricevuto dopo che la variabile è stata modificata.

Esempio: Risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA bit # HI	DATA bit # LO	DATA Word HI	DATA Word LO	CRC HI	CRC LO
23	06	00	19	03	A0	5E	07

FORCE MULTIPLE COILS (15)

Questa funzione permette di forzare lo stato di ciascuna variabile binaria in un blocco consecutivo. Il modo broadcast è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (15) il messaggio contiene l'indirizzo di partenza (starting Address) espresso su due byte, il numero di bit da scrivere, il numero di byte che contengono i dati e i caratteri di dati, i dati sono impaccati, così che un byte contiene lo stato di 8 bit, il bit meno significativo del primo byte deve contenere il bit corrispondente allo starting Address e così via. Se il numero di bit da scrivere non è multiplo di 8, l'ultimo carattere va completato con zeri nei bit più significativi. La numerazione degli indirizzi parte da zero (bit1 = 0).

Esempio: Richiesta di forzare, sullo slave 12, 4 bit a partire dall'indirizzo 1. I bit 1 e 4 forzati a "1", gli altri a "0".

ADDR	FUNC	DATA start ADDR HI	DATA start ADDR LO	DATA bit # HI	DATA bit # LO	DATA byte Count	DATA bit 1..4	CRC HI	CRC LO
0C	0F	00	00	00	04	01	09	3F	09

Risposta

Oltre all'indirizzo dello slave e al codice funzione (15) il messaggio comprende l'indirizzo di partenza (starting Address) e il numero di bit scritti.

Esempio: Risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA start ADDR HI	DATA start ADDR LO	DATA bit # HI	DATA bit # LO	CRC HI	CRC LO
0C	0F	00	00	00	04	55	15

PRESET MULTIPLE REGISTERS (16)

Questa funzione permette di impostare il valore di un blocco consecutivo di registri a 16 bit. Il modo broadcast è permesso.

Domanda

Oltre all'indirizzo dello slave e al codice funzione (16) il messaggio contiene l'indirizzo di partenza (starting Address), il numero di word da scrivere, il numero di byte che contengono i dati e i caratteri di dati.

La numerazione degli indirizzi parte da zero (word1 = 0).

Esempio: Richiesta di impostare, sullo slave 17, 1 word all'indirizzo 35. con valore 268.

ADDR	FUNC	DATA start ADDR HI	DATA start ADDR LO	DATA Word # HI	DATA Word # LO	DATA byte Count	DATA Word 35 HI	DATA Word 35 LO	CRC HI	CRC LO
11	10	00	22	00	01	02	01	0C	6C	87

Risposta

Oltre all'indirizzo dello slave e al codice funzione (16) il messaggio comprende l'indirizzo di partenza (starting Address) e il numero di word scritte.

Esempio: Risposta alla richiesta sopra riportata.

ADDR	FUNC	DATA start ADDR HI	DATA start ADDR LO	DATA bit # HI	DATA bit # LO	CRC HI	CRC LO
11	10	00	22	00	01	A3	53

LA GESTIONE DEGLI ERRORI

In MODBUS esistono due tipi di errori, gestiti in modo diverso: errori di trasmissione ed errori operativi.

Gli errori di trasmissione sono errori che alterano il messaggio, nel suo formato, nella parità (se è usata), o nel CRC16.

Il dispositivo che rilevi errori di questo tipo nel messaggio lo considera non valido e non da risposta.

Qualora invece il messaggio sia corretto nella sua forma ma la funzione richiesta, per qualsiasi motivo, non sia eseguibile, si ha un errore operativo. A questo errore il dispositivo slave risponde con un messaggio di eccezione.

Questo messaggio è composto dall'indirizzo, dal codice delta funzione richiesta, da un codice d'errore e dal CRC. Per indicare che la risposta è la notifica di un errore il codice funzione viene ritornato con il bit più significativo a "1".

Domanda

Esempio: richiesta di lettura dallo slave 10 del bit 1185.

ADDR	FUNC	DATA start Addr HI	DATA start Addr LO	DATA bit # HI	DATA bit # LO	CRC HI	CRC LO
0A	01	04	A1	00	01	AC	63

Risposta

La richiesta chiede il contenuto del bit 1185 che non esiste nello slave.

Questo risponde con il codice d'errore "02" (ILLEGAL DATA ADDRESS) e ritorna il codice funzione 81h (129).

Esempio: Eccezione alla richiesta sopra riportata.

