

Tema 7. Protocolo Modbus

1 Introducción

La designación Modbus Modicon corresponde a una marca registrada por Gould Inc. Como en tantos otros casos, la designación no corresponde propiamente al estándar de red, incluyendo todos los aspectos desde el nivel físico hasta el de aplicación, sino a un protocolo de enlace (nivel OSI 2). Puede, por tanto, implementarse con diversos tipos de conexión física y cada fabricante suele suministrar un software de aplicación propio, que permite parametrizar sus productos.

No obstante, se suele hablar de MODBUS como un estándar de bus de campo, cuyas características esenciales son las que se detallan a continuación.

2 Estructura de la red

Medio Físico

El medio físico de conexión puede ser un bus semidúplex (half duplex) (RS-485 o fibra óptica) o dúplex (full duplex) (RS-422, BC 0-20mA o fibra óptica).

La comunicación es asíncrona y las velocidades de transmisión previstas van desde los 75 baudios a 19.200 baudios. La máxima distancia entre estaciones depende del nivel físico, pudiendo alcanzar hasta 1200 m sin repetidores.

Acceso al Medio

La estructura lógica es del tipo maestro-esclavo, con acceso al medio controlado por el maestro. El número máximo de estaciones previsto es de 63 esclavos más una estación maestra.

Los intercambios de mensajes pueden ser de dos tipos:

- Intercambios punto a punto, que comportan siempre dos mensajes: una demanda del maestro y una respuesta del esclavo (puede ser simplemente un reconocimiento («acknowledge»).
- Mensajes difundidos. Estos consisten en una comunicación unidireccional del maestro a todos los esclavos. Este tipo de mensajes no tiene respuesta por parte de los esclavos y se suelen emplear para mandar datos comunes de configuración, reset, etc.

3 Protocolo

La codificación de datos dentro de la trama puede hacerse en modo ASCII o puramente binario, según el estándar RTU (Remote Transmission Unit). En cualquiera de los dos casos, cada mensaje obedece a una trama que contiene cuatro campos principales, según se muestra en la figura 1. La única diferencia estriba en que la trama ASCII incluye un carácter de encabezamiento («:»=3A_H) y los caracteres CR y LF al final del mensaje. Pueden existir también diferencias en la forma de calcular el CRC, puesto que el formato RTU emplea una fórmula polinómica en vez de la simple suma en módulo 16. Con independencia de estos pequeños detalles, a continuación se da una breve descripción de cada uno de los campos del mensaje:

: (3A _H)	Nº Esclavo (00-3F _H)	Código de Operación	Subfunciones, Datos	LRC(16) H L	CR (0D _H)	LF (0A _H)
-------------------------	--	---------------------------	---------------------	----------------	--------------------------	--------------------------

Codificación ASCII

Nº Esclavo (00-3F _H)	Código de Operación	Subfunciones, Datos	CRC(P16) H L
--	---------------------------	---------------------	-----------------

Codificación RTU

Figura 1. Trama genérica del mensaje según el código empleado

Número de esclavo (1 byte):

Permite direccionar un máximo de 63 esclavos con direcciones que van del 01_H hasta 3F_H. El número 00_H se reserva para los mensajes difundidos.

Código de operación o función (1 byte):

Cada función permite transmitir datos u órdenes al esclavo. Existen dos tipos básicos de órdenes:

- Órdenes de lectura/escritura de datos en los registros o en la memoria del esclavo.
- Órdenes de control del esclavo y el propio sistema de comunicaciones (RUN/STOP, carga y descarga de programas, verificación de contadores de intercambio, etc.)

La tabla 1 muestra la lista de funciones disponibles en el protocolo MODBUS con sus correspondientes códigos de operación.

Campo de subfunciones/datos (n bytes):

Este campo suele contener, en primer lugar, los parámetros necesarios para ejecutar la función indicada por el byte anterior. Estos parámetros podrán ser códigos de subfunciones en el caso de órdenes de control (función 00_H) o direcciones del primer bit o byte, número de bits o palabras a leer o escribir, valor del bit o palabra en caso de escritura, etc.

