MODBUS-RTU per TWM3IO

Specifiche protocollo di comunicazione MODBUS-RTU per controllo in rete dispositivi serie TWM3IO

Nome documento: **MODBUS-RTU_TWM3IO_01_13_ITA**
Software installato: **TWM3IO.elf Rev. 0 e successive**

LEGGERE E CONSERVARE

INDICE

1: DESCRIZIONE GENERALE

1.1 IL PROTOCOLLO MODBUS

Il sistema di comunicazione dati basato sul protocollo Modbus consente di collegare fino a 247 strumenti in una linea comune RS485 con modalità e formato di comunicazione standardizzati.
La comunicazione avviene in half duplex per mezzo di frame (trasmesso in maniera continuativa); Solo il master (PC , PLC ...) può iniziare il colloquio con gli slaves del tipo domanda/risposta (un solo slave indirizzato) e lo slave interrogato risponde. La risposta dello slave avviene dopo una pausa minima di 3,5 caratteri tra il frame ricevuto e quello che deve trasmettere.
Esiste anche la modalità di comunicazione broadcast dove il master invia un messaggio a tutti gli slave contemporaneamente, i quali non danno risposta di ritorno; quest'ultima modalità non è però utilizzabile con questo controllo.
La modalità di trasmissione seriale dei dati implementata sul controllo è di tipo RTU (Remote Terminal Unit), dove i dati vengono scambiati in formato binario (caratteri di 8 bit).

1.2 CONFIGURAZIONE SERIALE

Linea seriale:	***RS485***
Baud rate:	***300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400***
Lunghezza dati:	***8 bit***
Parità:	***nessuna, pari o dispari***
Stop bit:	***1 o 2***

Trasmissione seriale dei caratteri in formato RTU

Start	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	Parità (optional)	Stop 1	Stop 2 (optional)

1.3 FORMATO DEI MESSAGGI (FRAME)

Ogni messaggio (Frame) è costituito, secondo lo standard MODBUS-RTU, dalle seguenti parti:

Start	Indirizzo dispositivo	Codice funzione	Dati	CRC16		Stop
silenzio di (3,5 x tempo carattere) msec	Byte	Byte	n x Byte	LSByte	MSByte	silenzio di (3,5 x tempo carattere) msec

- **Start / Stop :**
  Il messaggio inizia con un silenzio di 3.5 volte il tempo di trasmissione di un carattere. Vedi cap. 1.4 per maggiori chiarimenti.

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo con cui il master ha stabilito il colloquio; è un valore compreso tra 1 e 247. L'indirizzo 0 è riservato al broadcast, messaggio inviato a tutti i dispositivi slave (non attivo su questo controllo). La linea RS485 consente di collegare insieme fino a 32 dispositivi (1 Master + 31 slave) , ma con appositi "bridge" o dispositivi ripetitori è possibile sfruttare tutto il campo di indirizzamento logico.

- **Codice funzione:**
  Il codice della funzione da eseguire o che è stata eseguita; Nel dispositivo sono attivi i codici 0x03 (lettura registro), 0x06 (scrittura registro singolo) e 0x2B/0x0E (lettura dati di identificazione).

- **Dati:**
  I dati che devono essere scambiati.

- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16. Il CRC16 viene calcolato sull'intero messaggio dal dispositivo master trasmittente ed appeso al messaggio stesso. Lo slave, alla fine della ricezione, calcola il CRC16 sul messaggio e lo confronta con il valore appeso dal master; se i due valori non corrispondono il messaggio verrà considerato non valido e verrà scartato senza inviare alcuna risposta al master.
  Il seguente frammento di codice C illustra la modalità di calcolo del CRC16:

```
unsigned int CRC16
void Modbus_CRC(unsigned char *Frame, unsigned char FrameLength)
{
unsigned char ByteCount;
unsigned char i;
unsigned char bit_lsb;
CRC16 = 0xFFFF;
for (ByteCount=0;ByteCount<FrameLength;ByteCount++)
  {
  CRC16^=Frame[ByteCount];
  for (i=0;i<8;i++)
    {
    bit_lsb = CRC16 & 0x0001;
    CRC16 = CRC16>>1;
    if (bit_lsb == 1)
      CRC16 ^= 0xA001;
    }
  }
}
```