ADDR	FUNC	DATA exept. code	CRC HI	CRC LO
0A	81	02	B0	53

CODICI D'ECCEZIONE

Sotto vengono riportati i codici di eccezione più utilizzati:

Codice	Nome	Significato
01	ILLEGAL FUNCTION	Il codice di funzione ricevuto non corrisponde ad una funzione permessa sullo slave indirizzato.
02	ILLEGAL DATA ADDRESS	L'indirizzo cui fa riferimento il campo dati non è un indirizzo permesso sullo slave indirizzato.
03	ILLEGAL DATA VALUE	Il valore da assegnare cui fa riferimento il campo dati non è permesso per questo indirizzo.

Salvataggio delle informazioni con lo Standard Modbus

Le informazioni sono salvate nel dispositivo slave in quattro differenti tabelle.

Due tabelle contengono i valori binari on/off (coils) e due i valori numerici (registers). Le coils e i registers hanno ognuno una tabella in sola lettura e una in lettura-scrittura.

Ogni tabella contiene 9999 valori.

Ogni coil o contact è 1 bit e assegna un data address tra 0000 e 270E (notazione esadecimale).

Ogni registro è 1 word = 16 bits = 2 bytes e anch'esso ha un data address tra 0000 e 270E (notazione esadecimale).

Coil/Register Numbers	Data Addresses	Type	Table Name
00001-09999	0000 to 270E	Read/Write	Discrete Output Coils
10001-19999	0000 to 270E	Read Only	Discrete Input Contacts
30001-39999	0000 to 270E	Read Only	Analog Input Registers
40001-49999	0000 to 270E	Read/Write	Analog Output Holding Registers

Coil/Register Numbers possono essere pensati come rappresentazione del nome della locazione in memoria ma non appaiono nei messaggi. I Data Address sono usati nei messaggi.

Per esempio, il primo Holding Register, numero 40001, ha il Data Address 0000.

La differenza tra questi due valori è l'offset.

Ogni tabella ha un differente offset. 1, 10001, 30001 and 40001.

INFORMAZIONI SPECIFICHE

SPECIFICHE HARDWARE

Il protocollo di comunicazione è Modbus - RTU.

L'integrato utilizzato nella scheda per la comunicazione RS485 Modbus prevede il collegamento fino ad un massimo di 32 dispositivi, tuttavia questo limite può risultare inferiore in quanto non tiene conto della presenza del circuito di polarizzazione del bus, della presenza di resistenze di terminazione di linea e della lunghezza complessiva della linea stessa.

Nel caso di reti particolarmente estese, dal momento che l'hardware non prevede l'optoisolamento tra la rete e la scheda, la scheda deve rimanere sempre alimentata per poter assumere uno stato di alta impedenza, così da non attenuare la comunicazione sulla linea. In questi casi si consiglia, inoltre, di prevedere un collegamento costituito da 3 conduttori (A, B, GND) e schermatura, la schermatura va collegata a terra ad un solo capo del cavo.

CARATTERISTICHE DEL PROTOCOLLO

Alcune caratteristiche del protocollo:

- | | | |
|----------------------|-----------------|-----------------------|
| - indirizzo di rete | 1 | definito da parametro |
| - velocità | da 1200 a 38400 | definito da parametro |
| - lunghezza dati | 8 bit | valore fisso |
| - parità | nessuna | valore fisso |
| - numero di stop bit | 1 | valore fisso |

CODICI FUNZIONI DISPONIBILI

- | | | |
|------|---------------------------|---|
| - 01 | Read coil status | lettura variabili binarie read/write |
| - 02 | Read input status | lettura variabili binarie read only |
| - 03 | Read holding registers | lettura variabili analogiche read/write |
| - 04 | Read input registers | lettura variabili analogiche read only |
| - 15 | Force multiple coils | scrittura variabili binarie read/write |
| - 16 | Preset multiple registers | scrittura variabili analogiche read/write |

CABLAGGIO ELETTRICO



Mantenere il cavo di linea più lontano possibile da cavi di potenza, al fine di non compromettere la trasmissione del segnale e quindi la comunicazione tra i dispositivi collegati alla rete.

Per le istruzioni di cablaggio, fare riferimento al MIUM, manuale uso installazione e manutenzione; paragrafo installazione.