Palabra de control de errores (2 bytes):

En código ASCII, esta palabra es simplemente la suma de comprobación ('checksum') del mensaje en módulo 16 expresado en ASCII. En el caso de codificación RTU el CRC se calcula con una fórmula polinómica según el algoritmo mostrado en la figura 2.

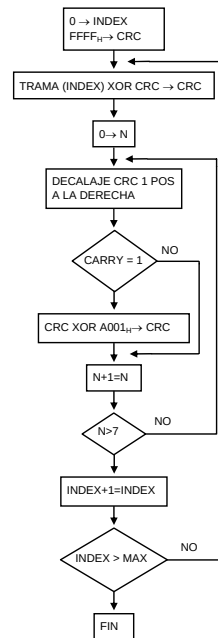
Función	Código	Tarea
0	00 _H	Control de estaciones esclavas
1	01 _H	Lectura de <i>n</i> bits de salida o internos
2	02 _H	Lectura de <i>n</i> bits de entradas
3	03 _H	Lectura de <i>n</i> palabras de salidas o internos
4	04 _H	Lectura de <i>n</i> palabras de entradas
5	05 _H	Escritura de un bit
6	06 _H	Escritura de una palabra
7	07 _H	Lectura rápida de 8 bits
8	08 _H	Control de contadores de diagnósticos número 1 a 8
9	09 _H	No utilizado
10	0A _H	No utilizado
11	0B _H	Control del contador de diagnósticos número 9
12	0C _H	No utilizado
13	0D _H	No utilizado
14	0E _H	No utilizado
15	0F _H	Escritura de <i>n</i> bits
16	10 _H	Escritura de <i>n</i> palabras

Tabla 1. Funciones básicas y códigos de operación**3.1 Descripción de las funciones del protocolo****Función 0:**

Esta función permite ejecutar órdenes de control, tales como marcha, paro, carga y lectura de programas de usuario del autómat. Para codificar cada una de las citadas órdenes se emplean los cuatro primeros bytes del campo de datos. La trama resultante es la representada en la figura 3 y la interpretación de los códigos de subfunción se especifica en la tabla 2.

En caso de las órdenes de marcha y paro, el campo de «información» de la trama representada en la figura 3 está vacío y, por tanto, el mensaje se compone simplemente de 6 bytes de función más 2 bytes de CRC. La respuesta del esclavo a estas órdenes es un mensaje idéntico al enviado por el maestro. Cabe señalar, además, que después de un paro el autómat sólo acepta ejecutar subfunciones de la función 00_H.

Nº Esclavo (00-3F ₁₆)	00 _H	Código Subfunción SF0 SF1	Datos Subfunción D0 D1	Información	CRC(16) H L
-----------------------------------	-----------------	---------------------------	------------------------	-------------	-------------

Figura 3. Trama genérica de las subfunciones de control de esclavos (cód. función 00H)**Figura 2. Cálculo del CRC codificación RTU**

Código subfunción SF0 SF1		Datos subfunción D0 D1		Tarea
00 _H	00 _H	00 _H	00 _H	
00 _H	01 _H	00 _H	00 _H	Paro del esclavo sin inicializar
00 _H	02 _H	00 _H	00 _H	Marcha del esclavo sin inicializar
00 _H	03 _H	00 _H	00 _H	Marcha e inicialización del esclavo
00 _H	04 _H	00 _H	XX _H	Lectura de la secuencia XX de programa de usuario en el esclavo
00 _H	05 _H	YY _H	XX _H	Carga de una secuencia de programa de usuario en el esclavo Petición: YY = secuencia a cargar, XX= próxima secuencia Respuesta: XX= código error, YY= 00

Tabla 2. Subfunciones correspondientes a la función =00H**Funciones 1 y 2:**

Lectura de bits del autómat. La trama es la indicada en la figura 4. La forma de direccionamiento de los bits es a base de dar la dirección de la palabra que los contiene y luego la posición del bit. Obsérvese también que la respuesta es dada siempre en octetos completos.