1.4 SINCRONIZZAZIONE DEI MESSAGGI

La sincronizzazione del messaggio tra trasmettitore e ricevitore si ottiene interponendo una pausa tra i messaggi di almeno 3.5 volte il tempo di trasmissione di un carattere. Se il ricevitore non riceve alcun Byte per almeno questo tempo, ritiene completato il messaggio precedente e considera il successivo Byte ricevuto come il primo di un nuovo messaggio.
Lo slave, una volta ricevuto il messaggio completo, lo decodifica e, se non ci sono errori, invia il messaggio di risposta al master. Per inviare la risposta, lo slave impegna la linea RS485, attende una pausa di almeno 3.5 volte il tempo di trasmissione di un carattere, invia il messaggio completo, attende una pausa di almeno 3.5 volte il tempo di trasmissione di un carattere e poi libera la linea RS485. L'unità master dovrà tenere conto di queste tempistiche, in modo da evitare rischi di sovrapposizione di trasmissioni; in particolare è necessario prevedere un adeguato time-out di ricezione della risposta prima di iniziare una nuova trasmissione (valore tipico di time-out: 500msec o superiore, per baud rate = 9600).

1.5 MESSAGGI DI ERRORE (ECCEZIONI)

Il dispositivo, se non è in grado di eseguire l'operazione richiesta dal comando ricevuto, risponde con un messaggio di errore che prevede il seguente formato:

Indirizzo dispositivo	*Codice funzione*	*Codice eccezione*	*CRC16*	
Byte	Byte	Byte	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave che risponde
- **Codice funzione**:
  Codice funzione con MSb =1 (per indicare l'eccezione); esempio 0x83 (per la lettura 0X03) o 0x86 (per la scrittura 0x06)
- **Codice eccezione**:
  I codici delle eccezioni gestite dal dispositivo sono i seguenti:

Codice eccezione	*Descrizione*	*Causa di generazione eccezione*
0x01	Funzione non implementata	E' stato richiesto un codice funzione non disponibile, diverso da 0x03, 0x06 e 0x2B/0x0E.
0x02	Indirizzo non valido	Viene generato in diverse situazioni: - è stato richiesto un registro non implementato (o un'area inesistente) - è stata richiesta la lettura di un numero di registri che va oltre l'area implementata (partendo dall'indirizzo richiesto) - si è tentato di scrivere in un'area read-only
0x03	Valore non valido per il dato	Viene generato in diverse situazioni: - il DeviceIdCode del messaggio 0x2B/0x0E non è corretto - si è tentato di scrivere un parametro con un valore fuori range

- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16.

Nota:
Nel caso il dispositivo individui nel messaggio ricevuto un errore di formato o nel CRC16 , il messaggio viene scartato (non viene considerato valido) e non viene generata alcuna risposta.

2: DESCRIZIONE COMANDI

Tutti i registri, per uniformare la modalità di interpretazione, sono gestiti in formato Word (16 bit), anche se contengono un parametro ad 8 bit.

2.1 *LETTURA REGISTRO (0x03)*

Formato del comando inviato dal Master:

Indirizzo dispositivo	***Codice funzione***	***Indirizzo registro***		***Numero di registri***		***CRC16***	
Byte	Byte	MSByte	LSByte	MSByte	LSByte	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave da interrogare
- **Codice funzione**:
  Codice funzione da eseguire, in questo caso lettura registro (0x03)
- **Indirizzo registro**:
  indirizzo registro di partenza per la lettura espresso su due Byte; (MSByte) e (LSByte).
- **Numero di registri**:
  indica il numero di Word richieste a partire dall'indirizzo di partenza. Se viene richiesto un numero di registri superiore ad 1, nel messaggio di risposta verranno forniti tutti i registri richiesti con indirizzi consecutivi partendo dall'indirizzo riportato nel campo "indirizzo registro".
  Il numero di registri da leggere è espresso su due Byte, in particolare per questo controllo (MSByte) deve sempre essere 0x00.
- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16.