MODIFICA CONFIGURAZIONE, INDIRIZZO DI RETE E VELOCITA'

Di default l'unità è impostata con:

- seriale RS485 disabilitata
- indirizzo di rete 1
- velocità 9600

Per la modifica dei parametri seguire questa procedura:

- Posizionarsi sul display
- Dalla schermata principale tenere premuti contemporaneamente i tasti SU, OK e GIÙ per qualche secondo
- con i tasti SU e GIÙ inserire "0010" e premere il tasto OK per confermare (menu installatore)
- con i tasti SU e GIÙ scorrere tra le varie schermate finché non ci si posiziona sulla schermata "RS485 - MODBUS"
- Premendo il tasto OK ci si posiziona sul primo parametro da modificare
- Con i tasti SU e GIÙ si modifica il parametro e con il tasto OK si passa al parametro successivo o si esce dalla modifica
- Premere il tasto Exit per uscire

Nello specifico il parametro "abilitazione seriale" può essere impostato in uno dei modi seguenti:

- **OFF:** unità gestita interamente da display, è sempre consentita la sola lettura di tutte le variabili esposte in seriale.
- **SLAVE:** unità gestita interamente da seriale.
- **MASTER JR:** l'unità controlla via seriale il dispositivo di ionizzazione dell'aria JR.
- **SL-STAGIONE:** l'unità riceve via modbus esclusivamente le variabili riguardanti la stagione (Register Number 3 Read/Write, Coil Number 5 Read/Write), tutti gli altri comandi vengono gestiti da display, è sempre consentita la sola lettura di tutte le altre variabili esposte in seriale.

Analog Input Registers – Read only (signed int, 16 bits) (funzione 04 read)

Register number	Descrizione variabile	LIMITI	U.M.
1	Temperatura ambiente		°C / 10
2	Temperatura esterna		°C / 10
3	Temperatura mandata (se presente kit controllo temperatura mandata)		°C / 10
4	Umidità relativa ambiente (se presente sonda umidità)		% / 10
5	VOC ambiente (se presente sonda VOC)	0 / 2000	ppm
6	CO2 ambiente (se presente sonda CO2)	0 / 2000	ppm
7	Stato ventilatore di mandata		%
8	Stato ventilatore di estrazione		%
9	Stato valvola acqua		%
10	Set effettivo di temperatura		°C / 10
11	Taglia macchina		15/200
12	Ore funzionamento unità		ore
13	Livello ionizzatore effettivo	0 - 4	
14	Ore di ionizzazione effettiva rimanenti prima della successiva pulizia tubi		ore
15	Ore di ionizzazione effettiva rimanenti prima della successiva sostituzione tubi		ore
16	Portata aria in mandata [solo con trasduttori di portata]		m ³ /h
17	Portata aria in estrazione [solo con trasduttori di portata]		m ³ /h

Analog Output Holding Registers - Read/Write (signed int, 16 bits) (funzione 03 read, funzione 16 write)

Register number	Descrizione variabile	LIMITI	U.M.
1	Set temperatura ambiente in celsius	100 / 350	°C / 10
2	Livello di ricambio	0 / 5	
3	Stagione: 0. Estate 1. Inverno 2. Mezza stagione (controllo della temperatura disabilitato)	0 / 2	
4	Orologio ore	0 / 23	
5	Orologio minuti	0 / 59	
6	Orologio giorno	1 / 31	
7	Orologio mese	1 / 12	
8	Orologio anno (ultime 2 cifre)	17 / 99	
9	Orologio giorno della settimana 0. Lunedì 1. Martedì 2. ...	0 / 6	
10	Gestione temperatura di mandata: 0. Off 1. Neutra 2. Controllata	0 / 2	
11	Set temperatura di mandata controllata	100 / 450	°C / 10 °F
12	Set temperatura ambiente in fahrenheit	50 / 100	°F
13	Livello ionizzatore: 0 - 3 = livelli temporizzati 4 = Always on (tubi ionizzanti sempre accesi)	0 - 4	-
14	Set umidità relativa ambiente	30,0 / 95,0	% / 10



Eneren S.r.l.

info@eneren.it - www.eneren.it

Sede Operativa Viale Spagna, 31/33 - 35020 - Tribano (PD) – Italy

Sede Legale Viale Spagna, 31/33 - 35020 - Tribano (PD) - Italy
Tel +39 049 9588511 - Fax +39 049 9588522

Registro AEE: IT18080000010592

È vietata la riproduzione, anche parziale, di questo documento senza l'autorizzazione scritta di Eneren s.r.l.