Petición del maestro

Nº Esclavo (00-3F ₁₆)	01 _H o 02 _H	Dirección 1º Bit PP PB	Nº de Bits NN NN	CRC H L
-----------------------------------	-----------------------------------	------------------------	------------------	---------

PPP = Dirección de la palabra (hex), B = Dirección del bit dentro de la palabra 0 a F₁₆.

Respuesta del esclavo

Nº Esclavo (00-3F ₁₆)	01 _H o 02 _H	Nº Octetos leídos NN NN	1º Octeto B7..B0	Otros Octetos Hasta máx. 256	CRC H L
-----------------------------------	-----------------------------------	-------------------------	------------------	------------------------------	---------

Figura 4. Petición y respuesta de la función: Lectura de bits (01H, 02H)**Funciones 3 y 4:**

Lectura de palabras del autómat. La trama es la indicada en la figura 5. Obsérvese que la petición indica el número de palabras a leer, mientras que en la respuesta se indica el número de octetos leídos.

Petición del maestro

Nº Esclavo (00-3F ₁₆)	03 _H o 04 _H	Dirección 1ª Palabra PP PP	Nº de Palabras NN NN	CRC H L
-----------------------------------	-----------------------------------	----------------------------	----------------------	---------

PPPP = Dirección de la palabra (hex)

Respuesta del esclavo

Nº Esclavo (00-3F ₁₆)	03 _H o 04 _H	Nº Octetos leídos NN NN	1ª Palabra H L	Otras Palabras Hasta máx. 128 H L, H L, HL, ...	CRC H L
-----------------------------------	-----------------------------------	-------------------------	----------------	---	---------

Figura 5. Petición y respuesta de la función: Lectura de palabras (03H, 04H)

Función 5:

Escritura de un bit. La trama es la indicada en la figura 6. El direccionamiento del bit se efectúa tal como se ha indicado para las funciones 1 y 2.

Petición del maestro

Nº Esclavo (00-3F _H)	05 _H	Dirección Bit PP PB	XX _H	00 _H	CRC H L
--	-----------------	---------------------------	-----------------	-----------------	------------

PPP = Dirección de la palabra (hex), B= Dirección del bit dentro de la palabra 0 a F_H.

Respuesta del esclavo

Nº Esclavo (00-3F _H)	05 _H	Dirección Bit PP PB	XX _H	00 _H	CRC H L
--	-----------------	---------------------------	-----------------	-----------------	------------

XX_H = 00H para bit = 0 y XX_H = FF_H para bit = 1

Figura 6. Petición y respuesta de la función: Escritura de un bit (05H)**Función 6:**

Escritura de una palabra. La trama es la indicada en la figura 7.

Petición del maestro

Nº Esclavo (00-3F _H)	06 _H	Dirección Palabra PP PP	Valor Palabra DD DD	CRC H L
--	-----------------	-------------------------------	---------------------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	06 _H	Dirección Palabra PP PP	Nº de Palabras DD DD	CRC H L
--	-----------------	-------------------------------	----------------------------	------------

Figura 7. Petición y respuesta de la función: Escritura de una palabra (06H)**Función 7:**

Petición de lectura rápida de un octeto. La trama es la mostrada en la figura 8. Obsérvese que la petición no tiene campo de dirección, esto es debido a que el octeto legible por esta función es fijo en cada esclavo y viene fijado en su configuración.

Petición del maestro

Nº Esclavo (00-3F _H)	07 _H	CRC H L
--	-----------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	07 _H	Valor Octeto DD	CRC H L
--	-----------------	-----------------------	------------

Figura 8. Petición y respuesta de la función: Lectura rápida de un octeto (07H)**Función 8:**

Petición del contenido y control de los 8 primeros contadores de diagnóstico de un esclavo (véase tabla 3). Las tramas de petición y respuesta pueden verse en la figura 9.