Formato del messaggio di risposta dello slave:

Indirizzo dispositivo	***Codice funzione***	***N. di Bytes di dato***	***Dato 1***		***Dato 2***		***Dato n***		***CRC16***	
Byte	Byte	Byte	MSByte	LSByte	MSByte	LSByte	MSByte	LSByte	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave che risponde
- **Codice funzione**:
  Codice funzione a cui si sta rispondendo, in questo caso lettura registro (0x03)
- **Numero di Bytes di dato**:
  contiene il numero di Bytes totali dei dati.
  Considerare che il numero di Bytes di dato è il doppio del numero di registri (in quanto si tratta di word). Ad esempio, se nel messaggio di domanda vengono richiesti 2 registri, nel messaggio di risposta il numero di Bytes di dato deve essere impostato a 4.

- **Dato n** :
  contiene la sequenza dei dati ognuno espresso su due Byte; (MSByte) e (LSByte).
- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16.

2.2 *SCRITTURA REGISTRO SINGOLO (0x06)*

Formato del comando inviato dal Master:

Indirizzo dispositivo	*Codice funzione*	*Indirizzo registro*		*Dato*		*CRC16*	
Byte	Byte	MSByte	LSByte	MSByte	LSByte	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave da interrogare
- **Codice funzione**:
  Codice funzione da eseguire, in questo caso scrittura registro singolo (0x06)
- **Indirizzo registro**:
  indirizzo del registro che si vuole scrivere espresso su due Byte; (MSByte) e (LSByte).
- **Dato**:
  Valore che deve essere assegnato al registro espresso su due Byte; (MSByte) e (LSByte).
- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16.

Formato del messaggio di risposta dello slave:

Indirizzo dispositivo	*Codice funzione*	*Indirizzo registro*		*Dato*		*CRC16*	
Byte	Byte	MSByte	LSByte	MSByte	LSByte	LSByte	MSByte

Il messaggio di risposta è un semplice echo del messaggio di richiesta per confermare che la variabile è stata modificata.

2.3 *LETTURA DATI DI IDENTIFICAZIONE DISPOSITIVO (0x2B / 0x0E)*

Formato del comando inviato dal Master:

Indirizzo dispositivo	*Codice funzione*	*Tipo MEI*	*Read Device Id Code*	*Object Id*	*CRC16*	
Byte	Byte	Byte	Byte	Byte	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave da interrogare
- **Codice funzione**:
  Codice funzione da eseguire, in questo caso lettura dati identificazione (0x2B)
- **Tipo MEI**:
  Tipo di Modbus Encapsulated Interface: deve essere 0x0E.
- **Read Device Id Code**:
  Indica il tipo di accesso ai dati: deve essere 0x01.
- **Object Id**:
  Indica l'oggetto di partenza per la lettura dati (range: 0x00 – 0x02).
- **CRC16:**
  Il campo di controllo di errore formato secondo l'algoritmo CRC16.

Formato del messaggio di risposta dello slave:

Indirizzo dispositivo	*Codice funzione*	*Tipo MEI*	*Read Device Id Code*	*Conformity level*	*More Follows*	*Next Object Id*	*Number Of Object*	*Object Id (n)*	*Object Length (n)*	*Object Value (n)*	*CRC16*	
Byte	Byte	Byte	Byte	Byte	Byte	Byte	Byte	Byte	Byte	ASCII String	LSByte	MSByte