Petición del maestro

Nº Esclavo (00-3F _H)	08 _H	Código Subfunción SF0 SF1	Dato Subfunción D0 D1	CRC H L
--	-----------------	---------------------------------	-----------------------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	08 _H	Código Subfunción SF0 SF1	Valor Contador H L	CRC H L
--	-----------------	---------------------------------	--------------------------	------------

Figura 9. Petición y respuesta de la función: Control de contadores (08H)

Subfunción		Datos		Tarea	
Nº	Código	D0	D1		
0	00 _H	00 _H	XY _H	ZT _H	El esclavo envía el eco XYZT de petición como test.
3	00 _H	03 _H	ZZ _H	00 _H	Modifica el carácter de fin de trama en modo ASCII por ZZ _H
10	00 _H	0A _H	00 _H	00 _H	Puesta a cero de los contadores
11	00 _H	0B _H	00 _H	00 _H	Lectura del contador 1
12	00 _H	0C _H	00 _H	00 _H	Lectura del contador 1
13	00 _H	0D _H	00 _H	00 _H	Lectura del contador 1
14	00 _H	0E _H	00 _H	00 _H	Lectura del contador 1
15	00 _H	0F _H	00 _H	00 _H	Lectura del contador 1
18	00 _H	12 _H	00 _H	00 _H	Lectura del contador 1

Tabla 3**Función 11:**

La petición del contenido del contador de diagnóstico número 9, no se realiza por la función 8, sino por la función 11. Las tramas de petición y respuestas son las indicadas por la figura 10.

Petición del maestro

Nº Esclavo (00-3F _H)	0B _H	CRC H L
--	-----------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	0B _H	00 00	Valor Contador H L	CRC H L
--	-----------------	-------	--------------------------	------------

Figura 10. Petición y respuesta de la función: Contenido contador 9 (0BH)**Función 15:**

Escritura de bits del autómatas. La trama es la indicada en la figura 11. La forma de direccionamiento es análoga a la indicada para las funciones 1 y 2.

Petición maestro

Nº Esclavo (00-3F _H)	0F _H	Dirección 1º Bit PP PB	Nº de Bits NN NN	Nº de Octetos M	Valor de los bits 8xM valores	CRC H L
-------------------------------------	-----------------	------------------------------	---------------------	--------------------	----------------------------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	0F _H	Dirección 1º Bit PP PB	Nº de Bits NN NN	CRC H L
-------------------------------------	-----------------	------------------------------	---------------------	------------

Figura 7.11. Petición y respuesta: Escritura de bits (0FH)

Función 16:

Escritura de palabras del autómat. La trama es la indicada en la figura 12.

Petición maestro

Nº Esclavo (00-3F _H)	10F _H	Dirección 1ª Palabra PP PP	Nº de Palabras NN NN	Nº de Octetos M	Valor de las palabras HL, HL, ...	CRC H L
-------------------------------------	------------------	----------------------------------	-------------------------	--------------------	--------------------------------------	------------

Respuesta del esclavo

Nº Esclavo (00-3F _H)	10 _H	Dirección 1ª Palabra PP PP	Nº de Palabras NN NN	CRC H L
-------------------------------------	-----------------	----------------------------------	-------------------------	------------

Figura 12. Petición y respuesta: Escritura de palabras (10H)

Mensajes de error:

Puede ocurrir que un mensaje se interrumpa antes de terminar. Cada esclavo interpreta que el mensaje ha terminado si transcurre un tiempo de silencio equivalente a 3,5 caracteres. Después de este tiempo el esclavo considera que el carácter siguiente es el campo de dirección de esclavo de un nuevo mensaje.

Cuando un esclavo recibe una trama incompleta o errónea desde el punto de vista lógico, envía un mensaje de error como respuesta, excepto en el caso de mensajes de difusión. La trama del mensaje de error es la indicada en la figura 13.