- **Indirizzo dispositivo**:
  L'indirizzo del dispositivo slave che risponde
- **Codice funzione**:
  Codice funzione da eseguire, in questo caso lettura dati identificazione (0x2B)
- **Tipo MEI**:
  tipo di Modbus Encapsulated Interface: deve essere 0x0E.
- **Read Device Id Code**:
  indica il tipo di accesso ai dati: deve essere 0x01.
- **Conformity level**:
  indica il livello di conformità dello slave: è sempre 0x01.
- **More Follows**:
  indica il numero di transazioni aggiuntive richieste: è sempre 0x00.
- **Next Object Id**:
  indica l'oggetto da richiedere nell'eventuale successiva transazione: è sempre 0x00
- **Number Of Object**:
  numero di oggetti che seguono (1, 2 o 3).
- **Lista di**:

- **Object Id**:
  numero oggetto corrente.
- **Object Length**:
  lunghezza della stringa seguente.
- **Object Value**:
  stringa ASCII contenente l'informazione di identificazione.

- **CRC16:**

Il campo di controllo di errore formato secondo l'algoritmo CRC16.

Esempio di lettura di tutte le informazioni identificative dei controlli con software TWM3IO rev. 0 ed indirizzo 1

Messaggio di richiesta: (01 2B 0E 01 00 70 77)

- **Indirizzo dispositivo**: 0x01
- **Codice funzione**: 0x2B
- **Tipo MEI**: 0x0E
- **Read DeviceIdCode**: 0x01
- **ObjectId**: 0x00
- **CRC16:** da calcolare sui valori precedenti

Messaggio di risposta: (01 2B 0E 01 01 00 00 03 00 04 50 45 47 4F 01 08 54 57 4D 33 49 4F 5F 5F 02 03 30 30 30 EA D9)

- **Indirizzo dispositivo**: 0x01
- **Codice funzione**: 0x2B
- **Tipo MEI**: 0x0E
- **Read DeviceIdCode**: 0x01
- **Conformity level**: 0x01
- **More Follows**: 0x00
- **Next ObjectId**: 0x00
- **Number Of Object**: 0x03
- **ObjectId**: 0x00
- **Object Length**: 0x04
- **Object Value**: 'PEGO' (campo Vendor Name in ASCII)
- **ObjectId**: 0x01
- **Object Length**: 0x08
- **Object Value**: 'TWM3IO__' (campo Product Code in ASCII)
- **ObjectId**: 0x02
- **Object Length**: 0x03
- **Object Value**: '000' (campo Revision in ASCII)
- **CRC16:** da calcolare sui valori precedenti

3: DESCRIZIONE REGISTRI E INDIRIZZI

Ciascun registro ha una dimensione di 16 bit. Sono stati formati dei blocchi di variabili (ciascuno con diverso MSByte di indirizzo) in base alla tipologia delle variabili stesse. Nei seguenti paragrafi vengono descritti nel dettaglio tutti i blocchi disponibili e, per ciascun blocco, le variabili implementate.
All' inizio di ogni tabella viene indicata nella prima riga se il dati corrispondenti ad essa possono essere solo letti (READ-ONLY) o letti e scritti (READ/WRITE).

DESCRIZIONE COLONNE DELLE TABELLE:

- **Registro** :
  Indica l' indirizzo del registro da utilizzare nella struttura del comando Modbus per leggere o scrivere i dati nello strumento . Esso è espresso su due Byte; (MSByte) e (LSByte).
- **Descrizione** :
  Descrizione del registro ed eventuale corrispondente variabile di programmazione dello strumento.
- **Significato e range Bytes :**
  Dimensione (MSByte e LSByte), range consentito e note relativi al registro.
- **U.M. :**
  Unità di misura del dato contenuto nel registro.
- **Conv. :**
  I valori contenuti nei registri che rappresentano variabili con segno richiedono una conversione e vengono contraddistinti dal segno **X** nella seguente colonna.
  Procedura di conversione:
  - se il valore contenuto nel registro è compreso tra 0 e 32767, esso rappresenta un numero positivo o nullo (il risultato è il valore stesso)
  - se il valore contenuto nel registro è compreso tra 32768 e 65535, esso rappresenta un numero negativo (il risultato è il valore del registro - 65536)
- **Molt :**
  Indica il fattore di moltiplicazione che deve essere applicato al dato del registro e che in abbinamento alla colonna U.m e Conv permettono l'esatta interpretazione del valore in esso contenuto.
  Esempi:
  Un dato **(0x0012)** = 18 con Molt =**0,1** / U.m= **°C** / Conv=**C** corrisponde ad una temperatura di (18x0,1)= **1,8 °C**
  Un dato **(0xFFF0)** = 65520 con Molt =**0,1** / U.m= **°C** / Conv=**C** corrisponde ad una temperatura [(65520 – 65536) x0,1] = **-1,6 °C**
  Un dato **(0x0078)** = 120 con Molt =**1** / U.m= **min** / Conv=**C** corrisponde ad un tempo di (120x1)= **120 minuti**
  Un dato **(0x0014)** = 20 con Molt =**0,1** / U.m= **°C** / Conv=**C** corrisponde ad una temperatura di (20x0,1)= **2,0 °C**

3.1 *INGRESSI – USCITE DIGITALI*

READ-ONLY						
Registro	***Descrizione***	***Significato e range Bytes***		***U.M.***	***Conv***	***Molt***
256	Ingresso digitale 1	MSByte LSByte	1 = ingresso attivo 0 = ingresso disattivo	-	-	-
257	Ingresso digitale 2	MSByte LSByte	1 = ingresso attivo 0 = ingresso disattivo	-	-	-
258	Ingresso digitale 3	MSByte LSByte	1 = ingresso attivo 0 = ingresso disattivo	-	-	-
259	Uscita digitale 1	MSByte LSByte	1 = uscita attiva 0 = uscita disattiva	-	-	-

3.2 PARAMETRI

READ / WRITE						
Registro	**Descrizione**	**Significato e range Bytes**		**U.M.**	**Conv**	**Molt**
768	**DI1** Configurazione ingresso digitale 1	MSByte	-2 = allarme, attivo se ingresso in circuito aperto -1 = attivo se ingresso in circuito aperto 0 = disabilitato 1 = attivo se ingresso in circuito chiuso 2 = allarme, attivo se ingresso in circuito chiuso	num	X	1
		LSByte				
769	**DI2** Configurazione ingresso digitale 2	MSByte	-2 = allarme, attivo se ingresso in circuito aperto -1 = attivo se ingresso in circuito aperto 0 = disabilitato 1 = attivo se ingresso in circuito chiuso 2 = allarme, attivo se ingresso in circuito chiuso	num	X	1
		LSByte				
770	**DI3** Configurazione ingresso digitale 3	MSByte	-2 = allarme, attivo se ingresso in circuito aperto -1 = attivo se ingresso in circuito aperto 0 = disabilitato 1 = attivo se ingresso in circuito chiuso 2 = allarme, attivo se ingresso in circuito chiuso	num	X	1
		LSByte				
771	**DO1** Configurazione uscita digitale 1	MSByte	-2 = disattiva se sono presenti tutti gli allarmi -1 = disattiva se è presente almeno un allarme 0 = comandata da remoto (Telenet/Modbus) 1 = attiva se è presente almeno un allarme 2 = attiva se sono presenti tutti gli allarmi	num	X	1
		LSByte				
772	**Ald** Tempo di ritardo segnalazione e visualizzazione allarme	MSByte	passi di 1, senza segno range: 0..65535	num		1
		LSByte				

3.3 STATO INGRESSI / USCITE / ALLARMI

READ-ONLY							
Registro	**Descrizione**	**Significato Bytes**			**U.M.**	**Conv**	**Molt**
1280	stato allarmi	MSByte	bit 7 (MSb)	Non utilizzati	num		1
			bit 6				
			bit 5				
			bit 4				
			bit 3				
			bit 2				
			bit 1				
			bit 0 (LSb)				
		LSByte	bit 7 (MSb)	Non utilizzato			
			bit 6	Non utilizzato			
			bit 5	Non utilizzato			
			bit 4	errore EEPROM (EM)			
			bit 3	Allarme ingresso digitale 3 (E3)			
			bit 2	Allarme ingresso digitale 2 (E2)			
			bit 1	Allarme ingresso digitale 1 (E1)			
			bit 0 (LSb)	Tutti gli ingressi disabilitati (E0)			