Respuesta del esclavo

Nº Esclavo (00-3F _H)	Código Función	Código Error	CRC H L
-------------------------------------	-------------------	-----------------	------------

Figura 13. Trama de mensaje de error

Código Función = Código función recibido + 80_H

Código Error = 01 Código de Función erróneo:

- 02 Dirección incorrecta
- 03 Datos incorrectos
- 06 Autómata ocupado

Si la estación maestra no recibe respuesta de un esclavo durante un tiempo superior a un límite establecido, declara el esclavo fuera de servicio, a pesar de que al cabo de un cierto número de ciclos hace nuevos intentos de conexión.

3.2 Nivel de aplicación

Como se ha dicho a nivel general de buses de campo, el nivel de aplicación de MODBUS no está cubierto por un software estándar, sino que cada fabricante suele suministrar programas para controlar su propia red. No obstante, el nivel de concreción en la definición de las funciones permite al usuario la confección de software propio para gestionar cualquier red, incluso con productos de distintos fabricantes.

4 Variantes de MODBUS

4.1 JBUS

JBUS es una designación utilizada por la firma APRIL para un bus propio que presenta gran similitud con MODBUS, con protocolos prácticamente idénticos.

La designación JBUS, de la misma forma que MODBUS, corresponde a un protocolo de enlace más que a una red propiamente dicha. Puede, por tanto, implementarse con cualquiera de las conexiones físicas normalizadas.

4.2 Comparación entre JBUS y MODBUS

La arquitectura de la red, el formato general de la trama y muchos de los códigos de función de ambos buses coinciden exactamente. Existen, sin embargo, algunos códigos de función cambiados, otros que presentan ligeras diferencias o funciones añadidas.

Como diferencias más relevantes citaremos las siguientes:

- Posee un registro de estado en cada estación que permite un diagnóstico de la estación.
- El número de esclavo para JBUS (1er byte de la trama) permite valores que van del 01H hasta el FFH. Permite, por tanto, direccionar 255 esclavos en vez de 63. El número 00H se reserva igualmente para mensajes difundidos.
- Las funciones disponibles son prácticamente las mismas en ambos protocolos, pero algunos códigos de función (2º byte de la trama) y de las subfunciones no coinciden.

Función	Código	Tarea
1	01 _H	Lectura de <i>n</i> bits de salida o internos
2	02 _H	Lectura de <i>n</i> bits de entradas
3	03 _H	Lectura de <i>n</i> palabras de salidas o internos
4	04 _H	Lectura de <i>n</i> palabras de entradas
5	05 _H	Escritura de un bit
6	06 _H	Escritura de una palabra
7	07 _H	Lectura rápida de 8 bits
15	0F _H	Escritura de <i>n</i> bits
16	10 _H	Escritura de <i>n</i> palabras

Tabla 4. Funciones idénticas Modbus Jbus

4.3 MODBUS® TCP/IP

MODBUS® TCP/IP es una variante o extensión del protocolo Modbus que permite utilizarlo sobre la capa de transporte TCP/IP. De este modo, Modbus-TCP se puede utilizar en Internet, de hecho, este fue uno de los objetivos que motivó su desarrollo (la especificación del protocolo se ha remitido a la IETF=Internet Engineering Task Force). En la práctica, un dispositivo instalado en Europa podría ser direccionado desde EEUU o cualquier otra parte del mundo.

Las ventajas para los instaladores o empresas de automatización son innumerables:

- Realizar reparaciones o mantenimiento remoto desde la oficina utilizando un PC, reduciendo así los costes y mejorando el servicio al cliente.
- El ingeniero de mantenimiento puede entrar al sistema de control de la planta desde su casa, evitando desplazamientos.
- Permite realizar la gestión de sistemas distribuidos geográficamente mediante el empleo de las tecnologías de Internet/Intranet actualmente disponibles.

MODBUS® TCP/IP se ha convertido en un estándar industrial *de facto* debido a su simplicidad, bajo coste, necesidades mínimas en cuanto a componentes de hardware, y sobre todo a que se trata de un protocolo abierto.

En la actualidad hay cientos de dispositivos MODBUS® TCP/IP disponibles en el mercado. Se emplea para intercambiar información entre dispositivos, así como monitorizarlos y gestionarlos. También se emplea para la gestión de entradas/salidas distribuidas, siendo el protocolo más popular entre los fabricantes de este tipo de componentes.

La combinación de una red física versátil y escalable como Ethernet con el estándar universal de interredes TCP/IP y una representación de datos independiente de fabricante, como MODBUS®, proporciona una red abierta y accesible para el intercambio de datos de proceso.

El protocolo Modbus TCP

Modbus/TCP simplemente encapsula una trama Modbus en un segmento TCP. TCP proporciona un servicio orientado a conexión fiable, lo que significa que toda consulta espera una respuesta.

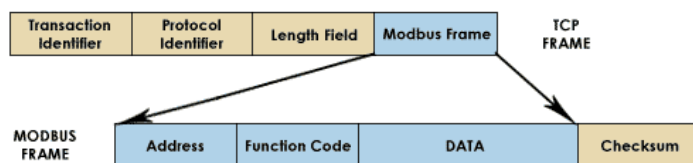


Figura 14. Encapsulamiento de la trama Modbus en TCP.

Esta técnica de consulta/respuesta encaja perfectamente con la naturaleza Maestro/Esclavo de Modbus, añadido a la ventaja del determinismo que las redes

Ethernet conmutadas ofrecen a los usuarios en la industria. El empleo del protocolo abierto Modbus con TCP proporciona una solución para la gestión desde unos pocos a decenas de miles de nodos.

Prestaciones de un sistemas MODBUS TCP/IP

Las prestaciones dependen básicamente de la red y el hardware. Si se usa MODBUS® TCP/IP sobre Internet, las prestaciones serán las correspondientes a tiempos de respuesta en Internet, que no siempre serán las deseables para un sistema de control. Sin embargo pueden ser suficientes para la comunicación destinada a depuración y mantenimiento, evitando así desplazamientos al lugar de la instalación.

Si disponemos de una Intranet de altas prestaciones con conmutadores Ethernet de alta velocidad, la situación es totalmente diferente.

En teoría, MODBUS® TCP/IP, transporta datos hasta 250/(250+70+70) o alrededor de un 60% de eficiencia cuando se transfieren registros en bloque, y puesto que 10 Base T proporciona unos 1.25 Mbps de datos, la velocidad de transferencia de información útil será:

$$1.25M / 2 * 60\% = 360000 \text{ registros por Segundo}$$

En 100BaseT la velocidad es 10 veces mayor.

Esto suponiendo que se están empleando dispositivos que pueden dar servicio en la red Ethernet aprovechando todo el ancho de banda disponible.

En los ensayos prácticos realizados por by Schneider Automation utilizando un PLC Ethernet Momentum™ con entradas/salidas Ethernet, demostró que se podían escanear hasta 4000 bloques I/O por segundo, cada uno con hasta 16 I/O analógicas de 12-bits o 32 I/O digitales (se pueden actualizar 4 bases por milisegundo). Aunque estos resultados están por debajo del límite teórico calculado anteriormente, pero debemos recordar que el dispositivo se probó con una CPU de baja velocidad (80186 a 50MHz con 3 MIPS).

Además, el abaratamiento de los ordenadores personales y el desarrollo de redes Ethernet cada vez más rápidas, permite elevar las velocidades de funcionamiento, a diferencia de otros buses que están inherentemente limitados una sola velocidad.

Cómo podemos comunicar dispositivos MODBUS existentes sobre MODBUS TCP/IP?

Puesto que MODBUS® TCP/IP es simplemente un protocolo MODBUS® encapsulado en TCP, es muy sencillo comunicar dispositivos MODBUS® existentes sobre MODBUS® TCP/IP. Para ello se requiere una pasarela que convierta el protocolo MODBUS a MODBUS TCP/IP.