3.4 STATO DISPOSITIVO

READ / WRITE							
Registro	**Descrizione**	**Significato Bytes**			**U.M.**	**Conv**	**Molt**
1536	stato dispositivo	MSByte	bit 7 (MSb)	non utilizzato	num		1
			bit 6	non utilizzato			
			bit 5	non utilizzato			
			bit 4	non utilizzato			
			bit 3	non utilizzato			
			bit 2	non utilizzato			
			bit 1	non utilizzato			
			bit 0 (LSb)	abilitaz. modifica stato uscita			
		LSByte	bit 7 (MSb)	non utilizzato			
			bit 6	non utilizzato			
			bit 5	non utilizzato			
			bit 4	non utilizzato			
			bit 3	non utilizzato			
			bit 2	non utilizzato			
			bit 1	non utilizzato			
			bit 0 (LSb)	stato uscita (solo se DO1=0) 1 = ON 0 = OFF			

Per richiedere la modifica di uno dei bit di stato del dispositivo, il master deve inviare nel LSByte il valore richiesto per il bit e nel MSByte il corrispondente bit settato a 1. Esempio: per forzare lo stato di stand-by, il master deve inviare MSByte = 00000001 e LSByte = 00000001.

4: GLOSSARIO

- **Numero Binario:**
  È usato in informatica per la rappresentazione interna dei numeri, grazie alla semplicità di realizzare fisicamente un elemento con due stati (0,1) anziché un numero superiore, ma anche per la corrispondenza con i valori logici vero e falso.

- **Numero decimale:**
  Nel sistema decimale tutti gli interi sono rappresentabili utilizzando le dieci cifre che indicano i primi dieci numeri naturali, incluso lo zero. Il valore di ciascuna di queste cifre dipende dalla posizione che essa occupa all'interno del numero, e cresce di potenza di 10 in potenza di 10, procedendo da destra verso sinistra.

- **Numero esadecimale:**
  Esso fa parte di un sistema numerico posizionale in base 16, cioè che utilizza 16 simboli invece dei 10 del sistema numerico decimale tradizionale. Per l'esadecimale si usano in genere simboli da 0 a 9 e poi le lettere da A a F, per un totale di 16 simboli. Per convenzione un numero espresso in esadecimale viene preceduto da 0x (esempio 0x03) oppure da H (esempio H03).

- **bit:**
  Un bit è una cifra binaria, (in inglese "binary digit") ovvero uno dei due simboli del sistema numerico binario, classicamente chiamati zero (0) e uno (1). Esso rappresenta l'unità di definizione di uno stato logico. Definito anche unità elementare dell'informazione trattata da un elaboratore.

- **Byte:**
  È la quantità necessaria di bit per definire un carattere alfanumerico; in particolare un Byte è costituito da una sequenza di 8 bit (es. 10010110).

- **Word:**
  Unità di misura che fissa la lunghezza si informazione a 16bits che equivale anche a 2 Bytes
  (es. 10010110 01101011).

- **LSb:**
  bit meno significativo di un numero binario (primo bit sulla destra del numero indicato)

- **MSb:**
  bit più significativo di un numero binario (primo bit sulla sinistra del numero indicato)

- **LSByte:**
  Byte meno significativo di una Word (Byte sulla destra della Word indicata)

- **MSByte:**
  Byte più significativo di una Word (Byte sulla sinistra della Word indicata)

PEGO S.r.l.
Via Piacentina, 6/b
45030 OCCHIOBELLO –ROVIGO-
Tel : 0425 762906
Fax: 0425 762905
www.pego.it
e-mail: info@pego.it

Distributore: